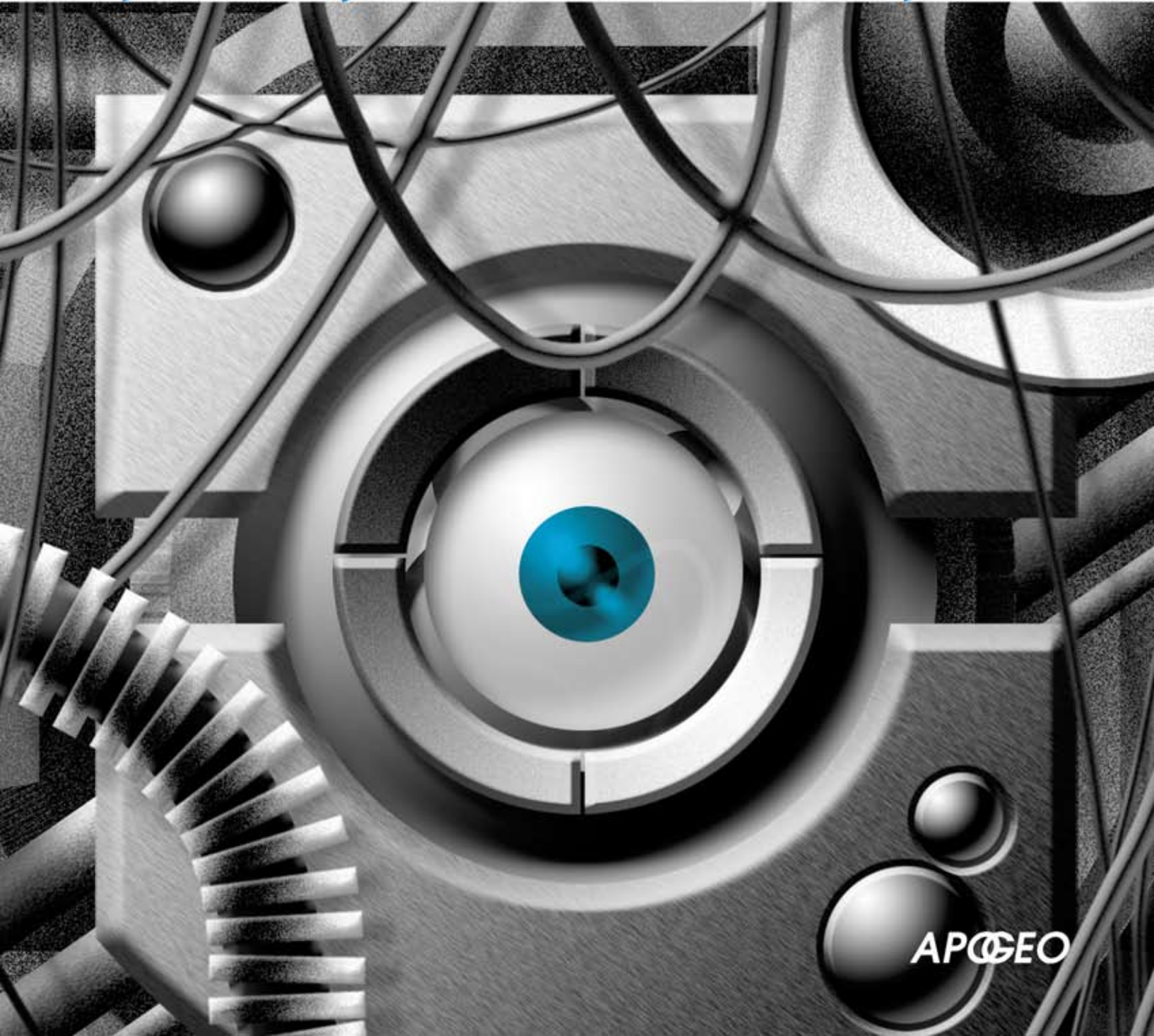




Stefano Bimbo
Enrico Colaiacovo

Sistemi SCADA

Supervisory control and data acquisition



APGEO

Sistemi SCADA

Autori:

Stefano Bimbo, Enrico Colaiacovo

Copyright © 2006 Stefano Bimbo, Enrico Colaiacovo

APOGEO srl

Socio Unico Giangiacomo Feltrinelli Editore srl

Via Natale Battaglia 12 – 20127 Milano (Italy)

Telefono: 02-289981 – Telefax: 02-26116334

Email ebook@apogeeonline.com

U.R.L. <http://www.apogeeonline.com/libri/88-503-1042-0/scheda>

ISBN 88-503-1042-0

**Impaginazione elettronica in $L^A T_{E}X$ a cura degli Autori
Copertina di Enrico Marcandalli**

È garantito il permesso di copiare, distribuire e/o modificare questo documento seguendo i termini della Licenza per la Documentazione Libera GNU, Versione 1.2 o ogni versione successiva pubblicata dalla Free Software Foundation; senza alcuna sezione non modificabile, senza testo di copertina e senza testo di quarta di copertina. Una copia della licenza è acclusa nella sezione intitolata Licenza per la Documentazione Libera GNU.

Sistemi SCADA

Supervisory control and data acquisition

Stefano Bimbo
Enrico Colaiacovo

Premessa

La realizzazione di un libro dedicato ai sistemi SCADA (*Supervisory Control And Data Acquisition*) è il frutto di un'esigenza alla quale le pubblicazioni disponibili nel momento in cui questa è iniziata non sono state in grado di dare una risposta. Lo spazio dedicato a questo tipo di sistemi è molto limitato e la trattazione è, di solito, sintetica e generica. La causa di questa lacuna è nel fatto che tali sistemi non appartengono a una categoria riconducibile a una specifica disciplina tecnologica ma sono caratterizzabili allo stesso tempo come sistemi informatici e come sistemi di controllo.

La necessità di disporre di un testo di riferimento in grado di presentare gli elementi fondamentali dei quali un sistema SCADA è dotato non coincide con l'esigenza di realizzare un testo completo, la *bibbia* di circostanza. Con questa consapevolezza la realizzazione è stata affrontata con lo scopo di disporre di uno strumento di introduzione al tema lasciando a un impegno futuro e a individui dotati delle adeguate competenze la produzione del testo sacro dei sistemi di supervisione e controllo.

Indice

I	Generalità	3
1	Cos'è un sistema SCADA	5
1.1	Gestione di un depuratore di liquami e acque reflue	6
1.2	Gestione del traffico ferroviario	10
1.3	Telerilevamento ambientale terrestre	14
2	SCADA: definizioni	17
2.1	Acquisizione dati	18
2.2	Supervisione	19
2.3	Controllo	19
2.4	SCADA vs DCS	19
3	Il processo controllato	21
3.1	Realtime	22
3.2	Alta affidabilità	23
3.3	Alta disponibilità	23
3.4	Grado d'interazione uomo-macchina	24
3.5	Sistemi di dimensioni geografiche	25
II	Architettura	27
4	Introduzione	29
5	Apparati di acquisizione dati	31
5.1	Funzionamento	31
5.2	Informazioni gestite	32
5.2.1	Classificazione in base alla direzione delle informazioni	33
5.2.2	Classificazione in base alla qualità delle informazioni	33
5.2.3	Classificazione in base alle caratteristiche elettriche	40
5.3	Tecnologia costruttiva	43

5.4	Evoluzione degli apparati di acquisizione dati	44
6	Protocolli e tecnologie di comunicazione	47
6.1	Velocità	48
6.2	Sicurezza	49
6.3	Servizi supportati	50
6.4	Affidabilità	51
6.5	Disponibilità	52
6.6	Intelligibilità	54
7	Sistema di elaborazione	55
7.1	Gestione dei dati	56
7.2	Processi di elaborazione	58
7.3	Condivisione dell'informazione	59
III	Sistema di elaborazione	61
8	Elaborazione dati	63
8.1	Trattamento dati	64
8.1.1	Tipi di dati	64
8.1.2	Database runtime	65
8.1.3	Configurazione dei dati trattati	67
8.2	Elaborazione comandi	72
8.2.1	Un buon motivo per realizzare azioni automatiche . . .	73
8.2.2	Motivi che impongono l'uso di azioni automatiche . . .	75
8.2.3	Caratteristiche delle azioni automatiche	76
8.2.4	Algoritmi e procedure	80
8.3	Calcoli in linea	81
8.3.1	Informazioni di tipo aggregato	82
8.3.2	Informazioni logiche	83
8.3.3	Informazioni statistiche	83
9	Interfaccia uomo-macchina	85
9.1	Caratteristiche	85
9.2	Funzioni	86
9.2.1	Presentazione dei dati	87
9.2.2	Gestione dei comandi operatore	92
9.3	Evoluzione	95

10	Eventi e allarmi	97
10.1	Differenza tra eventi e allarmi	97
10.2	Trattamento	99
10.2.1	Categorie	100
10.2.2	Priorità	101
10.2.3	Disabilitazione dinamica	101
10.2.4	Permessi operatore	102
10.3	Evoluzione dei sistemi di avviso	103
11	Archiviazione	105
11.1	Perché archiviare i dati	105
11.1.1	Studio del processo	105
11.1.2	Documentazione storica	106
11.1.3	Interesse statistico o contabile	107
11.2	Metodi e tecnologie	108
11.2.1	Organizzazione e modalità di archiviazione	108
11.2.2	Strumenti	110
12	Analisi dei dati	113
12.1	Trend Storici	113
12.2	Diagrammi e tabulati	116
12.3	Strumenti specifici di analisi	117
13	Sicurezza del sistema	119
13.1	Canali di comunicazione	120
13.2	Strumenti d'interazione con il sistema	121
13.3	Infrastrutture	123
IV	Conclusioni	125
14	Strumenti e competenze	127
14.1	Definizione dei requisiti	128
14.1.1	Definizione dei punti da sottoporre a controllo	129
14.1.2	Definizione funzionale	130
14.1.3	Definizione delle modalità di trasmissione dati	130
14.1.4	Definizione delle informazioni da archiviare	131
14.1.5	Definizione delle criticità	132
14.1.6	Definizione dell'interoperabilità con sistemi esterni	132
14.2	Fase di definizione dell'architettura	133
14.3	Fase di verifica	136

14.4 Fase di installazione	139
14.5 Fase di messa in servizio	141
14.6 Fase di esercizio e manutenzione	143
15 Evoluzione dei sistemi SCADA	145
15.1 Controllo di processo e sistemi informativi aziendali	146
15.2 Dai sistemi ai servizi SCADA	150
Glossario	154
Bibliografia	156
V Appendici	157
A GNU Free Documentation License	159
1. APPLICABILITY AND DEFINITIONS	160
2. VERBATIM COPYING	161
3. COPYING IN QUANTITY	162
4. MODIFICATIONS	162
5. COMBINING DOCUMENTS	165
6. COLLECTIONS OF DOCUMENTS	165
7. AGGREGATION WITH INDEPENDENT WORKS	165
8. TRANSLATION	166
9. TERMINATION	166
10. FUTURE REVISIONS OF THIS LICENSE	166
ADDENDUM: How to use this License for your documents	167

Parte I
Generalità

Capitolo 1

Cos'è un sistema SCADA

Argomentazioni sull'utilità, più spesso sulla necessità, dell'adozione di sistemi SCADA possono essere prodotte analizzando casi esemplari di applicazione di sistemi di questo genere per la risoluzione dei problemi di supervisione e controllo. Gli esempi provengono da ambienti produttivi caratterizzati da elementi tecnologici e organizzativi tra loro molto diversi ma che consentono di condurre un'analisi destinata a delineare gli aspetti che qualificano un sistema come SCADA.

Prima di procedere può essere utile dare una prima, generica, definizione di sistema SCADA, magari partendo dal significato dell'acronimo. SCADA sta per *Supervisory Control And Data Acquisition* (acquisizione dati, supervisione e controllo) e sintetizza le tre funzioni fondamentali svolte da questo genere di sistema. In uno SCADA l'acquisizione dati è funzionale allo svolgimento delle funzioni di supervisione, osservazione dell'evoluzione del processo controllato, e di controllo, attuazione di azioni volte alla gestione degli stati nei quali il processo controllato si trova e delle transizioni tra gli stati nei quali il processo può venire a trovarsi.

Quanto finora detto, molto poco per la verità, non si limita a qualificare i sistemi SCADA ma caratterizza un insieme molto ampio di sistemi di controllo che differiscono tra loro per elementi quali la distribuzione geografica del sistema, la distribuzione (o la centralizzazione) dell'intelligenza del controllo, il grado di interazione tra operatore umano e sistema, i tempi di reazione a un evento prodotto dal processo controllato e molti altri fattori. Per questo motivo vengono presentati alcuni esempi di applicazioni che possono essere considerati rappresentativi del tema trattato.

Un largo uso di sistemi di supervisione e controllo è fatto nell'ambito del controllo del traffico (aereo, ferroviario, automobilistico), della gestione dei sistemi di trasporto dei fluidi (acquedotti, gasdotti, oleodotti, ...), della distribuzione dell'energia (reti di trasmissione dell'energia elettrica), della

gestione delle linee di produzione che realizzano i processi industriali, del telerilevamento ambientale. Nel seguito sono presentati i casi di applicazione al settore dei trasporti ferroviari, con l'esempio del sistema di controllo del traffico interno a uno scalo, al trattamento delle acque, con l'esempio del sistema di gestione di un depuratore di liquami e acque reflue, al telerilevamento ambientale, con l'esempio di un tipico sistema di centraline di rilevamento della qualità dell'aria.

1.1 Gestione di un depuratore di liquami e acque reflue

Sin dalla sua comparsa sulla Terra, l'uomo ha avuto l'esigenza di unirsi con i suoi simili e formare dei nuclei sociali per mezzo dei quali ha tentato di migliorare le proprie condizioni di vita. In una prima fase si poteva parlare di semplici aggregazioni, poi di villaggi e poi, con il passare del tempo, questi villaggi sono andati via via aumentando di dimensioni fino a costituire i paesi, le nostre moderne città e perfino le metropoli. La convivenza di più persone nello stesso luogo fa nascere l'esigenza di mantenere il luogo di residenza nel miglior stato possibile in modo che la salubrità dello stesso non vada a perdersi con il tempo. Uno dei problemi che per primi si sono presentati agli abitanti dei villaggi è stato sicuramente lo smaltimento delle acque piovane e dei liquami prodotti. Senza voler trattare l'evoluzione che ha portato alla moderna gestione delle acque, si è voluto sottolineare quanto sia importante il problema di gestione delle stesse e di seguito sarà illustrato quanto un sistema di controllo possa essere di aiuto nel migliorare e semplificare la realizzazione delle modalità con cui questa gestione si ottiene. Un depuratore destinato al trattamento delle acque si compone sostanzialmente di tre elementi:

- la parte di raccolta delle acque che è distribuita nel territorio
- il depuratore vero e proprio che costituisce la parte centrale del sistema di depurazione
- la parte di immissione delle acque (depurate) nelle normali vie di smaltimento, fiumi o mare

La parte di raccolta delle acque costituisce la parte più articolata del sistema di depurazione. Tutti i punti nei quali si producono emissioni di liquami e tutti quelli nei quali si raccolgono le acque piovane devono essere individuati e, a partire da questi, i liquami debbono essere canalizzati per mezzo di apposite fognature o fossi di raccolta delle acque. Tutta questa rete di raccolta

delle acque permette di evitare il rilascio diretto nell'ambiente delle acque da trattare ed il loro invio al depuratore centrale. Spesso la rete fognaria o i fossi sono realizzati in modo tale che le acque provvedano naturalmente (per caduta) a fluire verso il depuratore. In altre occasioni è necessario realizzare delle stazioni di pompaggio che provvedano a far superare alle acque i dislivelli che le separano dal punto d'ingresso del depuratore. Tutta la rete di raccolta delle acque e le eventuali stazioni di pompaggio possono essere dotate di organi quali valvole, pompe, strumenti di misura, ecc.

Analogamente a quanto avviene nella rete fognaria, l'acqua in uscita dal depuratore può essere immessa nelle normali vie di smaltimento, fiumi, laghi o direttamente nel mare, per mezzo di una rete di collegamento tra queste ultime e il depuratore. A volte il depuratore ha la possibilità di produrre acqua depurata per gli usi industriali che viene distribuita alle aziende che la possono utilizzare in vece dell'acqua potabile per un utilizzo industriale (ad esempio per i sistemi di raffreddamento). La distribuzione di acqua per uso industriale presenta le stesse problematiche di una rete di distribuzione dell'acqua potabile e prevede l'allestimento di organi di manovra quali valvole, pompe, paratoie e strumenti di misura per la contabilizzazione. Questo sistema di canalizzazioni e organi che provvede a gestire i prodotti in uscita da un depuratore ha le stesse caratteristiche, per quel che riguarda l'automazione, della rete di raccolta delle acque. Questi due componenti del depuratore possono essere classificati con la definizione di impianti periferici. Le analogie che caratterizzano le modalità con le quali vengono gestiti rendono simili le tecniche con le quali un sistema SCADA sarà impiegato per il loro controllo. Per questo motivo nel seguito della trattazione le problematiche di queste due componenti sono analizzate all'interno della stessa categoria che riguarda l'automazione e il controllo degli impianti periferici.

Essendo gli impianti periferici distribuiti sul territorio con possibilità di estendersi fino a raggiungere dimensioni ragguardevoli (non è insolito che un depuratore raccolga oltre alle acque di una città, anche quelle di tutta la zona circostante), è opportuno avere dei mezzi per il controllo di tutti gli organi che li compongono. Se in un primo momento è stato l'uomo a farsi carico di ispezionare e controllare manualmente gli organi, attualmente questa funzione è svolta da apparati di acquisizione dati. I dati acquisiti possono essere immagazzinati dagli stessi in un'area dati locale ed essere trasmessi a un centro remoto di controllo in un secondo momento (su richiesta del centro o su base periodica), oppure possono essere costantemente trasmessi al centro avendo a disposizione un collegamento stabile tra gli apparati periferici e il centro. La particolare distribuzione geografica con cui normalmente ci

si confronta privilegia la prima delle due soluzioni anche in relazione al tipo di fenomeno che si vuole tenere sotto controllo, il quale non ha bisogno di tempi di reazione particolarmente bassi. In alcuni casi possono essere adottate centraline di acquisizione dati in grado di avere a bordo logiche di controllo con le quali provvedono autonomamente e automaticamente a comandare gli organi. Queste logiche possono essere preconfigurate al momento dell'installazione, oppure programmate di volta in volta (con intervento manuale dal centro remoto di controllo) consentendo di realizzare un certo grado di flessibilità nella gestione degli organi anche in risposta a situazioni che mutano nel tempo. Altra caratteristica degli apparati di acquisizione dati è la possibilità di inviare in modo spontaneo allarmi al centro remoto di controllo con l'obiettivo di informare riguardo a particolari situazioni di esercizio, quali carichi di lavoro anomali o eventuali malfunzionamenti degli organi.

Il depuratore che raccoglie tutte le acque provenienti dalla rete fognaria realizza la vera funzione di depurazione. Questa può essere semplicemente un'operazione di clorazione delle acque, una decantazione oppure un più complesso sistema composto da vari stadi di sedimentazione, filtrazione, ossidazione, accumulo dei fanghi con produzione di biogas, recupero di acqua per utilizzo industriale, formazione di fanghi inerti da inviare in discarica. Il ciclo completo di depurazione può comprendere anche la produzione di energia elettrica ricavata sfruttando il biogas prodotto dalla digestione anaerobica dei fanghi ad opera di particolari batteri e quindi l'immissione di questa energia elettrica nella rete di distribuzione oppure il riutilizzo all'interno del depuratore per la sua parziale alimentazione. Tutto il depuratore è costellato di organi preposti alla sua conduzione quali valvole, paratoie, pompe di vario tipo, nastri, motori in genere, strumenti di misura, ecc. Ogni organo o strumento di misura può essere gestito manualmente da un addetto, ma in un moderno complesso di depurazione questa funzione è svolta da un sistema di controllo (SCADA). Il sistema di controllo sarà composto da una serie di apparati di acquisizione dati disposti in prossimità dei vari organi e strumenti oppure in punti di aggregazione dei segnali (normalmente a questo scopo si utilizzano le stesse cabine elettriche in cui si trovano i quadri elettrici di comando degli organi). Questi apparati provvedono alla concentrazione di tutte le informazioni provenienti dall'impianto e all'invio delle stesse al centro di controllo. Il centro di controllo normalmente risiede in un'area appositamente predisposta all'interno del depuratore. In casi particolari, ad esempio piccoli depuratori che non prevedono il presidio, esso può essere sito presso gli uffici dell'ente di gestione che sono dislocati in posizione remota rispetto al depuratore. Analogamente agli apparati di acquisizione dati visti

per la parte relativa agli impianti periferici gli apparati utilizzati all'interno del depuratore possono essere dotati di logiche di automazione che governano la gestione dei singoli organi. Diversamente dagli apparati di acquisizione già visti, gli apparati presenti nel depuratore solitamente comunicano con continuità con il centro di controllo. Questo è dovuto principalmente a:

- la vicinanza tra centro di controllo e apparati di acquisizione dati consente la realizzazione di infrastrutture di comunicazione dati in grado di permettere una comunicazione caratterizzata da grandi quantità di dati, elevate velocità, bassi costi, continuità
- le logiche di automazione residenti negli apparati periferici provvedono alla corretta gestione degli organi, mentre per ottimizzare il funzionamento dell'intero complesso è necessario un centro gerarchicamente sovraordinato in grado di coordinare le diverse parti in funzione delle condizioni di esercizio
- i processi controllati hanno bisogno di essere tenuti costantemente sotto controllo e un sistema centralizzato può realizzare questa funzione solamente se continuamente informato dello stato di ogni singola parte di impianto

La concentrazione presso un unico centro di controllo di tutte le informazioni disponibili in impianto permette di effettuare una corretta gestione del depuratore. Di solito tutte le informazioni vengono collezionate da sistemi di acquisizione dati che sono in colloquio con gli apparati periferici (agli stessi sistemi faranno capo anche gli apparati della rete fognaria e della rete di emissione nell'ambiente delle acque trattate). Questi sistemi rendono disponibili tutti i dati acquisiti a ulteriori livelli di controllo che realizzano, a grandi linee, le seguenti funzioni:

- visualizzazione dei valori acquisiti per gli operatori responsabili dell'esercizio del depuratore
- fornitura dei dati primari di impianto alle logiche automatiche di gestione del depuratore per metterle in condizione di svolgere le elaborazioni finalizzate a realizzare il primo livello decisionale di sistema
- archiviazione dei dati per una loro analisi successiva (statistiche di funzionamento, operazioni di manutenzione programmata, dati aggregati da fornire agli enti preposti al controllo, dati per gli organi di contabilizzazione, ecc.)

Per la funzione di visualizzazione la realizzazione del sistema di controllo con sistemi informatici non esclude la possibilità di continuare a utilizzare strumenti quali il *quadro sinottico*, soprattutto in virtù dell'immediatezza di restituzione dell'informazione. Più moderni sistemi prevedono la sostituzione del quadro sinottico con monitor di computer ai quali si possono affiancare sistemi tipo *video wall* (schermi giganti utilizzati per la proiezione delle informazioni su un'intera parete della sala controllo). Anche il *banco di controllo* viene spesso affiancato o sostituito con i monitor dei computer. La sostituzione di questi strumenti che per anni hanno fatto la storia delle sale controllo (quante volte nei film si vedono primi piani su pareti intere coperte da disegni e luci e banchi sterminati colmi di luci, interruttori, manopole, ecc.) è dovuta sia alla necessaria diminuzione dei costi (un monitor di computer permette di sostituire un intero quadro sinottico) sia all'incremento della quantità di informazioni che gli operatori sono chiamati a gestire. Inoltre l'adozione di sistemi che sono riconfigurabili in modo semplice permette di avere una flessibilità nella rappresentazione degli impianti che può variare nel tempo a costi inferiori rispetto a quelli che caratterizzano quadri realizzati con componenti meccaniche o elettromeccaniche. Altri elementi fondamentali per la comprensione dell'importanza dell'introduzione di sistemi informatici nella gestione delle strutture di depurazione sono la disponibilità dei dati (acquisizione e archiviazione), che permette di effettuare operazioni prima impossibili o eccessivamente onerose, e la riduzione degli errori che la gestione manuale tende ad introdurre (sia nella realizzazione delle operazioni tese all'esercizio degli impianti, sia nella reazione a eventi inattesi). Inoltre le capacità di elaborazione dei sistemi attualmente disponibili consentono reazioni estremamente rapide.

Quanto detto della struttura di un depuratore, che prevede impianti periferici per la raccolta delle acque e per la restituzione di quelle trattate e un centro di depurazione vera e propria, mostra l'affinità che questa ha con l'architettura tipica di un sistema SCADA che prevede un centro di controllo al quale arrivano tutte le informazioni ed è in grado di prendere decisioni, e apparati periferici di acquisizione dati in grado di ricevere le informazioni dagli organi e dal processo, inviarle al centro di controllo ed eseguire i comandi che quest'ultimo impartisce.

1.2 Gestione del traffico ferroviario

Uno scalo ferroviario può essere descritto, in generale, come un sistema di gestione del flusso dei convogli dotato di un insieme di linee di ingresso, un

insieme di linee di uscita e un terzo insieme di linee interne allo scalo. La gestione del traffico consiste nell'associazione di una linea d'ingresso e una linea di uscita alla stessa linea interna in modo da generare continuità tra ingresso e uscita e, di conseguenza, permettere a un convoglio proveniente dalla linea d'ingresso di procedere (dopo aver effettuato la fermata per *servizio viaggiatori*) verso la meta raggiungibile dalla linea d'uscita.

Per anni la gestione è stata condotta per mezzo di operatori che, in base alle indicazioni dei responsabili del traffico, provvedevano al corretto posizionamento degli *scambi ferroviari*, cioè dei sistemi di deviazione che permettono l'associazione di una linea interna a una tra le due linee d'ingresso o d'uscita adiacenti. Con questa pratica venivano poste le basi per il movimento dei convogli, basi sulle quali è stato costruito un sistema di segnalazioni gestuali per la trasmissione del comando di partenza e di fermata.

Una prima evoluzione di questo sistema è stata l'introduzione dei semafori di segnalazione delle autorizzazioni relative al movimento. Il responsabile del traffico si è trovato così a poter demandare al semaforo tutte le funzioni di segnalazione relative al movimento. Allo stesso tempo è stato necessario rendere disponibile al personale addetto al traffico un sistema di gestione delle segnalazioni, banalmente un quadro elettrico con gli interruttori dei segnali luminosi.

Il secondo elemento di sviluppo degli scali ferroviari è stata l'introduzione dei sistemi semiautomatici di gestione del traffico i quali possono essere considerati a pieno titolo sistemi SCADA. L'evoluzione tecnologica ha consentito di realizzare scambi ferroviari dotati di sistemi elettromeccanici che permettono il controllo della posizione per mezzo di segnali elettrici impartiti a distanza. Controllo della posizione ovvero comando di assunzione di una tra le posizioni consentite e segnalazione della posizione raggiunta al sistema che ha impartito il comando. Sulla base del funzionamento di questi apparati è stato possibile pensare a un sistema che raccogliesse le informazioni relative alla posizione di ogni scambio ferroviario presente nello scalo e allo stato di segnalazione di ogni semaforo.

I sistemi che sono stati realizzati sono SCADA che agiscono per mezzo delle tre funzionalità fondamentali:

- **acquisizione dati:** acquisizione degli stati relativi agli scambi ferroviari (posizioni) e al sistema di semafori (segnalazioni)
- **supervisione:** visualizzazione dello stato di esercizio dello scalo basata sui dati acquisiti

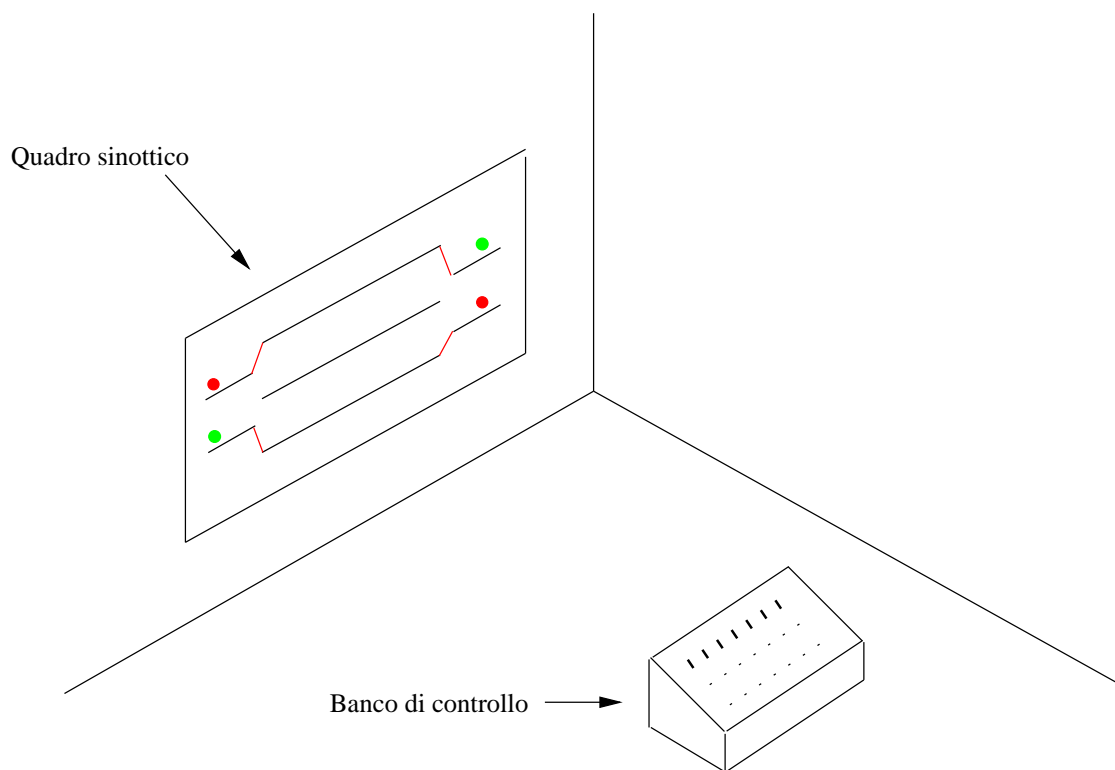


Figura 1.1: Sistema di controllo del traffico ferroviario

- **controllo:** gestione centralizzata della posizione degli scambi ferroviari e delle segnalazioni del sistema di semafori

Grazie a questi sistemi i responsabili del traffico ferroviario dispongono di una rappresentazione schematica completa dello scalo nella quale vengono riportati i percorsi attivi praticabili e lo stato d'uso degli stessi. Gli stessi sistemi sono corredati da dispositivi che permettono di impartire comandi agli apparati di deviazione e segnalazioni ai convogli.

In figura 1.1 è riportata una rappresentazione schematica di un sistema di controllo del traffico ferroviario. In particolare sono rappresentate le due componenti fondamentali per l'interazione tra operatori umani e sistema: il quadro sinottico e il banco di controllo. Il quadro sinottico contiene una rappresentazione topologica dello scalo animata da un meccanismo di retroilluminazione che consente di avere informazioni relative alle posizioni degli scambi ferroviari e agli stati delle segnalazioni luminose, cioè fornisce una rappresentazione dello stato di esercizio dello scalo. Il banco di controllo è dotato di pulsanti e leve che permettono di inviare segnali elettrici ai sistemi di manovra e di segnalazione, cioè di comandare la variazione di po-

sizione agli scambi ferroviari e il cambiamento della segnalazione al sistema di semafori.

Il quadro sinottico e il banco di controllo realizzano le funzioni di supervisione e controllo del sistema e svolgono tali funzioni sfruttando un'altra porzione di sistema (non riportata in figura) dedicata all'acquisizione dati. È opportuno precisare che a questo livello di trattazione per acquisizione dati si intende l'intero sistema di scambio delle informazioni: comandi diretti ai sistemi di segnalazione e manovra, informazioni di stato dirette al sistema di controllo per la rappresentazione sul quadro sinottico.

Lo sviluppo tecnologico dei sistemi di calcolo ha consentito ai sistemi di gestione del traffico ferroviario di affrontare una seconda fase evolutiva. In particolare è stato possibile introdurre procedure di elaborazione delle informazioni di stato dello scalo finalizzate alla verifica della congruenza tra posizioni degli organi di manovra e segnalazioni luminose impartite ai convogli, alla gestione di stati di esercizio anomali quali guasti e interruzioni del servizio per manutenzione, alla verifica della presenza di convogli nei tronchi di linea gestiti dal sistema. Continuando a far riferimento alla figura 1.1 è possibile dire che:

- la complessità del quadro sinottico è cresciuta per consentire la rappresentazione delle nuove informazioni
- il banco di controllo si è arricchito dei comandi di gestione dei nuovi stati previsti dal sistema
- il sistema di acquisizione dati è stato perfezionato per permettere lo scambio delle nuove informazioni gestite dal sistema
- l'intero sistema si è arricchito di calcolatori dedicati all'elaborazione delle informazioni di stato dello scalo

Gli stadi di sviluppo dei reali sistemi di gestione del traffico ferroviario sono stati caratterizzati dall'introduzione di meccanismi automatici per la gestione delle barriere dei passaggi a livello adiacenti agli scali, la segnalazione agli scali adiacenti della posizione dei convogli e dell'entità di eventuali ritardi, la configurazione automatica della topologia attiva in funzione dell'orario di esercizio. La complessità degli attuali sistemi dipende dall'insieme di funzioni che essi possono svolgere mentre la struttura che li caratterizza è in gran parte simile a quella dei primi prototipi realizzati.

1.3 Telerilevamento ambientale terrestre

Lo studio di fenomeni fisici, chimici, geologici, biologici ha condotto a un livello di conoscenza del sistema *Terra* che ancora non consente non solo di prevedere ma neppure di dare risposte certe ai fenomeni geofisici che caratterizzano il pianeta. Il tema riveste un'importanza particolare poiché alla naturale ricerca di conoscenza si sovrappone il dubbio che ci possano essere fenomeni che vengono generati, o più semplicemente amplificati, dall'attività dell'uomo. Tra i molti strumenti utilizzati per l'indagine dei fenomeni geofisici un ruolo importante è svolto da quelli classificabili nell'ambito del *telerilevamento ambientale terrestre*. Per mezzo di questi strumenti è possibile fare analisi meteorologiche, di inquinamento ambientale, delle cause di particolari calamità naturali.

Un elemento fondamentale dell'indagine dei fenomeni ambientali è l'insieme di dati sul quale viene condotta l'analisi e in particolare sono determinanti caratteristiche quali la qualità, la quantità, la disponibilità di serie significative di dati grezzi. I dati ambientali rappresentano misurazioni di grandezze termodinamiche, della composizione chimica e di caratteristiche fisiche realizzate in un contesto spaziale e temporale considerato significativo ai fini dello studio. Il telerilevamento ha contribuito allo sviluppo dello studio dell'ambiente dotando gli studiosi di strumenti automatici in grado di realizzare campagne di misurazione caratterizzate dall'acquisizione di grandi quantità di dati opportunamente referenziati in termini sia spaziali che temporali, strumenti corredati di sistemi di comunicazione, raccolta dati, elaborazione. Il lavoro degli scienziati viene ricondotto alla definizione delle regole di campionamento, alla scelta dei punti di osservazione e delle grandezze da osservare, alla elaborazione di procedure analitiche da applicare alle informazioni acquisite e all'analisi delle informazioni aggregate, cioè alle fasi "intellettuali" dello studio.

Le funzioni che rendono i sistemi di telerilevamento classificabili nell'ambito dei sistemi di supervisione sono l'acquisizione, l'archiviazione, l'elaborazione dei dati grezzi e la gestione delle informazioni aggregate frutto dell'analisi dei dati. Queste funzioni vengono svolte per mezzo di strutture tecnologiche comprendenti:

1. sistemi di acquisizione dotati di strumenti di misura, dispositivi di immagazzinamento dei dati, sistemi di comunicazione responsabili del trasferimento dei dati ai sistemi di elaborazione
2. sistemi di elaborazione dotati di capacità di calcolo, di archiviazione, di rappresentazione dei dati

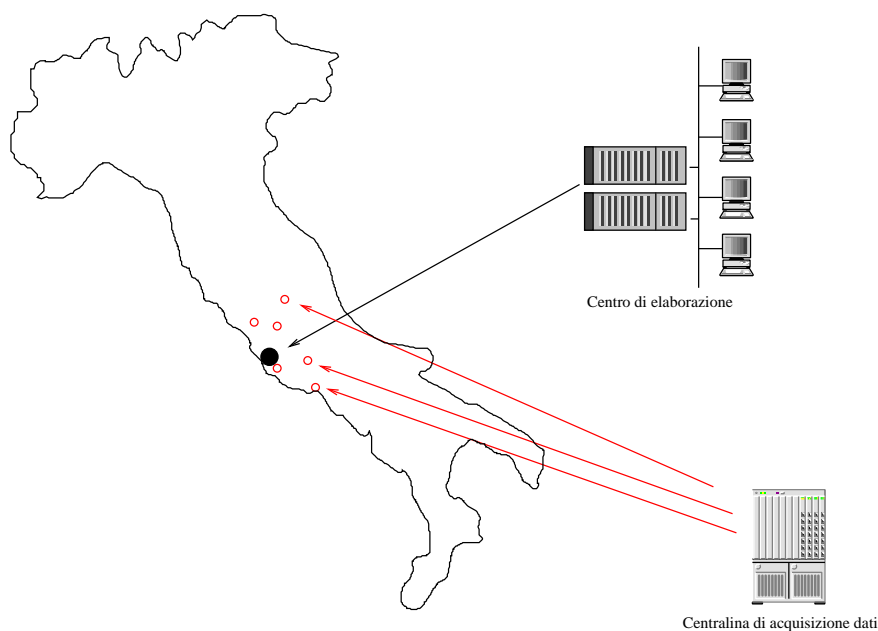


Figura 1.2: Sistema di telerilevamento ambientale

La rappresentazione schematica della struttura di un generico sistema di telerilevamento ambientale è riportata in figura 1.2.

Le centraline di acquisizione dati sono strutture allestite sul territorio e dispongono di strumenti di misura elettronici per l'acquisizione di dati che vengono riversati, secondo modelli di codifica prestabiliti, su supporti di archiviazione temporanea presenti nelle centraline stesse. Per quanto concerne la gestione di queste apparecchiature periferiche l'intervento umano consiste nella verifica periodica della correttezza della taratura degli strumenti e nella sostituzione dei componenti deperibili. Le centraline forniscono dati con una varietà e una continuità impensabili senza il livello di automazione e la complessità strutturale che le caratterizzano.

A un sistema di apparecchiature di acquisizione complesso corrisponde un sistema centrale di elaborazione che preleva periodicamente i dati temporaneamente archiviati nelle centraline, li rende disponibili ai processi di elaborazione (sia automatici che manuali), li deposita nei supporti di archiviazione permanente, realizza elaborazioni e produce informazioni aggregate fruibili per mezzo di strumenti specializzati nella gestione e nella rappresentazione di informazioni qualificate sia dal punto di vista chimico-fisico che spazio-temporale.

Esempi di prodotti dei sistemi di telerilevamento ambientale sono le carte di distribuzione di sostanze inquinanti nell'atmosfera, delle temperature, delle caratteristiche idrogeologiche dei bacini idrici, delle precipitazioni, del-

la distribuzione di elementi radioattivi e di molti altri elementi caratteristici dell'atmosfera. Alle analisi dei singoli fattori si aggiunge la possibilità di mettere in relazione elementi d'indagine distinti per analisi incrociate più o meno complesse e significative. Che si tratti di fotografie dello stato attuale della porzione di ambiente posta sotto osservazione o dell'analisi delle serie storiche prodotte da lunghi periodi di esercizio del sistema di rilevamento, è evidente che il prodotto è frutto di un processo analitico nel quale la funzione del sistema si limita alla realizzazione di campagne di monitoraggio, al primo trattamento dei dati acquisiti e alla fornitura dei dati per mezzo di strumenti evoluti di gestione dei dati.

Capitolo 2

SCADA: definizioni

La definizione comunemente utilizzata per l'identificazione di sistemi SCADA corrisponde al significato esteso dell'acronimo e rappresenta senza dubbio il mezzo più semplice per introdurre il modello rappresentato da questo tipo di sistemi. L'acronimo SCADA sta per *Supervisory Control And Data Acquisition* ed è nient'altro che l'enumerazione delle tre funzionalità principali realizzate dai sistemi di supervisione e controllo: supervisione, controllo e acquisizione dati. In realtà la versione estesa dell'acronimo SCADA non è una definizione poiché in nessun modo permette di discriminare quelli che effettivamente vengono considerati sistemi SCADA da una gran quantità di sistemi o semplicemente di dispositivi più o meno complessi che svolgono le tre funzioni o parte di esse. Ciò che manca all'acronimo per essere una definizione compiuta è la descrizione del modo in cui questo tipo di sistema espleta le proprie funzioni e il campo di applicazione. Utilizzando il linguaggio della matematica possiamo dire che i sistemi SCADA sono insiemi di funzioni dei quali si usa dare una definizione enumerando le funzioni dell'insieme senza che queste siano qualificate in termini di dominio e codominio (determinati dalle caratteristiche del campo di applicazione) e in termini di proprietà delle funzioni. È come se la trigonometria potesse essere definita come *Seno Coseno Tangente e Cotangente* senza la definizione delle caratteristiche di continuità, periodicità e quant'altro necessario a giustificare l'esistenza stessa del termine "trigonometria" e del metodo di calcolo che questa rappresenta. Così come in matematica lo studio di un insieme di funzioni come "caso particolare" serve a estendere la comprensione del problema ma non la conoscenza nel caso dei sistemi di controllo la distinzione tra sistemi SCADA e altri sistemi affini serve a comprendere meglio il ruolo che è stato attribuito loro dall'applicazione che hanno avuto per la risoluzione di problemi di controllo.

Le sezioni che seguono contengono una descrizione delle funzioni svol-

te da un sistema SCADA e le differenze che possono essere individuate nel confronto tra questo tipo di sistemi e un altro tipo, affine al primo, anch'esso destinato a realizzare funzioni di controllo e comunemente indicato con l'acronimo DCS (*Distributed Control System*).

2.1 Acquisizione dati

L'acquisizione dati è una funzione che nella maggior parte dei casi ha un ruolo di supporto alle funzioni di supervisione e controllo poiché mette in relazione il sistema con il processo controllato consentendo la conoscenza dello stato in cui si trova il processo e l'azione di controllo esercitata per mezzo della variazione di parametri caratteristici del processo. In questo senso "acquisizione dati" significa in realtà scambio dati in entrambe le direzioni: dal processo verso il sistema e viceversa. In alcuni sistemi classificati come sistemi SCADA l'acquisizione è la funzione principale svolta dal sistema; questo è il caso in cui non ci sono procedure di controllo implementate dal sistema e la fase di supervisione può essere realizzata sporadicamente o come analisi a posteriori degli stati acquisiti dal processo. Esempio di questo tipo di casi è un qualsiasi sistema di telerilevamento nel quale l'obiettivo primo è la raccolta e l'organizzazione dei dati sui quali possono essere condotte analisi non necessariamente predefinite.

L'acquisizione dati entra nella definizione di sistema SCADA per il fatto che non è possibile espletare funzioni di supervisione senza acquisire informazioni sullo stato in cui si trova il processo osservato così come non è possibile orientarne il comportamento, cioè controllarlo, senza avere la possibilità di influenzare lo stato cambiando il valore di parametri che lo caratterizzano.

La funzione di acquisizione dati di un sistema SCADA è considerata generalmente una funzione di scambio puro e semplice di informazioni tra la parte di sistema che realizza supervisione e controllo e processo controllato, cioè si considera assente qualsiasi processo decisionale interposto tra le strutture di supervisione e controllo e il processo controllato. Nei casi in cui questa condizione viene a mancare si ha a che fare con sistemi che realizzano qualcosa di diverso rispetto a quanto viene fatto da un sistema SCADA inteso in senso classico, si hanno cioè strutture a intelligenza distribuita. Uno dei motivi per il quali esiste questa distinzione consiste nel fatto che la distribuzione della capacità di elaborazione si rende necessaria solitamente nei casi in cui il processo controllato ha dimensioni geograficamente rilevanti, tali da ostacolare la realizzazione di un sistema di elaborazione concentrato e collocato a ridosso del processo.

2.2 Supervisione

La supervisione è la funzione per mezzo della quale un sistema SCADA rende possibile l'osservazione dello stato e dell'evoluzione degli stati di un processo controllato. A questa funzione appartengono tutte le funzionalità di visualizzazione delle informazioni relative allo stato attuale del processo, di gestione delle informazioni storiche, di gestione degli stati che costituiscono eccezioni rispetto alla normale evoluzione del processo controllato. La funzione di supervisione costituisce un fine per qualsiasi sistema SCADA. Questa funzione è determinante nella caratterizzazione di un sistema nel senso che un sistema che non permetta di accedere alle informazioni di stato corrente e/o storiche del processo osservato e/o controllato non può essere definito come sistema SCADA.

2.3 Controllo

La funzione di controllo rappresenta la capacità di un sistema di prendere decisioni relative all'evoluzione dello stato del processo controllato in funzione dell'evoluzione del processo medesimo. La modalità con la quale le procedure di controllo vengono realizzate nell'ambito dell'intera architettura del sistema dipende fortemente dal tipo di processo, essendo questo in grado imporre scelte architetture sia hardware che software. In questo senso i sistemi SCADA sono comunemente intesi come sistemi che hanno nella funzione di acquisizione dati l'intera catena di acquisizione che dai sensori al sistema di elaborazione e archiviazione veicola informazioni che sono i dati grezzi prelevati come valori di parametri di stato del processo. Le funzionalità di controllo sono quindi concentrate nel sistema di elaborazione il quale, una volta eseguite opportune procedure di elaborazione, sfrutta il sistema di acquisizione dati in senso inverso per cambiare il valore di opportuni parametri di stato del processo controllato.

2.4 SCADA vs DCS

La distinzione tra SCADA e DCS è basata sul grado di distribuzione dell'intelligenza del sistema. Il sistema SCADA è stato sempre considerato come sistema con funzioni di controllo concentrate nel sottosistema di elaborazione e fisicamente e tecnologicamente distinte dalle funzioni di acquisizione. I sistemi DCS sono caratterizzati da strutture di acquisizione dotate di elevata

capacità di elaborazione che hanno condotto alla realizzazione di funzioni di acquisizione e controllo fisicamente e tecnologicamente contigue.

Nel caso dei sistemi DCS non è possibile parlare di apparecchiature di acquisizione (come invece si fa per i sistemi SCADA) poiché consistono in veri e propri sistemi di elaborazione più o meno complessi in grado di interpretare i dati provenienti dall'osservazione del processo, valutarne le caratteristiche e prendere decisioni orientate al controllo dello stato. In questo contesto un eventuale centro di supervisione di un sistema DCS acquisisce informazioni che sono dati grezzi rappresentativi dello stato in cui si trova il processo ma anche informazioni aggregate relative allo stato di esercizio delle strutture di controllo.

L'osservazione degli orientamenti assunti dall'evoluzione delle tecnologie coinvolte nello sviluppo dei sistemi di controllo induce una riflessione sulla necessità di distinguere i sistemi SCADA dai sistemi DCS: la distinzione è stata prodotta dalle caratteristiche tecnologiche e dalle scelte realizzative divenute dominanti nell'ambito dei singoli problemi di controllo poiché obbligate o fortemente consigliate. Con lo sviluppo delle tecnologie dei sistemi di elaborazione e delle infrastrutture di comunicazione la scelta tra un sistema a controllo centralizzato e acquisizione pura e un sistema a controllo distribuito e apparecchiature di acquisizione complesse diviene sempre più un fatto di opportunità legato a fattori quali la scalabilità, la manutenibilità o altre caratteristiche di progetto diverse dalla realizzabilità del sistema di supervisione e controllo. In questo senso la distinzione tra DCS e SCADA si sta dirigendo verso l'estinzione in termini sia tecnologici che funzionali e si può prevedere che ben presto i due tipi di sistemi saranno inclusi in un'unica categoria.

Capitolo 3

Il processo controllato

Nei capitoli precedenti sono state introdotte le caratteristiche fondamentali di un sistema SCADA per mezzo della presentazione di casi classici di applicazione di questo tipo di sistemi. È stata fornita anche una serie di definizioni comunemente utilizzate per la caratterizzazione dei sistemi di supervisione e controllo. Prima di procedere alla descrizione dettagliata della struttura tipica e delle funzionalità realizzate da uno SCADA è opportuno porre l'attenzione sull'importanza rivestita dall'analisi del processo controllato nella definizione delle caratteristiche architettoniche e funzionali del sistema di controllo. La varietà dei processi controllati da sistemi classificati come sistemi SCADA si manifesta in notevoli differenze tra le diverse realizzazioni e la qualità dello sviluppo di sistemi di controllo è funzione dipendente in ugual misura dalla capacità di realizzazione di sistemi tecnologici e dall'efficacia dell'analisi del processo da controllare. Quest'ultima impone vincoli significativi nella realizzazione di sistemi di controllo rendendo quest'ultimo un processo che di volta in volta richiede tecniche di sviluppo adeguate difficilmente riconducibili a modelli convenzionali. L'analisi del processo controllato produce informazioni che influenzano le scelte progettuali sia dal punto di vista tecnologico che organizzativo ed è norma aurea anteporre l'approfondimento della conoscenza del processo alla definizione delle caratteristiche del sistema destinato a controllarlo. Nel seguito sono presentati alcuni elementi classici di indagine per la determinazione delle caratteristiche fondamentali del sistema di controllo. La qualificazione del processo rispetto a questi elementi permette di individuare vincoli nella definizione delle specifiche tecniche, funzionali, organizzative che nella maggior parte dei casi si traducono negli elementi distintivi del sistema realizzato rispetto a tutti gli altri.

3.1 Realtime

Il termine *realtime* si riferisce alla capacità del sistema di reagire alle sollecitazioni del processo con ritardi trascurabili rispetto alla dinamica evolutiva del processo medesimo. Allo stesso tempo la reazione del sistema deve essere caratterizzata da tempi di elaborazione compatibili con quelli imposti dagli obiettivi del controllo. Le funzioni svolte da un sistema di controllo sono tali da rendere questa capacità di reazione un requisito solitamente irrinunciabile mentre altri elementi di complessità del sistema e del processo controllato sono in contrasto con questo requisito.

Le soluzioni possono contemplare il contenimento dei tempi di reazione per insiemi ridotti di eventi generati dal processo, il sacrificio di funzioni complesse a favore di soluzioni semplici, l'adozione, quando possibile, di soluzioni tecnologiche dedicate (realizzazioni *ad hoc*) e altri accorgimenti che, come questi, acquisiscono un significato soltanto all'interno del contesto di sviluppo del singolo sistema.

Un primo elemento in contrasto con la caratteristica di un sistema di operare in tempo reale risiede nei limiti imposti dalla tecnologia. L'evoluzione dei sistemi di calcolo è tale da rendere realistico il desiderio di realizzare un sistema *realtime* ma l'idea che questa sia sufficiente a esaudire un desiderio di questo tipo è quantomeno ardita. Molti processi hanno una dinamica che non potrà mai essere superata da quella di un sistema di controllo a meno di una rivoluzione tecnologica (oltre la quale tutte le considerazioni fatte in questo testo sarebbero, o saranno, obsolete) e continueranno a essere "governati" più che "controllati". Limiti tecnologici risiedono, oltre che nella capacità dei sistemi di calcolo, nelle caratteristiche dei sistemi di comunicazione a disposizione dei sistemi di controllo. Questi intervengono quando le dimensioni del processo sono tali da rendere necessario l'allestimento di sistemi di comunicazione complessi e di grandi dimensioni (reti geografiche). L'uso delle migliori tecnologie, del presente e del futuro, non sarà mai in grado di rendere nulli i tempi di trasferimento dell'informazione, tempi che hanno effetti sui ritardi di reazione dell'intero sistema.

Ai limiti imposti dalla tecnologia si aggiungono elementi di complessità introdotti dalle sovrastrutture necessarie a un corretto esercizio del sistema. Tra i molti sono significativi i casi dell'*affidabilità* e della *disponibilità* per l'importanza che questi rivestono nel giudizio di qualità di un sistema di controllo. La capacità di operare correttamente con continuità può essere assicurata per mezzo di processi di elaborazione che in molti casi si sovrappongono a quelli di acquisizione e controllo inficiandone le caratteristiche

dinamiche.

3.2 Alta affidabilità

Una qualità della quale i sistemi di controllo non possono fare a meno è l'affidabilità intesa secondo il significato dato nel gergo tecnologico anglosassone al termine *reliability*. Un sistema di controllo è un mosaico di componenti ognuno dei quali caratterizzato da un determinato, o determinabile, grado di affidabilità, cioè da un valore di probabilità di malfunzionamento espresso come percentuale del tempo di esercizio del componente medesimo. Nella realizzazione di un sistema è necessario tenere in considerazione l'affidabilità dei singoli componenti per provvedere alla eventuale implementazione di contromisure destinate a contenere l'influenza che un dato sottosistema ha sull'affidabilità dell'architettura complessiva.

Per componenti forniti da terze parti è necessario valutare l'affidabilità dichiarata dai produttori e gli strumenti forniti per valutarla o, laddove possibile, migliorarla per mezzo di opportuni accorgimenti. Nella realizzazione *ex-novo* dei componenti è necessario procedere con adeguati strumenti di analisi e sviluppo allo scopo di giungere a implementazioni caratterizzate da gradi di affidabilità soddisfacenti per l'intero sistema.

L'obiettivo ultimo è la realizzazione di sistemi che assicurino il corretto svolgimento delle funzioni per quote del tempo totale di esercizio misurabili. Il raggiungimento del limite del 100% di affidabilità è un vincolo per la maggior parte dei processi controllati ma non per tutti poiché l'evento di malfunzionamento non sempre pregiudica in modo significativo la qualità del servizio offerto dal sistema. Un esempio è dato dai sistemi di telerilevamento ambientale per i quali la perdita di dati relativi a un intervallo di tempo può essere considerato un evento irrilevante se il rapporto tra l'intervallo di tempo e il tempo totale di osservazione è sufficientemente basso.

3.3 Alta disponibilità

La disponibilità è la percentuale di tempo per la quale deve essere assicurato lo stato di esercizio del sistema, cioè il valore complementare della percentuale di tempo in cui il sistema è in stato di fermo a causa di guasti, manutenzioni, aggiornamenti, altro. La disponibilità può essere riferita all'intero sistema o a parti critiche dello stesso e, come le altre, è una caratteristica che si esprime in vincoli che differiscono in funzione del tipo di processo da controllare. Un processo può avere esigenze stringenti di disponibilità per motivi di sicurezza

(si pensi ai sistemi di controllo di processi produttivi tipici dell'industria chimica nei quali l'indisponibilità del sistema di controllo può pregiudicare l'attività del processo di produzione lasciandolo in stati potenzialmente molto pericolosi per la sicurezza delle strutture e l'incolumità degli operatori) o di continuità del servizio (questo è il caso dei sistemi di gestione del traffico). In altri casi la disponibilità è un'esigenza di secondo piano rispetto ad altre caratteristiche anche se i vincoli che essa produce sono comunque stringenti.

3.4 Grado d'interazione uomo-macchina

La realizzazione delle funzioni di un sistema di supervisione e controllo comporta sempre la realizzazione di sottosistemi responsabili dell'interazione tra gli operatori e il sistema medesimo denominati interfacce uomo-macchina (in inglese si usa l'acronimo HMI di *human-machine interface*). La complessità dello sviluppo è funzione del tipo di interazione richiesta mentre quest'ultima dipende dalle caratteristiche del processo controllato. L'interfaccia uomo-macchina può realizzare molti gradi di interazione comprendendo funzionalità di semplice osservazione dello stato di esercizio del sistema, nel caso di sistemi che realizzano procedure completamente automatizzate, o funzionalità responsabili della esecuzione di procedure manuali gestite dagli operatori. In casi analoghi a quello dei sistemi di telerilevamento ambientale le procedure automatiche sono responsabili dell'acquisizione dei dati e di un'eventuale primo trattamento degli stessi (un esempio è dato dalle procedure di validazione) mentre l'interfaccia uomo-macchina rende disponibili funzionalità per tipi di analisi dell'informazione altrimenti non realizzabili. In altri casi, cioè in quelli che prevedono forme di controllo oltre che di supervisione, risulta fondamentale la realizzazione di interfacce di facile utilizzo e di funzionalità accessorie necessarie alla comprensione dello stato di esercizio del sistema comprendenti la gestione della notifica degli allarmi e la visualizzazione di grafici relativi alle grandezze più rappresentative.

Casi molto particolari di interfaccia uomo-macchina sono quelli per i quali non è possibile realizzare quadri sinottici per mezzo degli strumenti software grafici disponibili per i calcolatori elettronici ma l'evoluzione della tecnologia software e la disponibilità di schermi di grandi dimensioni (o, equivalentemente, l'uso di *video wall*) rende questi casi sempre più rari.

3.5 Sistemi di dimensioni geografiche

Le dimensioni geografiche di un sistema SCADA sono definite dalla collocazione delle apparecchiature di acquisizione dati e del sistema di elaborazione. Questi possono trovarsi all'interno di un edificio, essere collocati in un'area limitata a pochi edifici o essere distribuiti su aree territoriali di dimensioni maggiori (aree cittadine, territori regionali, nazionali e internazionali). Le dimensioni geografiche dipendono sia dal processo controllato che dalle esigenze organizzative introdotte dall'uso del sistema di controllo. Se il processo controllato è limitato geograficamente (come può essere una linea di produzione industriale, un sistema di trattamento dell'aria di un edificio o un depuratore) le dimensioni rimangono di solito limitate alla struttura che ospita il processo. Quando il processo controllato ha le caratteristiche di un sistema di trasporto (oleodotti, gasdotti, elettrodotti, ...) la collocazione delle apparecchiature di acquisizione segue la struttura del processo e una eventuale maggiore dimensione dipende dall'organizzazione definita per l'uso del sistema. In questo caso il sistema potrebbe essere utilizzato da un numero più o meno elevato di postazioni che possono trovare posto in luoghi distinti anche molto distanti tra loro.

Queste caratteristiche determinano una complessità maggiore nello sviluppo del sistema a causa delle criticità introdotte sia dalle infrastrutture di comunicazione utilizzate per gli scambi con le apparecchiature periferiche che dalle tecnologie utilizzate dal sottosistema di interfaccia uomo-macchina per l'accesso ai dati. Alle strutture tecnologiche che assicurano lo scambio dati tra i diversi componenti del sistema è richiesta un'elevata affidabilità intesa in termini di continuità e, soprattutto, qualità del servizio. Quest'ultima è uno degli elementi di valutazione dell'affidabilità dell'intero sistema poiché la corruzione dei dati trasferiti dovuta a un sistema di comunicazione inaffidabile pregiudica le elaborazioni compromettendo le funzioni allo svolgimento delle quali il sistema è preposto.

CAPITOLO 3. IL PROCESSO CONTROLLATO

Parte II
Architettura

Capitolo 4

Introduzione

Si è visto in precedenza che la parte periferica di un sistema SCADA è costituita dagli apparati di acquisizione dati. Questi apparati costituiscono gli organi attraverso i quali un sistema SCADA è in grado di relazionarsi con la realtà circostante. Essi sono assimilabili agli organi periferici di un organismo umano e costituiscono per lo SCADA quello che i recettori nervosi sono per l'uomo. Le informazioni collezionate dagli apparati di acquisizione dati sono necessarie al sistema SCADA per poter svolgere il suo compito di controllo. Analogamente a quanto svolto dai cinque sensi per l'uomo, il sistema SCADA ha la capacità di catalogare informazioni provenienti dall'esterno, elaborarle, prendere decisioni ed effettuare opere di controllo sulla realtà circostante per modificarla, governarla, controllarla.

Le terminazioni nervose poste nelle dita di una mano sono in grado di rilevare informazioni dall'ambiente circostante e trasmetterle al cervello, il quale decide il comportamento da tenere in base alla volontà di eseguire un certo compito e alle informazioni pervenute. Si pensi ad esempio alla semplice azione di togliere un oggetto dal fornello della cucina; il cervello comanda il braccio e la mano per prendere l'oggetto, i sensori nervosi posti nelle dita informano il cervello riguardo alla temperatura dell'oggetto ed il cervello decide se proseguire nella sua azione (la temperatura dell'oggetto non è dannosa per le dita) o se invece è conveniente servirsi di un mezzo che impedisca al calore dell'oggetto di procurare danni al corpo.

Anche in questo esempio molto semplice (sono state volutamente trascurate tutte le altre componenti in gioco quali ad esempio i muscoli e le informazioni scambiate con essi) si possono intravedere gli elementi basilari che compongono un sistema SCADA. Il cervello è l'organo centrale al quale arrivano tutte le informazioni; esso è in grado di compiere elaborazioni e prendere decisioni in base al compito che vuole svolgere. Le informazioni costituiscono gli elementi sui quali il cervello lavora per guidare al meglio il

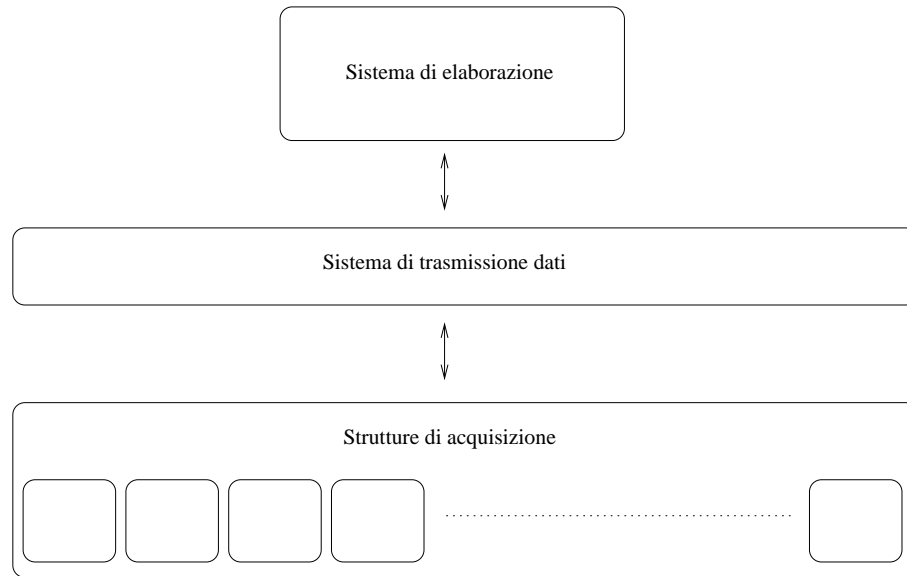


Figura 4.1: Architettura di un sistema SCADA

corpo verso la realizzazione del compito predefinito. I sensori posti in tutto il corpo, anche se in questo caso l'attenzione è stata posta su quelli periferici, costituiscono gli apparati di acquisizione dati in grado di percepire le informazioni dal mondo circostante e trasmetterle al centro di controllo. L'azione che svolgono i sensori consiste nella traduzione dei fenomeni fisici (temperatura, luce, pressione, ecc.) in segnali interpretabili per il cervello. Ultimo componente del sistema è il sistema nervoso, la fitta rete di fibre nervose che collega i sensori con il cervello e che permette la comunicazione tra gli uni e l'altro.

Una rappresentazione dell'architettura di un sistema SCADA, visto come struttura costituita da un sistema di acquisizione, uno di trasmissione e uno di elaborazione delle informazioni è riportata in figura 4.1.

A questa architettura si fa riferimento nello sviluppo della trattazione.

Capitolo 5

Apparati di acquisizione dati

Il presente capitolo tratta il funzionamento degli apparati di acquisizione dati e la qualità dei dati trattati. Nei successivi capitoli l'attenzione è invece incentrata sulla rete di comunicazione e sul sistema centrale di controllo.

5.1 Funzionamento

L'apparato di acquisizione dati costituisce il mezzo attraverso il quale il sistema SCADA è in grado di comunicare con il mondo circostante. Esso ha il compito di tradurre le informazioni prese dalla vita reale in informazioni gestibili da un sistema SCADA e viceversa.

Quando nasce la necessità di scambiare informazioni tra due attori è necessario stabilire un comune linguaggio di comunicazione che permetta lo scambio. In riferimento all'uomo il primo pensiero cade sulla comunicazione orale o, meglio, sulla lingua parlata, anche se questo non è l'unico strumento di comunicazione. Si pensi infatti alle difficoltà che ognuno di noi incontra nel comunicare le cose più semplici a una persona che non parli la nostra stessa lingua: in questi casi ci vengono in soccorso linguaggi non orali molto efficaci quali, ad esempio, la mimica.

Qualunque sia il metodo utilizzato esso si basa su precise regole per le quali un dato suono, gesto, movimento indica una stessa cosa per entrambe le parti. Alla base della comunicazione c'è sempre la definizione della modalità di scambio delle informazioni e la codifica delle stesse in modo da poter comprendere il significato delle informazioni scambiate. Alcune volte è possibile che gli attori della comunicazione non siano in grado di utilizzare un linguaggio comune. In questi casi è necessario ricorrere all'utilizzo di un traduttore (così come avviene tra persone che parlano lingue diverse). Il ruolo del traduttore è estremamente delicato in quanto deve essere svolto in modo

da tradurre le informazioni da un linguaggio a un altro senza introdurre errori che possano compromettere o alterare l'interpretazione delle informazioni.

Il ruolo dell'apparato di acquisizione è analogo a quello del traduttore. Questo viene svolto tanto meglio quanto minore è l'impatto delle elaborazioni su qualità e quantità delle informazioni gestite (come si potrebbe definire un traduttore che ogni cinque parole ne dimenticasse una?). Nel caso dei sistemi SCADA la traduzione consiste nella trasformazione di informazioni relative a grandezze fisiche (quali temperature, pressioni, correnti, tensioni, ...) in informazioni di tipo elettrico opportunamente codificate.

Nell'analogia tra apparato di acquisizione e traduttore umano si può introdurre un altro elemento. Come gli organi sensoriali dell'uomo sono soggetti a limiti fisici (l'apparato uditivo è in grado di operare correttamente all'interno di particolari intervalli di frequenza, d'intensità, ...) oltre i quali essi sono inutilizzabili, quando non soggetti a danneggiamento, così gli apparati di acquisizione hanno caratteristiche costruttive che debbono essere tenute in considerazione in sede di definizione dell'architettura del sistema, pena il malfunzionamento dell'intero sistema SCADA.

5.2 Informazioni gestite

Un apparato di acquisizione dati svolge la funzione di traduzione delle informazioni tra il mondo esterno e il sistema di elaborazione. La tipologia di informazioni che esso gestisce può essere classificata attraverso diversi criteri:

- **direzione delle informazioni:** informazioni che l'apparato riceve o trasmette
- **qualità delle informazioni:** natura delle informazioni
- **caratteristiche elettriche delle informazioni:** le caratteristiche elettriche delle informazioni trattate

Come si vedrà, quelle riportate sono solamente le caratteristiche principali delle informazioni gestite. Per ogni tipologia sarà necessario definire un'ulteriore classificazione delle caratteristiche. Tutte queste classificazioni sono necessarie per poter definire i criteri di scelta di un apparato di acquisizione dati nella realizzazione di un sistema SCADA.

5.2.1 Classificazione in base alla direzione delle informazioni

In relazione alla direzione delle informazioni, un apparato di acquisizione dati è in grado di gestire due tipologie distinte:

- **informazioni in ingresso:** informazioni che l'apparato riceve
- **informazioni in uscita:** informazioni che l'apparato trasmette

Questa classificazione avviene prendendo come riferimento l'apparato di acquisizione dati e non il sistema SCADA. Se infatti si prendesse a riferimento il sistema SCADA si perderebbero di vista le informazioni scambiate tra apparati di acquisizione dati e processo controllato.

Le informazioni in ingresso agli apparati di acquisizione dati sono provenienti dal mondo esterno o dal sistema centrale. Le informazioni in uscita sono quelle dirette al mondo esterno o al sistema centrale. Poiché l'apparato di acquisizione dati svolge principalmente la funzione di conversione, è chiaro che le informazioni in ingresso dal mondo esterno corrispondono molto spesso alle informazioni in uscita per il sistema centrale e quelle in ingresso dal sistema centrale sono spesso tradotte e inviate in uscita verso il mondo esterno.

Spesso, quando si guarda il sistema SCADA nel suo complesso, si utilizza il termine *monitoraggio* per identificare la direzione in ingresso al sistema e il termine *controllo* per indicare la direzione in uscita.

5.2.2 Classificazione in base alla qualità delle informazioni

Le informazioni provenienti dal mondo esterno derivano in massima parte da sensori e trasduttori che sono in grado di *interpretare* un fenomeno fisico e darne una rappresentazione in un diverso sistema di riferimento. L'apparato di acquisizione dati non svolge il compito tipicamente riservato ai sensori, ma è in grado di interagire con questi avendo definito il linguaggio con il quale scambiare informazioni. Analogamente, le informazioni destinate al mondo esterno arrivano a questo per mezzo di attuatori e organi che svolgono la funzione inversa a quella dei sensori: ricevono comandi da parte degli apparati di acquisizione dati e sono in grado di riprodurli in campo sugli organi di manovra. Risulta quindi indispensabile che per ogni informazione scambiata si definisca, oltre alla direzione, la qualità della stessa in modo da poterla trattare correttamente.

Una prima classificazione macroscopica basata sulla qualità dell'informazione è la seguente:

- **informazioni di tipo digitale**
- **informazioni di tipo analogico**
- **informazioni di tipo impulsivo**
- **informazioni di tipo complesso**

Informazioni di tipo digitale

Le informazioni di tipo digitale sono informazioni che riescono a dare una rappresentazione della grandezza attraverso una serie di stati digitali ben identificati e distinti tra loro.

Per fare un esempio di informazione digitale è possibile riferirsi allo stato di funzionamento di un motore. Il motore può assumere solamente due stati di funzionamento: motore fermo o motore in movimento. Questi stati costituiscono gli *stati fisici* del dispositivo e possono essere rappresentati per mezzo di un'informazione di tipo digitale. L'informazione digitale classica è un'informazione che rappresenta solamente due stati di funzionamento distinti, solitamente antitetici tra loro (motore fermo o in marcia, interruttore aperto o chiuso, ecc.). Quest'informazione è facilmente rappresentabile con la presenza o l'assenza di una determinata tensione in ingresso a una *porta* dell'apparato di acquisizione dati. La presenza di tensione viene associata allo *stato logico ON*, l'assenza di tensione viene associata allo *stato logico OFF*. Lo stato logico non è altro che la rappresentazione convenzionale che viene data dell'informazione digitale (in questo caso la più semplice che consta di due soli stati). A ogni stato logico viene associato uno stato fisico del dispositivo controllato. L'associazione dipende dalla modalità di trasduzione dell'informazione primaria. Ritornando all'esempio del motore si potrebbe dire che lo stato logico ON corrisponde allo stato fisico di marcia del motore, mentre lo stato logico OFF corrisponde allo stato fisico di arresto.

Non è raro però avere informazioni digitali che hanno la necessità di rappresentare lo stato fisico di un dispositivo attraverso un insieme più ampio di stati logici. Spesso questo è dovuto alla necessità di introdurre una sorta di controllo di congruenza dell'informazione. Ad esempio si pensi al fatto che lo stato logico OFF corrisponde a una mancanza di tensione sulla porta di ingresso dell'apparato di acquisizione dati. Questa mancanza di tensione non ci fornisce nessuna informazione sullo stato del collegamento fisico con

il dispositivo di trasduzione (un cavo interrotto potrebbe indurre a pensare che il motore di cui sopra sia fermo, mentre in realtà esso è in marcia). È possibile allora introdurre un semplice controllo sullo stato di congruenza dell'informazione utilizzando due porte separate collegate a due informazioni distinte che, prese insieme, forniscano anche uno stato diagnostico. Si consideri un'informazione che indica lo stato di marcia del motore e un'altra che indica lo stato di fermo: combinando opportunamente le informazioni, ne risultano due stati ammissibili e due stati non ammissibili (ammissibili sono motore in marcia contemporaneamente a motore non fermo e motore non in marcia contemporaneamente a motore fermo, mentre non ammissibili sono motore in marcia contemporaneamente a motore fermo e motore non in marcia contemporaneamente a motore non fermo). Risulta da questo esempio che l'informazione da considerare è sempre lo stato di funzionamento del motore, ma esso viene rappresentato da quattro stati logici differenti e non più da due. Aumentando le informazioni a disposizione si è aumentato il grado di affidabilità delle stesse.

Le informazioni di tipo digitale sono disponibili sia in ingresso all'apparato di acquisizione dati che in uscita dallo stesso. Le informazioni digitali che si riferiscono all'ingresso dell'apparato dalla parte del campo, che sono quindi ingressi anche per il sistema SCADA visto nel suo complesso, sono denominate *telesegnali* (abbreviato TS) o *digital input* (abbreviato DI). Le informazioni digitali che si riferiscono all'uscita dall'apparato verso il campo, che sono quindi uscite anche per il sistema SCADA visto nel suo complesso, sono denominate *telecomandi* (abbreviato TC) o *digital output* (abbreviato DO).

Informazioni di tipo analogico

Le informazioni di tipo analogico forniscono una rappresentazione della grandezza per mezzo di valori che variano con continuità all'interno di un dato intervallo. In questi casi il sistema SCADA si trova a dover interpretare una grandezza fisica che non è rappresentabile per mezzo di stati fisici distinti e la rappresentazione digitale non è più adatta. Si pensi ad esempio alla necessità di rappresentare una temperatura. La grandezza fisica per sua natura assume valori che non possono essere ricondotti a stati logici ON e OFF. In questo caso si parla di grandezza analogica. Un dispositivo chiamato *trasduttore* si incarica di tradurre l'informazione da grandezza fisica a un'informazione gestibile da un dispositivo di acquisizione dati (molto spesso si tratta di valori continui di tensione o corrente che sono proporzionali ai valori assunti dalla grandezza fisica). Questa informazione viene collegata a

una porta del dispositivo di acquisizione dati in grado di interpretarla. Ovviamente le caratteristiche della misura che deve essere gestita devono essere compatibili con quelle della porta di acquisizione (avendo in ingresso una misura rappresentata da una tensione che può variare da 0 a 10 mV non la si può interpretare correttamente in una porta che si aspetta di leggere una corrente tra 4 e 20 mA). Quello che fino a ora è stato descritto però non è ancora sufficiente per permettere al sistema SCADA di gestire la misura. Infatti è stata semplicemente tradotta l'informazione da un linguaggio ad un altro, ma anche quest'ultimo non è ancora quello utilizzato dal sistema SCADA.

Una volta che la misura è collegata alla porta essa ha bisogno, per essere correttamente gestita dal sistema SCADA, di essere convertita da segnale analogico a rappresentazione digitale dello stesso. A questo compito provvede il *convertitore analogico digitale* (A/D). Il compito di questo dispositivo è quello di convertire in un numero il valore della misura collegata alla porta. La conversione avviene associando a ogni valore possibile in ingresso un valore numerico corrispondente. Volendo rappresentare un'informazione in ingresso che ha come campo di variazione l'intervallo 0-10mV con un numero che può assumere i valori che vanno da 0 a 10, si potrebbe realizzare un convertitore A/D che a ogni aumento del valore in ingresso pari al dieci per cento dell'intervallo di variazione aumenti del dieci per cento il valore della sua rappresentazione numerica. In questo caso a un ingresso di 0 mV corrisponderebbe il valore numerico 0, a un ingresso di 1 mV corrisponderebbe il valore numerico 1, a un ingresso di 2 mV corrisponderebbe il valore numerico 2 e così fino ad arrivare al valore numerico 10 corrispondente all'ingresso 10 mV.

Già questo semplice esempio permette di individuare un limite della conversione A/D. Dovendo rappresentare una misura continua con un intervallo di numeri interi si genera una conversione che a fronte di un valore specifico della misura in ingresso fornisce una rappresentazione numerica approssimata. Infatti come si comporterebbe il convertitore per un valore di ingresso pari a 1,5 mV? lo convertirebbe con il valore numerico 1 o con il valore numerico 2? Se avessimo a disposizione una scala numerica che invece che tra 0 e 10 potesse variare tra 0 e 100 il problema sarebbe risolto (al valore 1,5 mV sarebbe associato 15). Anche in questo caso però, esisterebbero valori non direttamente rappresentati. Che dire se la misura d'ingresso dovesse assumere il valore 1,55 mV? È chiaro a questo punto che più è ampio l'intervallo numerico utilizzato per rappresentare la misura, maggiore è la precisione della conversione e quindi più precisa la rappresentazione che il sistema SCADA

ha della realtà fisica che lo circonda.

La classificazione che viene abitualmente fatta per precisione dei convertitori A/D si basa proprio sulla estensione del campo di variazione della rappresentazione numerica. Questa caratteristica viene espressa nel corrispondente numero di bit utilizzati dal convertitore A/D per rappresentare la misura analogica in ingresso. L'adozione di questo metodo di riferimento si deve alle caratteristiche tipiche di un convertitore A/D che emette l'informazione in forma digitale e quindi sotto forma di serie di bit. Esistono quindi convertitori con precisioni da otto, dodici, sedici, ventiquattro o più bit di conversione. A un maggior numero di bit corrisponde, ovviamente, una precisione maggiore.

La caratteristica di precisione considerata precedentemente è solamente una delle caratteristiche con le quali si classifica un apparato di acquisizione di dati analogici. Un'altra caratteristica che deve essere tenuta in considerazione è *il tempo di conversione*. Per tempo di conversione si intende il tempo impiegato dal convertitore A/D per fornire un'informazione il più possibile precisa della misura in ingresso. Questa caratteristica è molto importante e deve essere posta in relazione alla grandezza fisica che deve essere rappresentata. Se infatti si vuole avere una rappresentazione del livello di un liquido in un recipiente e questo livello può variare di 10 cm al secondo, allora un tempo di conversione di 5 secondi (un valore enorme rispetto a quello che normalmente i convertitori garantiscono, ma che risulta chiarificatore per l'esempio) comporterebbe, nel caso peggiore, una variazione durante il tempo impiegato per la conversione di 50 cm. Di per sè ciò non vuol dire nulla in quanto questo valore dovrebbe essere messo in relazione con le altre caratteristiche sia del fenomeno fisico che si sta rappresentando sia del sistema SCADA utilizzato. Volendo utilizzare il solo livello del liquido nel recipiente per valutare il grado di imprecisione del sistema le caratteristiche del convertitore determinano l'adeguatezza del sistema. Voler misurare con precisione di un centimetro un livello e poi introdurre un errore di 50 cm nella lettura è evidentemente sbagliato. Di contro però l'accettazione di un'imprecisione di un metro rende i 50 cm sono tollerabili.

Il tempo di conversione è una caratteristica che deve essere tenuta in considerazione in relazione all'intero sistema. Si deve scegliere il tempo di conversione in relazione al tipo di fenomeno fisico, all'imprecisione tollerata nella lettura, alla frequenza delle letture, ecc. È chiaro che più basso è il tempo di conversione, migliore risulta il convertitore. A questo però si unisce anche un aumento del costo dell'apparato di acquisizione dati e l'individuazione del giusto compromesso tra prestazioni e costi è una sfida che

chi progetta un sistema SCADA deve tenere in adeguata considerazione.

Le informazioni di tipo analogico sono disponibili sia in ingresso all'apparato di acquisizione dati che in uscita dallo stesso. Le informazioni analogiche che si riferiscono all'ingresso all'apparato da parte del campo, che sono quindi ingressi anche per il sistema SCADA visto nel suo complesso, sono denominate *telemisure* (abbreviato TM) o *analog input* (abbreviato AI). Le informazioni analogiche che si riferiscono all'uscita dall'apparato verso il campo, che sono quindi uscite anche per il sistema SCADA visto nel suo complesso, sono denominate *teleregolazioni* (abbreviato TR) o *analog output* (abbreviato AO).

Informazioni di tipo impulsivo

In alcuni casi le informazioni che consentono al sistema SCADA di interagire con il mondo circostante non sono interpretabili in modo istantaneo ma deve essere conosciuto l'andamento nel tempo delle stesse per poter fornire una rappresentazione corretta. Si pensi ad esempio a un contatore di energia elettrica. Generalmente questi contatori sono realizzati con tecnologie che permettono di fornire un impulso in uscita ogni volta che una quantità prefissata di energia ha percorso il tratto di rete da loro gestito. Per ottenere il valore di energia (che non è un valore istantaneo, ma è sempre associato ad un intervallo di tempo), il sistema SCADA dovrà contare il numero di impulsi emessi in un dato intervallo di tempo. Per farlo gli apparati di acquisizione dati mettono a disposizione particolari ingressi che sono gestiti come dei registri ad accumulo degli impulsi ricevuti in ingresso. Il sistema SCADA leggerà questi registri di accumulo a intervalli di tempo regolari per calcolare il valore dell'energia elettrica nel corrispondente intervallo.

Analogamente agli ingressi, esistono le corrispondenti uscite impulsive che sono utilizzate, ad esempio, per la movimentazione di motori passo-passo. Un motore passo-passo esegue un movimento di un certo angolo per ogni impulso che riceve in ingresso. Quando il sistema SCADA si trova a dover movimentare un motore di questo genere comanda l'apparato di acquisizione dati inviando in un particolare registro il valore numerico corrispondente al numero di impulsi da generare per far compiere al motore una rotazione di un certo angolo. L'apparato di acquisizione dati traduce il valore ricevuto nel registro in un treno di impulsi e li genera su una porta di uscita.

L'informazione impulsiva nella direzione del comando è, in questo caso, non una semplice uscita digitale (DO o telecomando) ma una serie di impulsi inoltrati al processo fisico dall'apparecchiatura attraverso un'uscita digitale.

Informazioni di tipo complesso

In alcuni casi l'interazione del sistema SCADA con il mondo esterno non avviene per mezzo di semplici informazioni quali quelle descritte in precedenza. Può accadere che il sistema SCADA si debba interfacciare con dispositivi complessi per ottenere informazioni. Esistono contatori di energia elettrica che mettono a disposizione una serie molto ampia di informazioni (tensioni, correnti, potenze, cosfi istantanei, valori medi degli stessi nell'ultimo quarto d'ora e nelle ultime ventiquattro ore, valori massimi, ecc.). Gestire questa serie di informazioni con un equivalente numero di uscite analogiche dal contatore è tecnicamente sconveniente e, quindi, i costruttori hanno previsto un'interfaccia al contatore che sia in grado di stabilire un colloquio con un dispositivo esterno attraverso un protocollo di comunicazione (spesso per questi dispositivi si trovano disponibili protocolli di tipo ModBus, LonWorks, CANbus, ecc.). In questi casi, benché le informazioni acquisite siano rappresentabili come informazioni semplici di tipo digitale o analogico, la modalità di acquisizione non è riconducibile a una tra quelle descritte. In questo caso l'apparato di acquisizione ha a disposizione una porta di comunicazione evoluta che lo mette in condizioni di stabilire una comunicazione autonoma con il dispositivo di campo e acquisire le informazioni desiderate.

Perché questa comunicazione possa avvenire il dispositivo periferico deve essere configurato con i parametri specifici del canale e del protocollo di comunicazione scelto. Ad esempio se si volesse interfacciare un dispositivo che espone un'interfaccia ModBus ASCII in una porta seriale RS-232 si dovrebbero definire la velocità di trasmissione, il numero dei bit dati, il numero dei bit di stop, il controllo di parità, il numero dello slave ModBus, tipo e indirizzo dei registri da leggere, ecc. La configurazione può avvenire direttamente nell'apparato di acquisizione dati o essere comandata dal sistema SCADA centrale all'avviamento. Indipendentemente dalla modalità di configurazione, risulta chiaro che l'insieme delle informazioni gestite, sia per la configurazione, sia per la comunicazione vera e propria, è di tipo diverso rispetto a quanto fino ad ora descritto. In questo caso è possibile parlare di informazioni di tipo complesso tralasciando una loro descrizione dettagliata che, data la varietà delle soluzioni di mercato esistenti, sarebbe per forza di cose non esaustiva.

5.2.3 Classificazione in base alle caratteristiche elettriche

Si parla di classificazione in base alle caratteristiche elettriche solo per le informazioni in ingresso e in uscita da un apparato di acquisizione dati nei confronti del campo. Le informazioni scambiate con il centro di controllo dello SCADA saranno veicolate attraverso una rete di telecomunicazione che sarà oggetto di una successiva analisi.

Ogni informazione trattata per essere interpretata da un apparato di acquisizione dati deve essere rappresentata con un segnale elettrico. Alla conversione da grandezza fisica a equivalente rappresentazione elettrica provvedono i dispositivi di campo. Ad esempio la temperatura di un oggetto viene convertita in segnale elettrico corrispondente attraverso l'uso di una termocoppia o di una resistenza variabile con la temperatura (resistenze NTC o PTC). Gli apparati che eseguono questa conversione sono definiti *trasduttori*. Nel caso di una regolazione per il comando di un apparato (ad esempio il posizionamento di una valvola di regolazione) è necessaria la conversione inversa: da segnale elettrico a comando per un motore che permette il movimento della valvola. In questo caso si parla di *attuatore*. Anche nel caso di segnali o comandi digitali è necessaria la conversione in segnale elettrico. Nel caso dei segnali un livello predefinito di tensione, la presenza o assenza di una tensione indica all'apparato di acquisizione dati lo stato logico del segnale. Solitamente questi segnali sono prelevati da contatti elettrici forniti senza alcun collegamento elettrico (nel gergo si definiscono *contatti puliti*). Per permettere all'apparato di acquisizione dati di interpretare la posizione del contatto è necessario collegare un estremo del contatto ad una sorgente di tensione elettrica e l'altro estremo all'ingresso dell'apparato di acquisizione dati. L'apparato misura la tensione presente al suo ingresso rispetto al potenziale comune e verifica se il contatto è chiuso (tensione presente all'ingresso) o aperto (tensione assente). In questo modo il contatto è stato sottoposto ad un *condizionamento* in modo da renderlo intellegibile all'apparato. Nel caso di comando digitale, la condizione sarà esattamente opposta: l'apparato di acquisizione dati fornisce lo stato dell'uscita attraverso un contatto pulito che, per agire sull'organo da comandare, deve essere sottoposto a condizionamento. In alcuni casi le uscite digitali possono essere fornite già in tensione e in questo caso è necessario definirne le caratteristiche.

In generale si può dire che dovendosi effettuare uno scambio dati tra gli apparati di campo e l'apparato di acquisizione dati è necessario definire il linguaggio comune. Nel mondo industriale, data l'eterogeneità dei produttori, è stato necessario introdurre degli standard che permettessero l'inter-

facciabilità degli apparati. Nel tempo si sono affermati standard ai quali i costruttori si sono allineati permettendo una facile integrazione dei loro prodotti. Di seguito si riporta un elenco degli standard più diffusi in relazione alle caratteristiche elettriche.

Per le informazioni di tipo digitale in ingresso le caratteristiche elettriche principali da tenere in considerazione nella definizione di un apparato di acquisizione dati sono:

- **segnali a 24 V in corrente continua**
- **segnali a 24 V in corrente alternata**
- **segnali a 48 V in corrente alternata**
- **segnali a 110 V in corrente continua**
- **segnali a 120 V in corrente alternata**
- **segnali a 220 V in corrente alternata**

Per un corretto dimensionamento del circuito di condizionamento si deve tenere in considerazione l'assorbimento in corrente di ogni singolo ingresso digitale.

Per le informazioni di tipo digitale in uscita le caratteristiche elettriche principali da tenere in considerazione nella definizione di un apparato di acquisizione dati sono:

- **comandi a 24 V in corrente continua**
- **comandi a 48 V in corrente continua**
- **comandi a 24 V in corrente alternata**
- **comandi a 110 V in corrente continua**
- **comandi a 220 V in corrente alternata**
- **comandi con uscita a relè**

Spesso un'uscita viene utilizzata per comandare un relè che poi, attraverso un suo contatto, sarà utilizzato nel circuito di comando vero e proprio. Questo passaggio è utilizzato per disaccoppiare elettricamente il circuito dell'apparato di acquisizione dati dal circuito di comando in modo che un problema tecnico su un apparato non pregiudichi allo stesso tempo le due funzioni. Per un corretto dimensionamento del circuito elettrico, sia nel caso di relè

di disaccoppiamento che in quello di comando diretto, si deve tenere in considerazione l'assorbimento in corrente di ogni utilizzatore in modo da non sovraccaricare l'apparato di acquisizione dati. Inoltre si deve considerare la tipologia dell'uscita (uscita impulsiva, viene chiusa e permane in questo stato per un certo tempo trascorso il quale torna in posizione di apertura, oppure è continua nel tempo).

Per le informazioni di tipo analogico in ingresso le caratteristiche elettriche principali da tenere in considerazione nella definizione di un apparato di acquisizione dati sono:

misure in tensione

($\pm 10\text{mV}$, $\pm 250\text{mV}$, $\pm 500\text{mV}$, $\pm 1\text{V}$, $\pm 2,5\text{V}$, $\pm 5\text{V}$, $1\dots 5\text{V}$, $\pm 10\text{V}$)

misure in corrente

($\pm 10\text{mA}$, $\pm 3,2\text{mA}$, $\pm 20\text{mA}$, $0\dots 20\text{mA}$, $4\dots 20\text{mA}$)

misure di resistenze

(150Ω , 300Ω , 600Ω)

misure da termocoppie

(tipo B, E, N, J, K, L, N, R, S, T, U)

misure da termoresistenze

(Pt100, Pt200, Pt500, Pt1000, Ni100, Ni120, Ni200, Ni500, Ni1000, Cu10)

Per un corretto accoppiamento con l'apparato di campo si deve considerare l'impedenza d'ingresso caratteristica di ogni singolo ingresso dell'apparato e fare in modo che essa sia al più uguale a quella massima tollerata dall'uscita dell'apparato di campo.

Per le informazioni di tipo analogico in uscita le caratteristiche elettriche principali da tenere in considerazione nella definizione di un apparato di acquisizione dati sono:

- **regolazione in tensione ($0\dots 10\text{V}$, $\pm 10\text{V}$, $1\dots 5\text{V}$)**
- **regolazione in corrente ($4\dots 20\text{mA}$, $\pm 20\text{mA}$, $0\dots 20\text{mA}$)**

Per un corretto accoppiamento con l'apparato di campo si deve considerare l'impedenza massima che ogni singola uscita è in grado di alimentare e fare in modo che l'impedenza di ingresso dell'ingresso corrispondente dell'apparato di campo regolato sia inferiore o al massimo uguale a questa.

5.3 Tecnologia costruttiva

Nella descrizione delle informazioni trattate da un apparato di acquisizione dati nulla è stato detto riguardo alle tecnologie. L'apparato di acquisizione dati è stato sempre visto nel suo complesso come se fosse una scatola chiusa all'interno della quale non sia consentito vedere cosa c'è. Solo le interazioni di questa scatola con il mondo esterno sono state prese in considerazione e in particolare sono state analizzate le interfacce che questa scatola espone. Questo approccio è sufficiente per comprendere a grandi linee il funzionamento. L'*apertura* della scatola al fine di descriverne i componenti interni e il loro funzionamento è cosa che va ben oltre lo scopo di questo scritto e si rimanda alla consultazione di pubblicazioni specifiche per un approfondimento del tema. È opportuno però introdurre brevemente la tecnologia che l'apparato di acquisizione dati utilizza per la gestione delle informazioni che transitano attraverso di esso.

Al fine di consentire il trattamento delle informazioni in modo indipendente dalla loro natura è necessario che l'apparato le possa manipolare facilmente. Allo stato attuale il modo più semplice che un apparato ha per manipolare informazioni è il trattamento di informazioni di tipo digitale. Il cuore di un apparato di acquisizione è infatti composto da un dispositivo a logica digitale (molto spesso un microprocessore) in grado di eseguire operazioni sui dati trattati (calcoli, salvataggio di valori da utilizzare in seguito, algoritmi di trattamento delle informazioni, dai più elementari ai più complessi). Tutto questo è possibile, e relativamente semplice, se le informazioni da trattare sono rappresentate da sequenze di cifre digitali (comunemente dette *bit*). Perché un apparato di acquisizione dati possa lavorare è quindi necessario che ogni informazione sia convertita in bit, operazione eseguita da una serie di circuiti che compongono la sezione input/output (I/O). La conversione delle informazioni di tipo analogico in informazioni di tipo digitale è una funzione svolta dai convertitori A/D dei quali si è già parlato. I convertitori D/A svolgono la funzione inversa.

Si potrebbe pensare di realizzare un apparato di acquisizione dati anche con la tradizionale elettronica di tipo analogico e permetterne ugualmente il funzionamento. I problemi di messa a punto e le limitate funzioni che in questo modo potrebbero essere realizzate ne hanno però sconsigliato l'utilizzo al punto che nessun prodotto di mercato viene prodotto con queste tecnologie. L'adozione dell'elettronica digitale ha introdotto vantaggi quali la semplificazione costruttiva, la semplicità di messa a punto, la facilità d'integrazione di funzioni, la possibilità di gestire una configurazione, la programmazione.

Quest'ultima è una caratteristica che consente la riduzione dei modelli che un produttore deve realizzare senza limitare le potenziali funzionalità (che possono essere realizzate in funzione delle esigenze specifiche).

5.4 Evoluzione degli apparati di acquisizione dati

Fino ad ora sono stati descritti gli apparati di acquisizione dati come strumenti che svolgono il ruolo di traduttori delle informazioni in modo da rendere possibile lo scambio dati tra i dispositivi di campo e il sistema SCADA. Questa funzione è stata per molti anni l'unica funzione che gli apparati di acquisizione dati hanno svolto. Con il tempo essa è stata perfezionata permettendo un filtraggio sempre migliore delle informazioni in modo che il centro potesse trovarsi a elaborare solamente informazioni realmente significative e non false variazioni dei dati. Sono stati realizzati algoritmi di pre-trattamento dei dati in ingresso volti alla diminuzione della quantità di informazioni scambiate con il centro. Questo è stato in parte dovuto ai limiti dei vettori di telecomunicazione, in parte alla limitata capacità di elaborazione del centro.

L'adozione di algoritmi di pre-trattamento delle informazioni eseguiti a bordo degli apparati di acquisizione dati ha comportato la realizzazione di dispositivi dotati di capacità elaborativa che va oltre la semplice conversione dei formati delle informazioni. Gli apparati di acquisizione hanno iniziato a richiedere potenze di calcolo tali da renderne più complessa la realizzazione e in breve si è arrivati a dotarli di potenzialità confrontabili con quelle dei calcolatori del sistema centrale. Questa migliorata capacità degli apparati di acquisizione dati ha fatto sorgere spontanea la richiesta di realizzare funzioni a bordo degli stessi, al punto da diventare apparati *intelligenti*, in grado cioè di prendere decisioni in base ai valori delle informazioni gestite.

La possibilità di suddividere la capacità elaborativa del sistema SCADA tra il centro e gli apparati di acquisizione dati ha generato un'ulteriore possibilità di evoluzione dei sistemi di controllo (cfr. sezione 2.4). Un apparato intelligente è in grado di sostituirsi al centro nella gestione delle informazioni che acquisisce e di aprire il passo all'*automazione di cella*. Un insieme di dati di campo viene raccolto in un punto nel quale viene installato un apparato di acquisizione dati. L'accorpamento delle informazioni spesso è fatto su base geografica, ma corrisponde anche ad un insieme funzionale di processo (ad esempio tutti i segnali di una cabina elettrica, un settore dell'impianto che svolge una funzione ben precisa e circoscritta, ecc.). Con l'uso di apparati intelligenti la gestione della cella può avvenire in modo autonomo rispetto al

sistema centrale: è sufficiente definire gli algoritmi di controllo dei dispositivi controllati e effettuare il controllo in base al valore corrente di segnali e misure. Il centro sarà in grado di influenzare la logica di controllo definendo gli obiettivi di funzionamento del singolo dispositivo ma non si occuperà della gestione dei dispositivi. Un esempio può essere preso dalla gestione dei motori asincroni: il sistema SCADA comanda l'avvio e l'arresto mentre i controlli necessari a garantire che queste procedure avvengano correttamente vengono attuati dall'apparato di acquisizione.

In alcuni casi l'aumentata capacità elaborativa di un apparato di acquisizione dati ha consentito anche l'integrazione di funzioni che in precedenza richiedevano l'utilizzo di dispositivi progettati allo scopo. Si pensi ad esempio a un controllo di tipo PID. Se le grandezze in gioco non richiedono capacità e velocità di elaborazione elevate è possibile realizzare un algoritmo di controllo di questo tipo a bordo di un apparato di acquisizione dati. L'integrazione di questa funzione nell'apparato comporta una semplificazione della rete di acquisizione dati e un migliore controllo da parte del sistema.

L'evoluzione degli apparati di acquisizione dati ha assottigliato la differenza che intercorre tra questi e gli apparati a logica programmabile, o PLC (*Programmable Logic Control*), questi ultimi realizzati per sostituire circuiti logici cablati di controllo di campo e dotati dell'elettismo dei dispositivi programmabili, cioè della possibilità di adattarsi alle esigenze d'impianto. Gli apparati di acquisizione dati sono pensati per il trattamento dei segnali e la comunicazione con il sistema di supervisione su una grande mole di dati mentre i PLC sono orientati alla realizzazione di logiche di controllo e sono dotati di funzioni elementari utili per la programmazione delle stesse. I principi di progettazione sono tra loro diversi perché diversa è la funzione che sono chiamati a svolgere ma l'aver dotato gli apparati di acquisizione di capacità di elaborazione e i PLC di strumenti di comunicazione con sistemi di supervisione ha reso questi dispositivi membri di un'unica grande famiglia.

Andando oltre si può dire che non è raro trovare dei dispositivi di campo quali sensori e attuatori che dispongono di una capacità di elaborazione, anche se ridotta. L'evoluzione degli apparati di acquisizione dati comporta la richiesta di:

- **capacità di elaborazione sempre crescenti**
- **integrazione di funzioni comuni programmabili con facilità**
- **standardizzazione delle interfacce e dei protocolli di comunicazione**

- **capacità di interfacciamento con altri apparati di campo**

L'evoluzione delle tecnologie di comunicazione, degli apparati di acquisizione dati e dei sistemi di elaborazione, degli strumenti di campo quali sensori e attuatori stanno conducendo a una visione nuova dell'architettura dei sistemi di controllo. Le accresciute capacità di ognuno di questi elementi rendono sempre più ampio il ventaglio delle scelte relative alla distribuzione o concentrazione delle funzionalità del sistema, alla definizione dei flussi informativi (che non si limitano più agli scambi centro-periferia ma vedono spesso gli apparati periferici comunicare autonomamente tra loro), alla localizzazione dell'informazione. Un'espressione di questa evoluzione sono i PAC (*Process Automation Suite*), cioè sistemi a basso costo che integrano capacità di acquisizione, supervisione e controllo i quali, benché ancora in embrione, mostrano una chiara tendenza alla realizzazione di sistemi distribuiti sull'impronta dei DCS ma, rispetto a questi, dotati di grande flessibilità di configurazione.

Quanto detto mostra con evidenza che coloro che si trovano a realizzare sistemi di controllo hanno a disposizione una varietà di soluzioni impensabile solo pochi anni or sono e, per questo, sono chiamati a una competenza che supera il problema della realizzazione per giungere alla capacità di compiere la scelta migliore caso per caso. La scelta dei diversi componenti e la loro configurazione per la realizzazione di questa o quella funzione, la distribuzione di alcune funzioni e la concentrazione di altre, caratteristiche tecnologiche e funzionali sono tutti elementi che debbono essere analizzati all'ombra di un'architettura del sistema che prende forma dalle scelte che verranno compiute non essendo più il punto di riferimento dal quale far discendere le scelte.

Capitolo 6

Protocolli e tecnologie di comunicazione

La realizzazione di un sistema di supervisione e controllo passa per la definizione delle interfacce tra processo controllato e dispositivi di interazione tra sistema e processo (sensori e attuatori), tra dispositivi e apparecchiature di acquisizione, tra apparecchiature di acquisizione e sistema di elaborazione, tra sistema di elaborazione e sistema di gestione dei dati e, se possibile “infine”, tra sistema di gestione dei dati e sistemi di rappresentazione dell’informazione. A pensarci bene può essere necessario definire interfacce tra il sistema nel suo complesso e altri sistemi, anche molto diversi tra loro, come i sistemi gestionali aziendali, i sistemi informativi territoriali, i sistemi di informazione di utilità pubblica. In generale esiste un’interfaccia di comunicazione in ogni sezione del sistema che definisca una separazione fisica, tecnologica, funzionale, di responsabilità.

Ognuna delle interfacce di interazione tra sottosistemi o tra sistema e mondo esterno si traduce in requisiti destinati a orientare la realizzazione del canale di comunicazione corrispondente. Le scelte possibili sono in molti casi estremamente limitate in numero e in capacità di rispondere alle esigenze evidenziate per l’interfaccia. In molti altri è necessario scegliere in un ampio ventaglio di soluzioni ma non per questo la decisione risulta meno critica. La scelta delle tecnologie e dei protocolli di comunicazione possono avere infatti un ruolo importante nella efficienza delle funzionalità che supportano pur senza compromettere la loro realizzabilità. Un altro elemento da tenere in considerazione, quando possibile, è ciò che il sistema non è e non fa oggi ma che potrebbe essere o fare domani se dotato delle caratteristiche necessarie.

Lo sviluppo di sistemi di supervisione e controllo richiede sempre un’attenta analisi delle interfacce di comunicazione e una saggia scelta di protocolli e tecnologie; questa analisi è caratterizzata da quesiti ricorrenti per i quali è

possibile dare una descrizione e suggerire elementi di analisi utili nel momento in cui deve essere presa una decisione definitiva.

Le sezioni che seguono hanno l'obiettivo di suggerire elementi di analisi per la scelta di infrastrutture di comunicazione adeguate alle caratteristiche del sistema in sviluppo. L'approfondimento di temi legati alle comunicazioni può essere affrontato consultando testi specifici (rif. [12], [11])

6.1 Velocità

La velocità di scambio dati è un elemento che può essere oggetto di analisi per ragioni di necessità o di opportunità. Analizzando lo scambio dati tra apparecchiature di acquisizione e sottosistemi di controllo è necessario tenere in considerazione le caratteristiche dinamiche del processo controllato in modo da provvedere alla realizzazione di un canale di comunicazione sufficientemente veloce da permettere che l'intero processo di acquisizione, trasmissione, elaborazione, trasmissione, attuazione avvenga in tempi tali da rendere efficaci le azioni di controllo. In questi casi i vincoli imposti dal processo controllato possono essere stringenti al punto da impedire che l'azione di controllo si realizzi in funzione delle elaborazioni realizzate dal sistema "centrale", costringendo alla realizzazione di sistemi a intelligenza distribuita. Sistemi di gestione della distribuzione dell'energia o di gestione di strutture di trasporto di gas sono esempi di sistemi che necessitano di canali di comunicazione ad alta velocità e che spesso richiedono la realizzazione di strutture periferiche in grado di attuare politiche di controllo autonome rispetto al centro di controllo. Sono evidentemente casi nei quali la tecnologia non supporta servizi di comunicazione adeguati alle velocità necessarie alla realizzazione del controllo.

Sistemi di notevoli dimensioni geografiche risentono maggiormente dei limiti di velocità imposti dalle tecnologie disponibili anche perché non permettono, in genere, di realizzare un'infrastruttura dedicata obbligando allo sfruttamento di strutture commerciali rese disponibili dai gestori telefonici i quali, per ovvie ragioni commerciali, offrono servizi di tipo *general purpose* non sempre adeguati. Anche nei casi in cui i gestori di sistemi di trasporto dell'informazione erogano servizi adeguati alle esigenze questi possono rivelarsi proibitivi in termini di costi di gestione costringendo all'adozione di architetture a intelligenza distribuita. Processi di dimensioni tali da consentire la realizzazione di infrastrutture di comunicazione dedicate conducono, di solito, a una maggiore libertà di scelta consentendo lo sviluppo di un'analisi non vincolata alla velocità dei canali di comunicazione.

La comunicazione tra centro di elaborazione e interfacce uomo-macchina deve essere caratterizzata da velocità che siano tali da consentire una corretta percezione dell'evoluzione del processo oltre che un'efficace reazione del sistema all'intervento umano finalizzato all'attuazione di azioni di controllo. Naturalmente la rappresentazione cosiddetta "in tempo reale" dell'evoluzione del processo è una chimera dell'uomo tecnologico ma lo stato dell'arte della tecnologia rende possibili velocità di scambio nella catena acquisizione, elaborazione, rappresentazione dell'informazione che spesso sono superiori alle capacità di reazione dell'operatore umano pur essendo basse per la dinamica che caratterizza del processo.

I canali di comunicazione tra il sistema di controllo e sistemi concorrenti hanno vincoli di velocità che dipendono dal motivo che conduce alla instaurazione dei canali medesimi. Se i sistemi esterni sono a loro volta sistemi di controllo hanno, di solito, esigenze prestazionali confrontabili con la dinamica del processo controllato. In questi casi il canale di comunicazione deve essere analizzato come un caso particolare di scambio tra sistema centrale e struttura periferica di acquisizione. Se il sistema concorrente non realizza funzioni di controllo (questo è il caso in cui, ad esempio, il sistema di controllo interagisce con sistemi gestionali) la scelta del canale di comunicazione non impone, di solito, particolari vincoli prestazionali.

Naturalmente la velocità effettiva dell'infrastruttura di comunicazione risulta anche da compromessi che derivano dalla necessità di soddisfare altri vincoli (alcuni dei quali trattati nelle sezioni che seguono).

6.2 Sicurezza

La sicurezza è una caratteristica dei sistemi di comunicazione che diventa rilevante quando questi possono trovarsi a essere esposti a intrusioni indesiderate e potenzialmente pericolose, anche nel caso in cui queste non dovessero essere effetto di comportamenti deprecabili (cfr. sezione 13). La sicurezza del sistema di comunicazione deve rispondere, cioè, a esigenze che non dipendono solo dalla "cattiva fede" ma anche dalla probabilità di errore che caratterizza qualsiasi comportamento umano. Anche se il sistema sicuro è soltanto il sistema "chiuso" è possibile prendere provvedimenti per limitare il rischio di malfunzionamenti delle comunicazioni causati da imperizia o dolo.

La gestione della sicurezza deve essere considerata adeguatamente sia dal punto di vista delle comunicazioni tra sistema e apparati periferici, le quali veicolano le informazioni di stato del processo controllato e, con esse, le azioni di comando impartite dal sistema, che dal punto di vista dell'interazione tra

sistema di controllo e sistemi esterni, interazione potenzialmente in grado di influenzare il comportamento del sistema e, di conseguenza, del processo controllato.

I provvedimenti che possono essere presi fanno capo a tecniche di separazione delle aree accessibili alle funzioni del sistema e all'attività degli addetti, siano esse relative all'esercizio del sistema o alla fruizione delle funzionalità rese disponibili. Tale separazione può essere fisica o logica e ha caratteristiche che dipendono dalle tecnologie utilizzate per la realizzazione delle infrastrutture di comunicazione. La realizzazione di adeguate politiche di sicurezza solitamente non presenta particolari condizioni di criticità ma è spesso caratterizzata da un atteggiamento superficiale in fase progettuale. La causa della diffusione di questo tipo di approccio risiede, probabilmente, nelle pratiche che nella storia hanno caratterizzato lo sviluppo dei sistemi di controllo. Questo tipo di sistemi, infatti, sono sempre stati caratterizzati da un grande isolamento rispetto al mondo esterno. Soltanto negli ultimi anni, grazie allo sviluppo di sistemi di comunicazione di dimensioni geografiche a basso costo (si pensi alla diffusione delle infrastrutture che supportano i protocolli UDP o TCP, oppure delle tecnologie di telefonia radiocellulare) il vantaggio di utilizzare servizi di trasporto pubblici ha comportato una riflessione seria sul tema della sicurezza.

6.3 Servizi supportati

Una caratteristica dei protocolli e delle tecnologie di comunicazione è il tipo di servizi erogati. Nell'analisi delle caratteristiche dei sistemi di comunicazione è necessario valutare correttamente la tipologia dei dati da trasferire per permettere una scelta adeguata alle esigenze dell'intero sistema. Tecnologie diverse e protocolli diversi possono erogare servizi di trasporto caratterizzati da tipi di dati affini o addirittura identici ma quasi certamente con prestazioni differenti tra loro (velocità, meccanismi di ritrasmissione, metodi di controllo degli errori di trasmissione o, detto semplicemente, qualità del servizio). Una volta individuate le caratteristiche minime in termini di tipi di dati è necessario, quindi, valutare la qualità del servizio offerta dall'infrastruttura di comunicazione per valutare l'opportunità di adottarla (magari realizzando nell'ambito del progetto contromisure a eventuali limiti individuati).

Tra i servizi supportati da un sistema di comunicazione da tenere in considerazione ci sono, naturalmente, quelli relativi al monitoraggio della qualità di erogazione degli stessi e dello stato di esercizio dei canali di comunicazione, alla interazione con infrastrutture caratterizzate da tecnologie o protocolli

distinti, alle risorse disponibili per la realizzazione dell'interazione tra il sistema costruendo e i servizi medesimi. Tali servizi possono essere considerati da un'analisi superficiale come servizi accessori ma in realtà essi sono responsabili dell'efficacia dell'uso fatto della trasmissione dati e degli interventi a scopo evolutivo ai quali il sistema può essere sottoposto nel tempo.

6.4 Affidabilità

La trasmissione dei dati è un processo caratterizzato da fenomeni che possono pregiudicare l'integrità dell'informazione trasportata comportando un reale rischio di valutazione errata dello stato di esercizio del processo controllato. In un sistema di controllo destinato a gestire processi caratterizzati da tempi di evoluzione molto bassi è impensabile procedere a una validazione dei dati ricevuti (sia dal centro di elaborazione in fase di supervisione che dalle apparecchiature periferiche in sede di attuazione del controllo). Algoritmi di validazione efficaci possono essere approntati per la valutazione della qualità dell'insieme di dati raccolti nel caso di sistemi di supervisione privi di meccanismi di controllo, sistemi per i quali i tempi di elaborazione sono legati, di solito, all'intervento diretto degli addetti alla supervisione. Nella maggioranza dei casi, quindi, l'integrità dei dati deve essere considerata un elemento caratteristico dei meccanismi di trasmissione.

Architetture tecnologiche e protocollari diverse sono dotate di algoritmi di controllo per l'individuazione di errori causati dalle infrastrutture di trasporto tra loro molto diversi. Allo stesso modo molto diversi sono i provvedimenti che i servizi di comunicazione sono in grado di prendere per colmare la lacuna introdotta nel flusso informativo da eventuali errori di trasmissione. Tali differenze però influenzano attributi non meno importanti del sistema di comunicazione tra i quali senza dubbio il più sensibile è la velocità di trasmissione. La certezza di ricevere un flusso di dati privo di errori comporta, infatti, l'introduzione di meccanismi di controllo della presenza di errori, di richiesta di ritrasmissione dell'informazione errata all'entità trasmittente, di gestione dell'ordinamento delle unità informative all'interno del flusso.

I due estremi tra le molte soluzioni possibili al problema dell'integrità del flusso informativo sono quelli che realizzano la trasmissione senza alcun controllo, lasciando al fruitore del servizio la responsabilità di intercettare gli errori e di scegliere i provvedimenti da adottare, e quelli che garantiscono l'integrità del flusso come elemento caratteristico della trasmissione dati. Come spesso accade la grande libertà di scelta si traduce in una maggiore efficacia del sistema se la soluzione adottata è frutto di una corretta anali-

si, quest'ultima possibile soltanto per mezzo dell'osservazione del sistema di comunicazione nella sua interezza.

Un'architettura protocollare che non assicura servizi per la gestione degli errori di trasmissione può essere una soluzione molto efficace quando il mezzo trasmissivo e le apparecchiature di gestione del traffico dati sono caratterizzati da probabilità di errore molto bassa. Questo è il caso in cui le dimensioni fisiche del processo controllato consentono la realizzazione di infrastrutture di piccole dimensioni, opportunamente protette da fattori di disturbo, destinate alla sola funzione di scambio dati tra sistema e processo controllato. Un altro caso di questo genere è dato dall'uso di mezzi trasmissivi ad altissima affidabilità (ad esempio la fibra ottica ha da tempo un *bit error rate* inferiore a 10^{-9}) rispetto ai quali altri componenti del sistema si comportano come cause d'errore a criticità maggiore.

Nel caso in cui il mezzo trasmissivo e le apparecchiature di comunicazione sono caratterizzate da una inaffidabilità intrinseca (si pensi al caso dei canali radio) l'uso di architetture protocollari prive di meccanismi di gestione degli errori è impensabile e la scelta consiste nella decisione tra due soluzioni possibili: usare servizi di trasmissione affidabili oppure realizzare nell'ambito del progetto i meccanismi di gestione dell'errore dei quali il servizio scelto non è dotato.

Analisi completamente diverse si fanno nel caso in cui si è di fronte alla scelta del sistema di comunicazione destinato allo scambio dati tra sistema di controllo e sistemi esterni. Come detto precedentemente è bene considerare la trasmissione dati con sistemi che concorrono al controllo del processo alla stregua di scambi tra sistema e apparecchiature di acquisizione dati. Quando il caso non appartiene a questa categoria è possibile accettare condizioni di servizio molto meno vincolanti e fare scelte di opportunità basate su elementi quali l'esistenza di servizi già disponibili, l'effettivo vantaggio dato da comunicazioni a tasso d'errore trascurabile e, di conseguenza, la ragionevolezza del costo dei servizi di trasmissione.

6.5 Disponibilità

Nella realizzazione di un sistema di supervisione e controllo è sempre importante valutare correttamente gli effetti causati da disservizi nel trasferimento dell'informazione, cioè da eventuali interruzioni del servizio di trasmissione dati. In generale un sistema di supervisione è caratterizzato da un legame diretto tra continuità del servizio di trasmissione tra sistema e apparati di acquisizione dati e continuità dell'attività di controllo. Lo stesso legame non

si manifesta mettendo in relazione l'attività del sistema e i canali di comunicazione con sistemi esterni. Quanto segue si riferisce, quindi, al sistema di controllo considerato nelle sue componenti interne.

Solitamente il sistema di comunicazione interno a un sistema di controllo deve essere dotato di una continuità del servizio almeno pari a quella richiesta al sistema nella sua interezza. Questo accade nella maggioranza dei casi ma non in tutti. Molti sistemi, in particolare quelli che non realizzano funzioni di controllo, non impongono vincoli alla continuità delle comunicazioni e sono, al contrario, caratterizzati da comunicazioni per natura discontinue. Un esempio è dato dai sistemi di telerilevamento ambientale i quali sono dotati di apparecchiature di acquisizione equipaggiate con dispositivi di archiviazione temporanea dei dati; gli stessi dati vengono periodicamente trasferiti al centro di supervisione per mezzo dell'instaurazione di opportuni canali di comunicazione e con il loro rilascio nel momento in cui il trasferimento dei dati si è concluso.

Se il sistema attua politiche di controllo necessita di un continuo aggiornamento dello stato di esercizio del processo controllato e, al tempo stesso, della disponibilità immediata di un canale di comunicazione nel caso in cui si renda necessaria l'attuazione di un'azione di controllo. Per assicurare continuità delle comunicazioni è necessario scegliere tecnologie e protocolli che prevedano servizi dotati di questa caratteristica e allestire infrastrutture in grado di colmare il vuoto lasciato nell'infrastruttura di comunicazione da eventuali guasti. Generalmente si fa ricorso al principio di ridondanza dei dispositivi lungo l'intero canale di comunicazione, con particolare attenzione agli elementi più sensibili a fenomeni che possono causare guasti o malfunzionamenti.

Un principio che è bene tenere a mente quando si realizzano sistemi di comunicazione ad alta disponibilità nega l'idea di infallibilità degli stessi. Dispositivi altamente affidabili, architetture *failsafe* e quant'altro pensabile per fornire servizi ad alta disponibilità permettono una riduzione significativa della probabilità che uno o una serie di guasti producano interruzioni del servizio, non l'eliminazione definitiva. Per rendere credibile questo principio alcuni invocano la legge di Murphy secondo la quale se il verificarsi di un evento fosse in grado di causare una catastrofe sarebbe bene mettersi l'anima in pace. Interpretata come uno dei molti modi di leggere la legge dei grandi numeri la legge di Murphy dovrebbe essere sufficiente a convincere gli scettici e condurli a un approccio più cauto all'analisi del problema.

6.6 Intelligibilità

L'intelligibilità dell'informazione è un elemento fondamentale per la realizzazione di un sistema dotato di potenziale evolutivo per le funzioni che realizza e di efficienza nell'interazione con sistemi esterni. Le soluzioni che possono essere adottate sono molte ma soltanto in numero limitato sono quelle che permettono di utilizzare interfacce di comunicazione condivise. In questo senso è fondamentale analizzare attentamente le soluzioni proposte dai produttori di dispositivi e software utilizzati nello sviluppo del sistema di controllo.

Nella definizione delle interfacce è sempre buona norma fare riferimento agli "standard" disponibili privilegiando quelli che hanno dimostrato di essere soluzioni efficaci al problema delle comunicazioni. Le virgolette utilizzate per il termine "standard" vogliono sottolineare l'importanza dell'uso di tecnologie frutto del processo di produzione di modelli di comunicazione condivisi (sia esso condotto da istituti dedicati allo scopo o da altre entità) e, al tempo stesso, un suggerimento a interpretare correttamente il termine. Nel mondo della tecnologia si può considerare standard tutto ciò che viene convenzionalmente uniformato a un modello di riferimento comune. Il modello è un sistema di regole alle quali deve far riferimento una implementazione che voglia definirsi aderente allo standard. È un fatto, quindi, che un'architettura a elevata diffusione non deve essere considerata standard se per essa non esiste un'adeguata definizione del modello che realizza e la libertà per i produttori di infrastrutture di comunicazione di affrontare una propria realizzazione della stessa. L'uso di prodotti non standard è una scelta che risulta vincolante da un punto di vista sia funzionale che tecnologico. Entrambi gli aspetti sono legati al fatto che un sistema di comunicazione proprietario impone l'uso di dispositivi per i quali la scelta è limitata, di solito, ai soli dispositivi (tra quelli funzionalmente adeguati agli scopi del sistema) in grado di utilizzare l'interfaccia di comunicazione adottata, così come accade per la realizzazione o l'adeguamento di sistemi esterni destinati a comunicare con il sistema di controllo.

Un altro elemento di riflessione sull'uso di architetture standardizzate consiste nel fatto che tutto ciò che appartiene alla comunità scientifica e tecnologica non dipende dal mercato, dalla fortuna di un'azienda, dall'abilità di un manager. La condivisione dei modelli è garanzia di continuità prima che di qualità e rappresenta un bene irrinunciabile per chiunque si trovi a realizzare sistemi che abbiano aspettative di vita superiori alla vita media di un prodotto tecnologico commerciale.

Capitolo 7

Sistema di elaborazione

Con il capitolo relativo al sistema di elaborazione si completa la presentazione dell'architettura di un generico sistema di supervisione e controllo. Il modello proposto per la porzione di sistema destinata alle funzioni di elaborazione (cfr. figura 7.1) rappresenta una soluzione classica del problema tecnologico di realizzazione di architetture di calcolo chiamate a svolgere compiti di controllo. Al tempo stesso questo modello ha un significato di architettura funzionale che rimane valido anche in vista delle evoluzioni alle quali i sistemi SCADA sembrano destinati e, quindi, di strumento per la presentazione delle caratteristiche tipiche di tali sistemi.

Dalla figura emerge una visione del sistema quale struttura caratterizzata da tre elementi fondamentali: gestione dati, elaborazione, disponibilità dell'informazione. Per gestione dati si intende il complesso di funzioni destinate allo scambio dati con le apparecchiature periferiche, al trattamento dei dati per la generazione di un insieme di dati intelligibile per le funzioni di elaborazione e di rappresentazione, all'archiviazione dei dati grezzi e dell'informazione aggregata frutto delle elaborazioni. Per elaborazione si intende tutto quanto responsabile della corretta interpretazione dei dati visti come insieme rappresentativo dello stato di evoluzione del processo controllato e dell'attuazione delle azioni di controllo. Il terzo elemento è la produzione dell'informazione finalizzata alla fruizione da parte di sistemi esterni e dalle strutture di interazione tra operatori e sistema.

Il contenuto delle sezioni che seguono ha lo scopo di illustrare con maggiore dettaglio le caratteristiche di questi elementi architettonici.

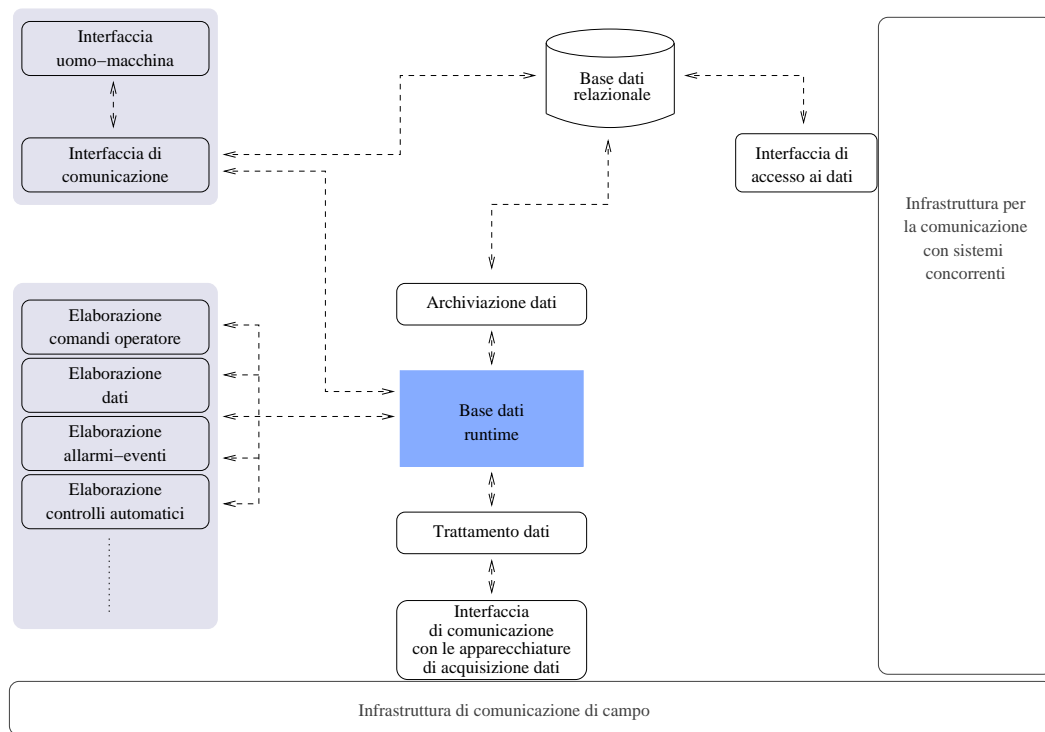


Figura 7.1: Architettura del sistema di elaborazione di un sistema SCADA

7.1 Gestione dei dati

Un sistema di supervisione e controllo ha nella gestione dati l'elemento cardine di tutte le sue attività. Esso riceve dati rappresentativi dello stato di esercizio del processo controllato provenienti dalle apparecchiature periferiche. In base alle convenzioni adottate per lo scambio dati con il *campo* il sistema opera un processamento destinato a uniformare l'informazione ricevuta a un formato predefinito considerato di riferimento per l'informazione interna al sistema. A un trattamento analogo è sottoposta tutta l'informazione diretta dal sistema alle periferiche, informazione destinata a richiedere l'attuazione di azioni di controllo.

Tali trattamenti si riferiscono all'informazione che fluisce attraverso il canale di comunicazione instaurato tra sistema e strutture periferiche. Dal punto di vista del sistema questo flusso ha un punto di raccolta, cioè una base dati, sorgente e destinazione del traffico. Si tratta di uno spazio con caratteristiche di banca dati destinato a servire le richieste di tutti i processi di elaborazione (automatici e manuali) che necessitano dell'insieme di dati rappresentativo dello stato del processo controllato. Il tipo di elaborazione alla quale questi dati sono sottoposti richiede comportamenti della

base dati che tipicamente si risolvono in un vincolo semplice ma stringente: tempi di accesso estremamente limitati. La base dati contenente le informazioni di stato con le quali i processi di elaborazione sono chiamati a decidere riguardo l'attuazione di azioni di controllo deve essere in grado di servire le richieste in tempi compatibili con la dinamica di evoluzione del processo controllato. Forzando il concetto usualmente sintentizzato con l'espressione *realtime* si può dire che la base dati contenente la rappresentazione dello stato del processo controllato deve essere caratterizzata da tempi di accesso che la qualificano come operante in tempo reale (dall'acquisizione dei dati al conseguente invio di azioni di controllo). Questa base dati viene comunemente denominata *database runtime* e una soluzione tecnologica per la sua realizzazione può essere, ad esempio, l'uso di aree di memoria fisica condivisa tra i processi che insistono sui dati che essa contiene. Il *database runtime* è sorgente di informazione per i processi automatici di elaborazione e per i sistemi di rappresentazione dell'informazione utilizzati dagli operatori umani per la gestione del sistema; in ogni caso esso contiene esclusivamente una rappresentazione dello stato di esercizio attuale del processo controllato.

Una gestione dei dati così fatta esaurisce le esigenze che caratterizzano un sistema SCADA per le funzionalità fondamentali di supervisione e controllo ma non permettono di accumulare conoscenza riguardo l'evoluzione del processo controllato. Per l'archiviazione dei dati acquisiti dalle apparecchiature periferiche e dell'informazione generata dal sistema nello svolgimento delle sue funzioni è necessario provvedere con un sistema di gestione dati che abbia le caratteristiche di una base dati relazionale. Le proprietà che rendono la base dati relazionale strumento privilegiato per la gestione delle informazioni storiche di un sistema di controllo sono l'intelligibilità dell'informazione, la disponibilità di strumenti di accesso di livello applicativo, l'abilità di gestire grandi quantità di dati. Queste caratteristiche si accompagnano a tempi di accesso ai dati che non sono confrontabili con quelli caratteristici dei database runtime ma l'analisi a posteriori di informazioni storiche non ha finalità di controllo e non necessita di prestazioni particolari. L'uso di basi dati relazionali introduce, così, elementi di accessibilità ai dati che consentono di supportare l'ampliamento delle finalità per le quali l'informazione raccolta dal sistema viene archiviata. La razionalità dell'organizzazione dei dati, la semplicità dei processi di interrogazione della base dati, la completezza dell'informazione e la possibilità di associare quest'ultima a quella proveniente da sistemi concorrenti consente di utilizzare i dati per ragioni tra loro molto diverse quali l'analisi dell'evoluzione del processo controllato finalizzata alla previsione, la contabilizzazione di grandezze gestite dal sistema legate

a processi economici e quant'altro immaginabile in sede di analisi. Per sua natura la base dati relazionale diventa, quindi, il canale di comunicazione privilegiato tra sistema di controllo e mondo esterno.

7.2 Processi di elaborazione

Da quanto visto si può dire che il sistema di controllo dispone di uno strumento di scambio delle informazioni con il processo controllato in grado di ricevere informazioni di stato e inviare comandi destinati al controllo dell'evoluzione dello stato. La mole di dati scambiati e la complessità del processo (e di conseguenza dell'interpretazione dei dati ricevuti) rende impossibile un'analisi diretta da parte degli operatori e suggerisce la realizzazione di procedure di calcolo responsabili della generazione di informazioni aggregate rappresentative della qualità dell'evoluzione dello stato.

Il controllo del traffico interno a uno scalo ferroviario ci fornisce un esempio per comprendere l'importanza dell'elaborazione finalizzata alla rappresentazione macroscopica del fenomeno in osservazione e permette di estendere lo stesso principio alle procedure di controllo. L'operatore di un sistema di controllo del traffico dispone di una rappresentazione dello scalo in termini di percorsi (occupazione e disponibilità). Per capire se un percorso è disponibile ad accogliere un convoglio è necessario verificare che la posizione degli scambi sul lato di provenienza del mezzo siano posizionati correttamente, che il percorso non sia già occupato da altri convogli, che sulla linea non ci siano attività di manutenzione, che la segnaletica sul lato opposto a quello di arrivo del convoglio impedisca l'ingresso di un altro mezzo. Non disponendo di processi di elaborazione dei dati l'operatore umano è chiamato di volta in volta a verificare la concorrenza di un numero di condizioni in molti casi eccessivo ed è portato inevitabilmente a perdere la visione dello stato del processo per la quale è più opportuno disporre dell'informazione macroscopica (*linea 1 disponibile da nord*). Allo stesso modo la procedura di occupazione di una linea può essere ricondotta a una operazione che dal punto di vista dell'operatore coincide con l'attuazione di una azione di controllo (i processi di elaborazione sono poi in grado di interpretare il comando e attivare il controllo su scambi, semafori, ...).

La realizzazione di processi di calcolo risponde a esigenze quali:

- generazione di rappresentazioni sintetiche dello stato del processo
- generazione di segnalazioni rappresentative di anomalie nell'evoluzione dello stato

- interpretazione dei comandi operatore e attuazione dei controlli puntuali
- produzione di informazioni aggregate (dati preventivi e/o consuntivi) rappresentative della tendenza evolutiva del processo
- realizzazione di procedure automatiche di controllo

L'elenco termina con un punto per il quale è opportuno fornire precisazioni. Nei casi in cui la dinamica del processo non consente un tempestivo intervento dell'operatore umano per l'attuazione di azioni o procedure di controllo, quando il sistema è caratterizzato dall'attuazione periodica di azioni di controllo predefinite, quando, cioè, è necessario introdurre elementi di automazione del sistema si procede alla realizzazione di processi che implementano procedure automatiche di controllo le quali agiscono in completa autonomia rispetto al controllo dell'operatore umano responsabile del presidio del sistema SCADA.

7.3 Condivisione dell'informazione

Un sistema di controllo composto dai due elementi presentati nelle precedenti sezioni è caratterizzato da autonomia ed efficacia operativa ma si presenta come un sistema accessibile dal mondo esterno solo attraverso gli strumenti d'interazione (interfaccia uomo-macchina) che esso porta con sé. L'attività di un tale sistema è invece oggetto di un interesse che raramente si limita alla semplice funzione che può essere svolta da un operatore. Si nota, al contrario, una tendenza a realizzare sistemi che siano in grado di minimizzare, se non annullare, l'intervento umano per scopi di controllo e a sviluppare strumenti e metodi di analisi dei dati con l'obiettivo di rendere disponibili informazioni aggregate di carattere consuntivo o preventivo. Per realizzare funzionalità di questo genere è necessario *uscire dal sistema*, cioè fare in modo che strutture esterne al sistema di controllo abbiano visibilità dei dati da esso gestiti e conservati. L'alternativa a questa soluzione è realizzare all'interno del sistema funzioni che producano e rendano disponibili (sempre tramite strumenti interni) le informazioni d'interesse. Questa soluzione comporta però una forzatura della natura del sistema di controllo la quale, invece, per soddisfare le esigenze di sicurezza, affidabilità e di prestazioni deve conservare le caratteristiche tipiche della supervisione e del controllo.

Ciò che serve è, dunque, un sistema di condivisione dell'informazione per mezzo del quale operatori, sistemi esterni e quant'altro in grado di elaborare

e analizzare dati possano prelevare le informazioni loro necessarie e utilizzarle opportunamente senza che il sistema di controllo venga coinvolto in queste attività. Tra le proprietà di un sistema di condivisione dell'informazione quelle che possono essere considerate irrinunciabili sono la disponibilità di metodi e strumenti di gestione di grandi moli di dati e la possibilità di osservare questi ultimi come un insieme non informe, cioè come una aggregazione strutturata costituente un archivio di informazioni compiute. Ciò che ci si aspetta dagli strumenti di condivisione dell'informazione è, quindi, la possibilità di accedere a una banca dati. Le soluzioni che possono essere proposte sono, al solito, molte, ma l'unico strumento realmente adeguato all'assolvimento delle funzioni finora descritte è la base dati relazionale. All'adeguatezza di carattere logico deve essere aggiunta quella relativa agli aspetti tecnologici: le basi dati relazionali sono realizzate da sistemi che rendono disponibili strumenti di accesso, gestione e analisi delle informazioni contenute, da sistemi che in tutta autonomia implementano tutte le funzionalità che rispondono alle esigenze qui qualificate come *condivisione dell'informazione*.

Parte III

Sistema di elaborazione

Capitolo 8

Elaborazione dati

Le informazioni gestite da un sistema SCADA sono di varia natura e possono essere acquisite con varie modalità. Si è visto in una sezione precedente che gli apparati di acquisizione dati provvedono a uniformare queste informazioni in modo da permettere al sistema di controllo di lavorare con un numero ristretto di tipologie di dati. Le informazioni trattate consentono di rappresentare il processo controllato sotto forma di un insieme finito di *tipi di dato*. Il trattamento che il sistema esegue su ogni tipo è tipico del dato trattato e prescinde dalla grandezza fisica che questo dato rappresenta. Questa generalizzazione è possibile in quanto le funzioni tipicamente realizzate dai sistemi SCADA sono indipendenti dalle caratteristiche del processo controllato. In questa ottica il sistema SCADA acquisisce le caratteristiche di sistema generalista che ha il compito di mettere a disposizione degli operatori e dei processi sovraordinati informazioni che questi sono in grado di interpretare e gestire e delle quali divengono responsabili. Questa visione ha una formulazione esplicita nei prodotti che il mercato del software propone come *piattaforme di sviluppo di sistemi SCADA*, pensate per dotare chi realizza sistemi di controllo di una base di riferimento completa di tutte le funzioni più comuni. Naturalmente quanto non fornito dalla piattaforma di sviluppo deve essere realizzato di volta in volta per soddisfare le esigenze di controllo.

Questo capitolo tratta l'elaborazione dei dati in relazione alle funzioni generali che un sistema SCADA deve essere in grado di realizzare. La *personalizzazione* di una piattaforma SCADA per la realizzazione di un sistema di supervisione e controllo specifico esula dalla natura della trattazione, ma nel corso della stessa sono stati presentati esempi specifici che possono aiutare a farsi un'idea su questo problema. In particolare le sezioni che seguono contengono la presentazione di cosa e come il sistema SCADA fa nel trattamento dei dati, nella gestione dei comandi operatore, nei calcoli che possono essere effettuati sui dati acquisiti e nella gestione delle azioni automatiche di

controllo.

8.1 Trattamento dati

8.1.1 Tipi di dati

Già nel capitolo dedicato agli apparati di acquisizione dati sono state illustrate le diverse tipologie di dati che possono essere gestiti da un apparato periferico e questo è stato fatto anche dal punto di vista fisico. Quanto detto mostra che tutti i dati trattati vengono ricondotti a categorie macroscopiche astratte. Un sistema SCADA è in grado di interagire con il processo controllato per mezzo di una sua rappresentazione basata sui seguenti tipi di dati:

- **dati di tipo discreto**
- **dati di tipo analogico**
- **dati di tipo stringa**

Alla categoria dei dati discreti fanno capo le informazioni che possono assumere solamente stati logici distinti. Tipico esempio è un ingresso digitale ad 1 bit che può assumere solamente lo stato logico ON o lo stato logico OFF. In alcuni casi è possibile avere anche dati discreti che possono assumere più di due stati logici e in questo caso si possono avere informazioni a due, tre, quattro, n bit. Si pensi ad esempio allo stato di un interruttore elettrico che, essendo rappresentato da due finecorsa, uno di chiusura e uno di apertura, può assumere i seguenti valori:

- 01** : il contatto del fine corsa di apertura aperto e quello del fine corsa di chiusura chiuso indicano che l'interruttore è in posizione di chiusura
- 10** : il contatto del fine corsa di apertura chiuso e quello del fine corsa di chiusura aperto indicano che l'interruttore è in posizione di apertura
- 00** : il contatto del fine corsa di apertura aperto e quello del fine corsa di chiusura aperto indicano che l'interruttore è in posizione intermedia (probabilmente si sta compiendo la manovra)
- 11** : il contatto del fine corsa di apertura chiuso e quello del fine corsa di chiusura chiuso indicano che l'interruttore è in posizione incongruente (probabilmente c'è un malfunzionamento nell'organo o nei contatti ausiliari)

Alla categoria dei dati analogici fanno capo le informazioni che si riferiscono ad un valore analogico e che normalmente sono rappresentate per mezzo di un valore intero o reale. Ad esempio il valore di temperatura letto da una termocoppia potrebbe essere convertito in informazione analogica che indica un intervallo di misurazione da 0 a 200 gradi centigradi.

Alla categoria dei dati stringa fanno capo tutte le informazioni che possono essere rappresentate come insieme di caratteri e che spesso corrispondono a un messaggio da interpretare direttamente nella lingua degli operatori. Si pensi ad esempio al caso in cui si debba comandare un pannello per segnalare un'informazione ad un operatore di campo riguardo una particolare operazione da svolgere. In qualche caso piuttosto che dire “esegui operazione: 13” dove 13 indica il codice di un'operazione da svolgere, è preferibile un messaggio del tipo “esegui operazione: *apertura valvola di bypass*”. In altri casi l'apparato periferico è chiamato a gestire dati di tipo complesso che però non è in grado di interpretare dovendo così trasferirli al sistema di elaborazione nella forma in cui li riceve.

8.1.2 Database runtime

Tutti i dati che il sistema SCADA gestisce risiedono in un unico database detto *database runtime*. È già stato specificato che il database runtime ha come caratteristica principale quella di permettere l'accesso a questi dati privilegiando la velocità. Questa caratteristica è necessaria per l'ottenimento di un'elaborazione realizzata in tempi compatibili con le esigenze del processo controllato ed è il vincolo che comporta la realizzazione del database runtime come struttura monolitica.

I dati che sono presenti nel database runtime sono spesso sottoposti anche a un altro vincolo: l'accesso concorrente da parte di più processori di elaborazione. Questo è il motivo per il quale il database runtime è spesso realizzato con l'uso di aree di memoria condivisa. Questo tipo di area di memoria, per tipologia costruttiva e limiti dovuti alle infrastrutture software, ha un tetto nelle dimensioni raggiungibili. Nella definizione dell'architettura di un sistema SCADA deve essere considerato questo limite, anche in relazione al fatto che la mole di dati può raggiungere le migliaia di unità. Fortunatamente l'evoluzione tecnologica ha ridotto questa limitazione ma l'organizzazione caratteristica che il database runtime ha acquisito negli anni per ovviare il problema tende a conservarsi.

Per ogni punto gestito dal sistema SCADA si debbono individuare due classi di informazioni distinte tra loro:

- **informazioni dinamiche:** informazioni che variano nella normale elaborazione
- **informazioni statiche:** informazioni che non variano nella normale elaborazione

Le prime informazioni sono quelle che riguardano l'evoluzione del valore assunto dalle variabili, le seconde sono quelle di definizione delle caratteristiche del dato (e non subiscono variazioni se non a causa di operazioni di configurazione). Il database runtime si occupa di gestire le informazioni del primo tipo, mentre le altre possono essere lette dai processi all'avvio del sistema SCADA e poi gestite internamente. In questo caso, dato che le prestazioni all'avvio del sistema non sono stringenti, le fonti da accedere per ottenere le informazioni di configurazione possono anche non essere particolarmente veloci (ad esempio file).

Informazioni immancabili in un database runtime sono:

- **l'identificativo del dato**
- **l'etichetta di tempo relativa all'ultima acquisizione**
- **il valore corrente**
- **il codice di qualità**

L'*identificativo del dato* è un codice interno al sistema che permette di identificare univocamente il dato trattato. Può essere rappresentato dal nome del dato così come impostato da chi configura il sistema SCADA o, ciò che accade comunemente, da un codice numerico imposto dal sistema. Attraverso l'identificativo il sistema è in grado di conoscere il dato che sta trattando e tutte le componenti del sistema si riferiscono a esso.

L'*etichetta di tempo relativa all'ultima acquisizione* è l'informazione sull'istante, in termini di tempo di sistema, nel quale si è verificata l'ultima variazione del valore. Nel caso di dati acquisiti questo si riferisce all'ultima lettura che ha generato un nuovo valore per il dato. Nel caso di comandi il tempo si riferisce all'ultima circostanza nella quale il comando è stato impartito. L'informazione tempo viene solitamente associata al dato direttamente dal sistema centrale ma in alcuni casi per i dati acquisiti possono essere gli apparati periferici a generare questa informazione. Ciò comporta un miglioramento della qualità dell'informazione in quanto si avrà una conoscenza dell'istante di variazione del valore più precisa, caratteristica particolarmente importante nel caso in cui gli apparati non sono in collegamento continuo con

il sistema centrale ma immagazzinano i dati in attesa di essere interrogati. In questo caso è importante non sottovalutare il problema della sincronizzazione tra tutti gli apparati che costituiscono il sistema SCADA.

Il *valore corrente* costituisce il valore che assume il dato nell'istante corrente. Questo valore si riferisce all'ultimo valore acquisito dal campo.

Il *codice di qualità* è un attributo che serve a completare il dato, fornisce un'informazione sulla qualità del valore. Si pensi ad esempio a un valore analogico che per sua definizione deve essere contenuto all'interno di un determinato intervallo di variazione ammissibile. Se il valore ricevuto dal campo dovesse risultare esterno a questo intervallo avere un codice di qualità che lo segnala significherebbe avere un'informazione migliore rispetto all'accettazione del valore posto all'estremo superiore o inferiore della scala. Analogamente a questo codice si possono avere codici di qualità che specificano altre caratteristiche del dato. Di seguito si riporta un elenco dei principali codici di qualità utilizzati nei sistemi SCADA:

- **fuori scansione:** il valore del dato non è correntemente acquisito
- **fuori range:** il valore è al di fuori dell'intervallo
- **valore manuale:** il valore è stato impostato manualmente
- **invalido:** il valore non è valido

8.1.3 Configurazione dei dati trattati

Nella sezione precedente è stato introdotto il problema della gestione dei dati con la presentazione delle informazioni dinamiche. Esiste un altro insieme di informazioni che sono necessarie alla definizione e alla gestione di ogni singolo dato. Queste informazioni sono generalmente indicate con l'espressione *informazioni di configurazione*.

Il trattamento che solitamente subisce un dato all'interno di un sistema SCADA può essere sintetizzato nel seguente elenco di operazioni:

- **acquisizione**
- **conversione in valore ingegneristico**
- **rilevamento allarmi**

Ogni processo che manipola i dati ha la necessità di avere una serie di informazioni per poter svolgere il proprio compito. Queste informazioni possono essere contenute in file di configurazione letti dai processori alla partenza

del sistema o, come accade nei sistemi più moderni, essere contenuti in un database relazionale. In generale per la gestione di un dato è necessario definire informazioni per ogni fase del suo trattamento. Questo è il tema trattato nelle sezioni che seguono.

Processo di acquisizione

Il processo di acquisizione è relativo all'acquisizione del dato dall'apparato periferico. Perché il processo possa compiersi è necessario definire per ogni dato:

- **canale di acquisizione**
- **identificativo del dato nel canale di acquisizione**
- **caratteristiche del dato da acquisire**

Il *canale di acquisizione* definisce sostanzialmente a quale apparato di acquisizione dati il dato viene associato. Nella definizione del canale saranno definite tutte le informazioni che permettono l'instaurarsi di uno scambio dati tra il sistema centrale e l'apparato periferico. Ad esempio per una comunicazione seriale punto-punto sarà necessario specificare quale porta di comunicazione seriale utilizzare (com1, com2, ecc.), la velocità di scambio dati, la parità, il numero di bit di dati, ecc. Queste informazioni sono specifiche del tipo di canale di comunicazione utilizzato e del protocollo di comunicazione utilizzato.

L'*identificativo del dato nel canale di comunicazione* è un identificativo che permette di individuare univocamente il dato all'interno del flusso informativo instaurato. Con questo identificativo si stabilisce una relazione univoca tra il dato definito al centro di controllo e il dato gestito dall'apparato di acquisizione dati. Solitamente per la definizione di questo identificativo si seguono regole che sono definite dal protocollo di comunicazione. Ad esempio nel caso di utilizzo del protocollo ModBus ogni dato viene riconosciuto con un particolare indirizzo del registro nel quale è contenuto essendo la mappatura dei registri con le morsettiere dell'apparato periferico definita dall'apparato stesso.

Le *caratteristiche del dato da acquisire* definiscono la tipologia del dato da trattare. Ad esempio dall'apparato possono essere acquisiti segnali digitali o analogici, allarmi, possono essere inviati comandi digitali o regolazioni. Per il trattamento di ognuno di questi tipi di dato sono definite regole che il sistema SCADA deve seguire. Come esempio possiamo citare la distinzione che viene

fatta nel caso dei dati di tipo analogico tra dati il cui valore è rappresentato tramite un valore intero e quelli rappresentati in virgola mobile.

Processo di conversione in valore ingegneristico

Abbiamo visto nella sezione dedicata agli apparati di acquisizione dati che ogni informazione gestita dal sistema subisce una serie di conversioni di valore durante il suo tragitto dal campo al sistema centrale. Queste conversioni sono necessarie per permettere agli apparati periferici di gestire contestualmente informazioni che rappresentano grandezze fisiche diverse e scale di valori diverse, cioè indipendentemente dalla tipologia di informazione fisica. Una volta che l'informazione arriva al centro deve subire il processo inverso per poter descrivere esattamente le caratteristiche della grandezza fisica originaria. La conversione assume caratteristiche diverse se si tratta di conversione di misure o di segnali. Quanto di seguito descritto si riferisce alle informazioni che viaggiano in direzione del centro, ma è valido, con le opportune considerazioni, anche per le informazioni che viaggiano dal centro verso il campo.

Si consideri la conversione nel caso di trattamento di segnali. In questo caso è noto che un segnale rappresenta per mezzo di stati logici un insieme di stati fisici dell'organo (ad esempio motore in marcia o fermo). La conversione che avviene al centro in questo caso è molto semplice e consiste nell'associare ad ogni valore logico che arriva dall'apparato di acquisizione il corrispondente stato fisico.

Nel caso di conversione per le misure il problema è più complesso. Le informazioni acquisite da un apparato periferico vengono scambiate con il centro per mezzo di unità di misura convenzionali che si definiscono *unità grezze*. Un'unità grezza in realtà non è un'unità di misura ma un valore adimensionale. Il valore grezzo rappresenta il valore assunto dal dato acquisito all'interno dell'intervallo di variazione definito dall'apparato che lo acquisisce. Ad esempio una misura analogica può essere rappresentata con un valore intero espresso con cifra a due byte con segno; l'intervallo di variazione della misura va così dal valore -32768 al valore +32767.

È impensabile di proporre ad un operatore un valore di questo genere in quanto non dà informazioni né sul tipo di misura, né sul valore assunto dalla misura. Si deve procedere in questo caso alla conversione in *valore ingegneristico*. Per poter procedere a questa conversione è necessario conoscere:

- **l'unità ingegneristica**

- **la funzione di conversione**

L'unità ingegneristica è semplicemente l'unità di misura utilizzata dallo strumento impiegato per la trasduzione in campo. Questa unità sarà tipica della grandezza fisica (gradi centigradi per una temperatura, bar per una pressione, metri per un livello, ...).

La funzione di conversione definisce l'algoritmo da utilizzare per convertire il valore grezzo in valore che esprime la misura della grandezza nella sua unità ingegneristica. In pratica corrisponde all'algoritmo complementare a quello utilizzato nella fase di acquisizione del dato. Solitamente gli algoritmi che si impiegano nella conversione sono:

- **conversione lineare:** del tipo $y = a \cdot x + b$
- **conversione quadratica:** del tipo $y = a \cdot x^2 + b \cdot x + c$
- **conversione quadratica inversa:** del tipo $y = a + b \cdot \sqrt{x}$

Per la definizione di questi algoritmi è necessario definire i parametri di conversione che spesso coincidono con i valori minimo e massimo grezzi e in unità ingegneristiche.

Processo di rilevamento allarmi

Quando un dato viene acquisito da un apparato periferico assume un'insieme di valori che possono rappresentare condizioni di normale funzionamento oppure di funzionamento anomalo. Nel secondo caso l'operatore deve essere avvisato dell'anomalia attraverso un'informazione di tipo allarme che ne attiri l'attenzione e ne forzi la reazione tendente a riportare il sistema in uno stato di normale funzionamento. Il dettaglio sul significato e la gestione degli allarmi è trattato in un'altra sezione mentre qui vengono descritte le informazioni necessarie per poter svolgere il processamento del dato al fine di generare l'allarme.

Innanzitutto è importante precisare che gli allarmi sono associati solamente a segnali o misure. La condizione di allarme non è infatti riferita a comandi che un operatore impartisce, ma a situazioni di campo che indicano stati di funzionamento al di fuori di quanto previsto. Esiste poi un trattamento diverso per le informazioni di tipo segnale rispetto a quello utilizzato per le informazioni di tipo misura.

Un segnale è un insieme di stati logici. L'allarme che si può definire per un segnale è semplicemente l'associazione di ogni singolo stato logico a una

condizione di normale funzionamento o di anomalia. Ad esempio per un interruttore elettrico le posizioni di aperto o chiuso potrebbero rappresentare un normale funzionamento, ma la posizione di incongruenza è sicuramente una situazione di malfunzionamento (probabilmente dovuta ad un guasto che genera la segnalazione anomala). La posizione intermedia invece merita un trattamento particolare. Essa è valida se permane per un tempo confrontabile con il tempo di manovra dell'interruttore, ma se protratta oltre limiti predefiniti indica un malfunzionamento. In questo caso c'è la necessità di un'ulteriore elaborazione che prenda in considerazione anche il tempo di permanenza in un certo stato per poter generare l'allarme.

Per le misure i tipi di allarme che possono essere generati sono molti. I più comuni sono:

- **allarme per superamento limite**
- **allarme di deviazione**
- **allarme di velocità di variazione (*ROC = Rate Of Change*)**

L'*allarme per superamento limite* viene generato nel momento in cui il valore di una misura supera un certo valore di riferimento definito come limite. Solitamente si definiscono due valori di limite superiore e due valori di limite inferiore. Si costruisce in questo modo una banda di normale funzionamento attorno al dato, una banda stretta di attenzione ed una banda ampia di pericolo. I dati necessari a generare questi allarmi sono semplicemente i quattro valori limite che definiscono le due bande di osservazione.

L'*allarme di deviazione* può essere utilizzato quando una misura rappresenta una grandezza fisica che il processo deve tenere sotto controllo per assicurare il rispetto costante di un valore predefinito. Si pensi ad esempio ad una regolazione che debba mantenere la temperatura di un recipiente stabilmente a 35 gradi centigradi. La misura della temperatura fornisce il valore corrente della temperatura ma può essere comodo associare alla temperatura un allarme che il sistema genera se il valore si allontana da quello impostato di una certa quota percentuale. Questo allarme verrà generato sia per variazioni che tendono ad innalzare la temperatura oltre il *set-point*, sia per variazioni che tendono ad abbassare la temperatura. Solitamente si possono associare due soglie di variazione: la variazione minima e la variazione massima in modo da definire anche in questo caso un limite di attenzione ed un limite di pericolo.

L'*allarme di velocità di variazione*, o *ROC (Rate Of Change)*, è un allarme che viene generato quando il valore di un dato subisce una variazione nel

tempo superiore a un limite prefissato. Si pensi ad esempio ad un processo che debba garantire il riempimento di un recipiente con un liquido garantendo una velocità del flusso limitata (ad esempio da problemi legati alla temperatura del liquido e dalla capacità di dilatazione del recipiente). In questo caso si può impostare il sistema per generare un allarme in corrispondenza di variazioni troppo repentine del livello di liquido nel recipiente. Si noti che non sarebbe sufficiente definire un valore massimo per il livello del liquido ma si deve assicurare che il livello non aumenti di quote prefissate dell'altezza del recipiente in determinati intervalli di tempo. Le informazioni necessarie per definire il limite di allarme di velocità di variazione sono il valore massimo di variazione limite ammessa, in unità ingegneristiche o in valore percentuale, e il tempo minimo nel quale essa può compiersi.

8.2 Elaborazione comandi

Le funzioni caratteristiche di un sistema SCADA realizzano, come detto, il controllo e la supervisione di un processo. La supervisione consiste nella rappresentazione dell'evoluzione dello stato del processo e viene realizzata per mezzo di strumenti che consentono da un lato una chiara e immediata percezione dello stato attuale, dall'altro l'analisi a posteriori dell'evoluzione dei parametri fondamentali e l'osservazione, sempre a posteriori, dello stato del processo in particolari istanti di tempo, cioè istantanee relative a fasi di evoluzione attraversate nel passato. Il controllo consiste nella realizzazione di funzioni che consentono al sistema SCADA di interagire con il processo con lo scopo di influenzarne l'evoluzione. Questa capacità del sistema di modificare l'evoluzione dello stato del processo deve corrispondere a un insieme finito di azioni di tipo deterministico attuabili a scopo di controllo. Se così non fosse il sistema potrebbe forzare il processo a un'evoluzione verso stati non contemplati dal normale sviluppo del processo medesimo, fatto che può non soltanto vanificare l'attività del processo ma anche condurre a condizioni di pericolo. A riguardo è possibile fare molti esempi e tra questi è senza dubbio significativo il caso in cui si debba controllare il processo di fissione all'interno di un reattore nucleare di una centrale. Molto più semplicemente si può dire che un sistema dotato di azioni di controllo che possono portare a esiti non deterministici non appartiene alla categoria dei sistemi di controllo.

La presente sezione concentra l'interesse su un tipo particolare di elaborazione dei comandi, quello delle azioni automatiche. Queste rivestono particolare interesse in virtù del fatto che con esse si realizza l'automazione nel senso stretto del termine.

8.2.1 Un buon motivo per realizzare azioni automatiche

I sistemi SCADA sono dotati di strumenti che consentono il controllo da parte degli operatori i quali, solitamente, sono in grado di interpretare le informazioni di stato e di costruire con queste una rappresentazione del processo tale da permettere la definizione di adeguate strategie di controllo. In funzione del tipo di evoluzione seguita dal processo gli operatori agiscono con opportuni comandi e *guidano* il processo verso gli stati di evoluzione previsti. Le interazioni tra operatori e sistema avvengono per mezzo dell'interfaccia uomo-macchina e riguardano informazioni di stato e comandi di controllo che possono essere caratterizzati da diversi livelli di complessità. Solitamente per mezzo di questa interfaccia il sistema presenta sintesi rappresentative dello stato attuale del processo proponendo all'operatore un'informazione sufficiente alla determinazione del corretto provvedimento da adottare. Allo stesso modo le azioni di controllo che possono essere impartite dall'operatore vengono realizzate in modo che a un'operazione eseguita corrisponda un insieme di azioni di comando reali in grado di orientare l'evoluzione del processo nella opportuna direzione.

L'esperienza insegna che, ove possibile, l'intervento dell'operatore deve essere evitato e la realizzazione di comandi operatore e rappresentazioni di stato volta a raggiungere il massimo livello di sintesi possibile. Questo metodo consente di ridurre al minimo l'intervento umano ed evitare tutte le conseguenze che questo comporta. Non si tratta di un pregiudizio, o di un giudizio, negativo nei confronti degli individui che operano nel mondo dell'automazione industriale ma dell'esperienza, fatta anche per mezzo di strumenti di indagine appropriati, che mostra con evidenza che di fronte alla necessità di attuare un'azione di controllo la fermezza e l'abilità degli operatori tendono a subire la pressione della responsabilità decisionale. Una tipica manifestazione di quanto detto si ottiene con la misurazione del ritmo cardiaco degli operatori nel corso della loro attività: esso raggiunge e a volte supera i limiti di guardia in corrispondenza dell'attuazione di azioni di controllo. Questo vuol dire che gli operatori, di solito, agiscono in condizioni di pressione psicologica e di sforzo fisico.

Per comprendere meglio l'importanza di queste considerazioni è opportuno fare qualche esempio concreto. In precedenza si è detto della criticità del controllo della fissione all'interno di un reattore nucleare, ora immaginiamo una situazione che può essere considerata del tutto ordinaria nel funzionamento di un reattore. Il controllo della fissione dell'uranio all'interno del reattore avviene per mezzo di barre che vengono introdotte nel reattore con

lo scopo di ridurre l'intensità del processo o di spegnere il reattore. È inimmaginabile lo stress psico-fisico al quale sono stati sottoposti gli operatori della centrale di Cernobyl nei minuti precedenti l'esplosione del reattore il 26 aprile 1986. Un reattore attivo da quasi dieci anni mostra improvvisamente segni di instabilità con crescente intensità dell'attività nucleare, le normali contromisure di regolazione non sono in grado di contenere la reazione e gli operatori procedono allo spegnimento del reattore con l'inserimento delle barre di controllo. L'altissimo livello di formazione degli operatori della centrale non può nulla di fronte all'enormità dell'evento e, benché nel caso specifico sia stato fatto tutto quanto possibile e nel migliore dei modi, le operazioni avvengono in condizioni psico-fisiche estreme. Ma l'esempio non è questo. Piuttosto si dovrebbe pensare a tutti gli operatori che nel mondo hanno espletato, e continuano a farlo, funzioni analoghe a quelle degli *sfortunati* colleghi sovietici in piena consapevolezza della delicatezza del ruolo.

Condizioni di stress sono state riscontrate in attività di controllo caratterizzate da criticità di gran lunga inferiori quali, ad esempio, la gestione di linee di produzione industriali nelle quali i “disastri” sono dell'ordine di *minuti di fermo macchina e conseguente interruzione della produzione*, cioè fenomeni che non comportano pericoli ma soltanto la perdita di piccolissime quote di produzione.

Considerazioni come quelle appena fatte hanno indotto a pensare che in tutti i casi nei quali il sistema è in grado di interpretare uno stato in termini di provvedimenti da prendere, scelte da compiere, comandi da impartire è bene realizzare algoritmi per l'attuazione automatica di azioni di controllo e sollevare gli operatori dall'onere dell'intervento. Questo tipo di scelta consente di lasciare all'operatore tempo e serenità per dedicarsi all'attività di supervisione e approfondire la conoscenza delle caratteristiche del processo. Quest'ultima attività risulta molto preziosa quando si decide di coinvolgere gli operatori nello sviluppo delle funzionalità del sistema SCADA poiché, in ultima analisi, essi sono gli utilizzatori e, conoscendo il processo, hanno una chiara idea di cosa possa aiutarli nel controllo e cosa no.

Naturalmente quanto detto non significa rinunciare al dominio sull'attività del sistema e, quindi, del processo. La stessa azione automatica deve essere subordinata al controllo umano per mezzo di comandi di attivazione e disattivazione e deve essere realizzata in modo che il suo stato di elaborazione e il suo comportamento possano essere adeguatamente osservati per mezzo degli strumenti di supervisione.

8.2.2 Motivi che impongono l'uso di azioni automatiche

La realizzazione del controllo di un processo dipende in modo sostanziale dalla dinamica del processo; essa dipende cioè dalla rapidità con la quale il processo compie transizioni di stato. Dovendo il sistema SCADA controllare l'evoluzione, che si realizza per transizioni di stato, i tempi che caratterizzano il passaggio da uno stato al successivo impongono vincoli alla reattività del sistema. Nei casi in cui i processi controllati seguono percorsi evolutivi lenti rispetto alla capacità di reazione del sistema e degli operatori umani la realizzazione di azioni automatiche è una scelta di opportunità. Nei casi in cui i processi seguono evoluzioni rapide la realizzazione di azioni automatiche diventa una scelta obbligata, l'unico modo per realizzare il controllo. L'attributo "rapide" si riferisce a tempi di transizione di stato che non consentono di realizzare la catena di eventi che dall'acquisizione passa per la rappresentazione, l'interpretazione, la decisione, l'invio di un comando per giungere all'attuazione del comando medesimo. È evidente che transizioni che avvengono in tempi limitati a pochi secondi non lasciano spazi a scelte alternative alla realizzazione di azioni automatiche. In questi casi la dinamica del processo può essere tale da imporre non soltanto la scelta di automatizzare il controllo ma anche le soluzioni tecnologiche per realizzare l'automazione. La dinamica e la complessità del processo impongono, a volte, la realizzazione di azioni automatiche di controllo, meglio di procedure automatiche, per le quali la logica non risiede nel sistema centrale di elaborazione ma presso gli apparati periferici i quali, in funzione delle procedure che debbono essere realizzate, possono consistere di strutture più o meno complesse. Il caso estremo al quale si può giungere è quello del sistema di controllo distribuito nel quale l'intelligenza del sistema è realizzata da strutture periferiche molto complesse e il sistema centrale di elaborazione è destinato a funzioni di supervisione.

Un altro caso nel quale risulta necessario realizzare procedure automatiche di controllo si verifica quando il processo decisionale che conduce dall'analisi dei dati alla determinazione di impartire comandi è molto complesso. Accade, infatti, che il numero di variabili in gioco siano in gran numero e le combinazioni di valori di queste non facilmente controllabili in tempi accettabili da parte di un operatore. In questi casi si può decidere di realizzare calcoli per fornire visioni di sintesi dello stato del sistema e lasciare la decisione all'operatore oppure, scelta preferibile, realizzare le procedure di controllo per via automatica.

8.2.3 Caratteristiche delle azioni automatiche

Presentate le ragioni che conducono alla realizzazione di meccanismi automatici di controllo è possibile procedere alla descrizione delle stesse. Prima di far questo è necessario precisare che la trattazione che segue, in tutta la sua limitatezza (per una trattazione completa si può fare riferimento a pubblicazioni specializzate, vedi [5], [10], [7]), può essere considerata valida sia nel caso di integrazione degli algoritmi di controllo all'interno del sistema di elaborazione che nel caso in cui questi vengano ospitati dalle apparecchiature periferiche di acquisizione. La trattazione consiste nella presentazione in forma di semplici esempi di algoritmi di calcolo basati sui metodi fondamentali di controllo automatico; si tratta degli algoritmi di controllo a retroazione *proporzionale*, *proporzionale derivativo* e *proporzionale integrale derivativo*.

Azione Proporzionale: *P*

Si consideri la realizzazione di un meccanismo di controllo della velocità di un'automobile che sia in grado di lasciare all'automobilista il solo onere di scegliere la velocità desiderata. Esso deve conoscere il valore fissato dall'automobilista e, in base a questo, determinare la quantità di carburante da iniettare nel motore. L'automobile può essere vista così come un processo caratterizzato da un *ingresso*, la quantità di carburante iniettato nel motore, e un *uscita*, la velocità di marcia. Un sistema che abbia lo scopo di regolare la velocità in base al valore fissato dall'automobilista non può far altro che:

1. misurare il valore della velocità attuale
2. confrontare la velocità attuale con quella desiderata dall'automobilista
3. determinare il nuovo livello di iniezione in caso di scostamento tra i due valori

Il sistema di controllo deve ottenere il valore della velocità attuale la quale, per questo motivo, è vista dal sistema come un *ingresso*. Analogamente il livello di iniezione è la variabile che permette al sistema di controllo di attuare la regolazione, è cioè un *uscita*.

Quanto detto è sufficiente a capire il flusso di informazioni e gli strumenti usati dal sistema per attuare il controllo. Ciò che manca è capire come può essere calcolato il corretto livello d'iniezione, quello che permette di imporre all'automobile la velocità desiderata. Una rappresentazione del problema è riportata in figura 8.1; come si può vedere tutto ciò che rimane da determinare è il comportamento dell'algoritmo di controllo. Il primo esempio di algoritmo,

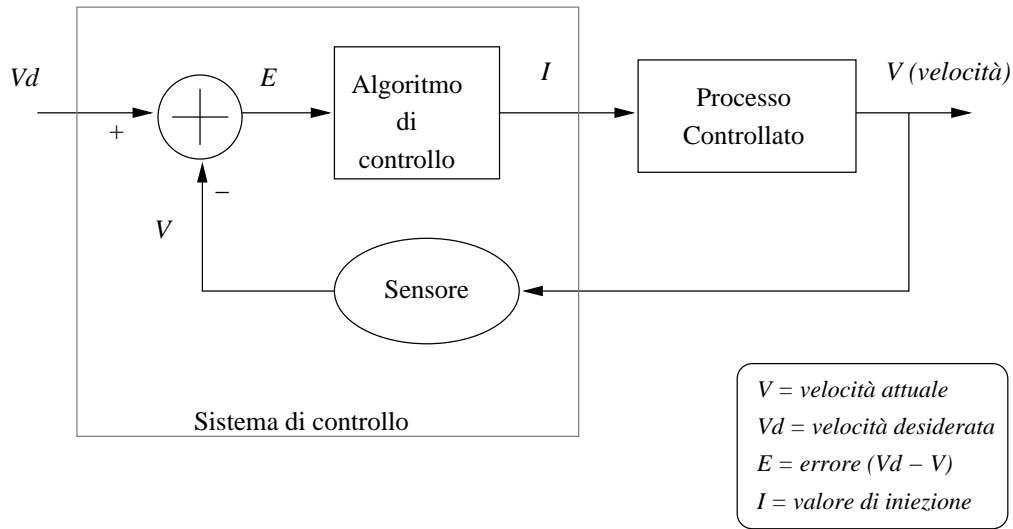


Figura 8.1: Schema a blocchi del problema di controllo della velocità

il più semplice tra quelli trattati, prevede l'attuazione di un controllo detto *proporzionale* in virtù del fatto che il livello di iniezione viene calcolato come prodotto tra il valore acquisito dall'errore e una costante. Il livello di iniezione viene quindi calcolato come:

$$I = K \cdot E \quad (8.1)$$

dove I è il livello di iniezione, E è la differenza tra velocità desiderata e velocità attuale e K è una costante che caratterizza l'intensità dell'erogazione rispetto alla differenza tra velocità attesa e velocità attuale e, al tempo stesso, il rapporto tra velocità e quantità di carburante iniettato. Un controllo di questo tipo comporta un continuo inseguimento della velocità desiderata con continue oscillazioni attorno a tale valore da parte della velocità attuale. In particolare (vedi figura 8.1) accade che fin quando V è minore di Vd il valore di I è maggiore di zero e V tende a crescere mentre quando Vd supera V l'errore E è minore di zero e l'azione di controllo operata da I , anch'esso negativo, ha effetto frenante.

Il controllo proporzionale non ha informazioni relative all'evoluzione della regolazione e, quindi, non può che basarsi sul presente, cioè sul valore attuale dell'errore il quale, per questo, non verrà mai azzerato. Un altro problema di questo controllo consiste nel fatto che non introduce fattori di stabilizzazione rendendosi utile solo nei casi in cui il processo è intrinsecamente stabile.

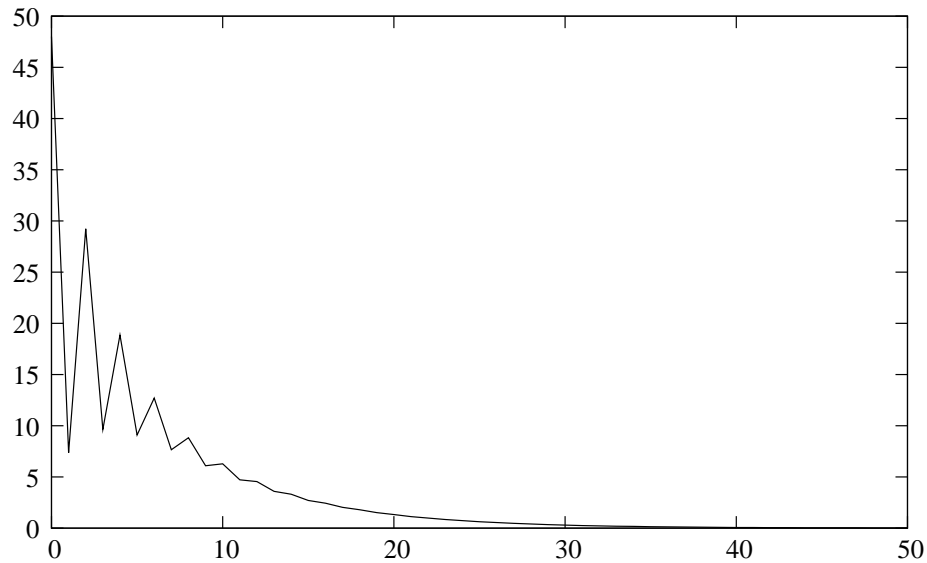


Figura 8.2: Esempio di componente derivativa della grandezza di controllo prodotta da un controllore PD

Azione Proporzionale-Derivativa: *PD*

Nella definizione dell'algoritmo di controllo si può pensare di aggiungere alla componente proporzionale una componente che sia in grado di tenere in conto la rapidità con la quale l'uscita (la velocità attuale misurata dal sensore) varia nel tempo. Una misura della variabilità di una grandezza è data, come noto, dalla derivata nel tempo della medesima. Un algoritmo di controllo contenente una componente proporzionale all'errore e una proporzionale alla derivata dello stesso utilizza la seguente formula di calcolo:

$$I = K_p \cdot E + K_d \cdot \frac{dE}{dt} \quad (8.2)$$

Un'equazione di questo genere viene calcolata tenendo in considerazione il fatto che nel sistema di controllo della velocità la misurazione della velocità attuale non è continua e l'errore può essere trattato come una funzione a dominio discreto (il tempo). La formula si trasforma così nella seguente:

$$I = K_p \cdot E_n + K_d \cdot \frac{E_n - E_{n-1}}{T_n - T_{n-1}} \quad (8.3)$$

e produce valori della grandezza di controllo caratterizzati da una componente derivativa che ha un andamento del tipo mostrato in figura 8.2. Un controllore di questo tipo è detto *proporzionale-derivativo* o *PD*.

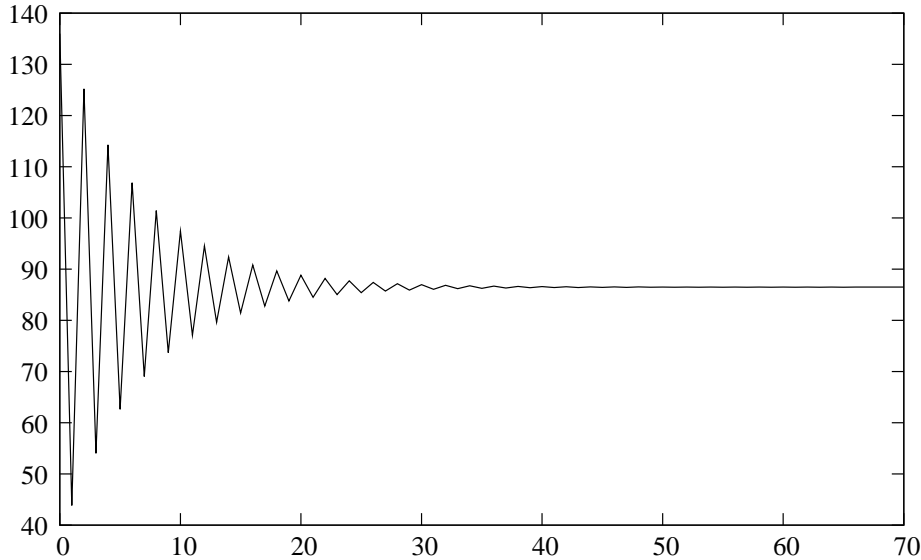


Figura 8.3: Esempio di andamento della grandezza di controllo prodotta da un controllore PID

Azione Proporzionale-Integrale-Derivativa: *PID*

Dopo aver introdotto la componente derivativa al fine di rendere il controllore in grado di rispondere prontamente a forti variazioni dell'uscita è lecito domandarsi se sia o meno possibile realizzare un controllore che, oltre a ciò, riesca a tenere memoria della “storia” dell'evoluzione del sistema per produrre un controllo che a lungo termine comporti l'annullamento dell'errore. Questo è possibile introducendo nella formula di calcolo una componente integrativa poiché è proprio l'operazione di integrazione quella che permette di conoscere i trascorsi di una grandezza. La formula che si utilizza in questo caso, e che rappresenta il controllore *proporzionale-derivativo-integrale* o *PID*, è la seguente:

$$I = K_p \cdot E + K_d \cdot \frac{dE}{dt} + K_i \cdot \int E(t) \cdot dt \quad (8.4)$$

Per tradurre questa formula in algoritmo di calcolo è necessario trasformarla derivandola membro a membro:

$$\frac{dI}{dt} = K_p \cdot \frac{dE}{dt} + K_d \cdot \frac{d^2E}{dt^2} + K_i E \quad (8.5)$$

per poi considerarne la versione approssimata nel dominio discreto:

$$\frac{I_n - I_{n-1}}{T_n - T_{n-1}} = K_p \cdot \frac{E_n - E_{n-1}}{T_n - T_{n-1}} + K_d \cdot \frac{(E_n - E_{n-1}) - (E_{n-1} - E_{n-2})}{(T_n - T_{n-1})^2} + K_i \cdot E_n \quad (8.6)$$

Essendo $T_n - T_{n-1}$ il periodo di campionamento dell'uscita la formula può essere riscritta come:

$$I_n = I_{n-1} + K_p \cdot (E_n - E_{n-1}) + K_d \cdot \frac{(E_n - 2 \cdot E_{n-1} + E_{n-2})}{T} + K_i \cdot E_n \cdot T \quad (8.7)$$

La figura 8.3 riporta un andamento tipico della grandezza di controllo prodotta da un controllore di tipo *PID*. È possibile notare che dopo un periodo di tempo nel quale le tre componenti di calcolo del controllore producono un andamento oscillatorio attorno al valore finale, cioè al valore che conduce a una velocità attuale pari a quella desiderata, l'oscillazione si annulla e il controllo va a regime come sperato. L'ampiezza, la rapidità delle variazioni e l'andamento dello smorzamento delle oscillazioni dipende, oltre che dalle caratteristiche del processo controllato, dalla scelta fatta per i parametri K_p , K_d e K_i .

8.2.4 Algoritmi e procedure

Per concludere è importante notare che nel gergo dei sistemi SCADA espressioni quali “logica di controllo” o “algoritmo di controllo automatico” non si riferiscono soltanto alla realizzazione di controllori per mezzo degli strumenti di progettazione resi disponibili dalle discipline ingegneristiche che si interessano ai problemi della stabilità e del controllo. Queste stesse espressioni si utilizzano quando la realizzazione di un sistema SCADA comporta l'attivazione di operazioni pianificate caratterizzate da una certa complessità o subordinate ad algoritmi di decisione che, però, nulla hanno in comune con il problema del controllo come finora presentato. Probabilmente l'uso di queste espressioni anche nei casi in cui in realtà ci si riferisce a procedure e non ad algoritmi di controllo è dovuto al fatto che la loro realizzazione, benchè apparentemente di natura più “prosaica”, può risultare per diverse ragioni molto complessa.

Può accadere che una procedura, intrinsecamente semplice in termini di algoritmo da realizzare, richieda tempi di esecuzione che portano ai limiti la capacità di elaborazione delle infrastrutture tecnologiche disponibili. Allo stesso modo accade che una procedura debba confrontarsi con problemi di sincronizzazione tra grandezze distinte costringendo a elaborazioni di supporto a quelle effettivamente dedicate al problema. Un ultimo esempio può essere fatto considerando il caso di un sistema distribuito nel quale l'attività di un apparato periferico dipende da quella di altri apparati del sistema; in questo caso il sistema di elaborazione deve ospitare procedure in grado di coordinare l'attività delle apparecchiature di acquisizione realizzando, di concerto con la periferia, l'intelligenza del sistema.

Come detto molti di questi problemi non si affrontano con gli strumenti dei “controlli automatici” ma, come se lo fossero, il gergo dei sistemi SCADA li qualifica, non del tutto a torto, come risolvibili per mezzo di “logiche” o “algoritmi” di controllo.

8.3 Calcoli in linea

Un sistema SCADA, per quanto finora osservato, utilizza, come fonte primaria di informazione, i dati acquisiti dal campo attraverso gli apparati di acquisizione dati e trattati con le modalità precedentemente descritte. Queste informazioni sono necessarie per avere un’immagine dello stato corrente del processo controllato ma non sempre sufficienti per restituire un’immagine del processo che sia la più precisa possibile e che permetta un immediato riconoscimento dello stato corrente di funzionamento del processo stesso.

I dati primari possono descrivere fedelmente una parte del processo controllato ma per avere un’informazione globale del processo potrebbe essere necessario dover valutare più parametri, magari effettuando anche delle correlazioni tra gli stessi per poter determinare se il processo sia o meno sotto controllo. Queste operazioni possono essere svolte dagli operatori, ma spesso questo comporta che ogni operatore potrebbe trarre conclusioni diverse pur valutando una stessa serie di dati e valori uguali degli stessi. Questa variabilità di conclusioni, escludendo l’errore umano che comunque può essere sempre presente, potrebbe essere determinato da conoscenze ed esperienze diverse proprie di ogni operatore. Sebbene in alcuni casi l’apporto delle esperienze degli operatori sia fondamentale per poter affrontare situazioni contingenti non facilmente risolvibili se non basandosi sull’esperienza, un sistema di controllo non può limitarsi a utilizzare l’esperienza degli operatori per determinare il miglior controllo possibile sul processo. Un sistema di controllo deve essere in grado di fornire tutti gli strumenti che garantiscano, laddove è richiesto il supporto alla decisione da parte di un operatore, la risposta più adatta alla situazione. È compito del sistema SCADA integrare le informazioni messe a disposizione dell’operatore attraverso i dati primari, con una serie di informazioni che guidino l’operatore stesso verso la comprensione dello stato di funzionamento del processo ed eventualmente verso le cause che ne hanno compromesso la correttezza. In questo modo l’operatore è guidato verso la decisione da parte del sistema e gli errori che egli può commettere in questa fase possono essere ridotti al minimo.

La definizione delle informazioni che il sistema SCADA deve generare e la modalità di generazione delle stesse saranno frutto delle esperienze degli

operatori. Si possono quindi valutare a priori possibili stati di funzionamento del processo e creare modelli di comportamento sperimentali che aiutino nell'individuazione delle informazioni fondamentali per la rappresentazione del processo. L'adozione di algoritmi certi e sempre uguali per la produzione di queste informazioni garantisce che esse siano espressione massima di tutte le esperienze che si hanno sul processo. La definizione dei dati calcolati solitamente viene fatta in fase di configurazione del sistema quando sono definiti anche gli algoritmi necessari alla produzione del valore di ogni singolo dato. In alcuni sistemi SCADA complessi è presente la possibilità di definire un insieme di dati da calcolare il cui algoritmo può essere definito e modificato durante l'utilizzo del sistema stesso. Questa capacità del sistema apre le porte alla possibilità di rendere dinamico il comportamento del sistema SCADA in modo da farlo evolvere con l'evoluzione delle esigenze del processo e delle esperienze degli operatori.

Tutte queste informazioni permettono all'operatore di avere una serie di dati da valutare per conoscere meglio sia lo stato corrente del processo che lo stato immediatamente precedente all'attuale e stimare la possibile evoluzione nel futuro prossimo del sistema. Questa serie di operazioni è definita come "calcoli in linea" proprio perché la loro elaborazione avviene contestualmente all'elaborazione dei dati primari e fornisce un insieme di dati che interessa intervalli di tempo limitati. Per informazioni statistiche che abbraccino intervalli più lunghi o che richiedano elaborazioni più complesse, si faccia riferimento a quanto descritto nella sezione che tratta l'analisi dei dati in tempo differito.

In generale le informazioni che un sistema SCADA deve essere in grado di generare possono essere suddivise nei seguenti gruppi:

- informazioni di tipo aggregato
- informazioni di tipo logico
- informazioni di tipo statistico

8.3.1 Informazioni di tipo aggregato

Le informazioni di tipo aggregato sono costituite da quella serie di dati che derivano il loro valore dai valori di insiemi di dati primari o da altre informazioni aggregate. Ad esempio in un impianto di produzione elettrica composto da più generatori potrebbe essere comodo avere a disposizione in un unico dato la somma di tutte le potenze elettriche correnti prelevate da ciascun generatore. La rappresentazione di questo dato in una pagina riassuntiva

dello stato dell'impianto fornisce immediatamente all'operatore un'indicazione del funzionamento dell'impianto stesso. Esempi più complessi possono essere fatti in relazione a complessità di processi da controllare crescenti ma, in generale, la richiesta che si può fare a un sistema SCADA è la capacità di esprimere informazioni come risultato di algoritmi di aggregazione dei valori.

Operazioni e funzioni matematiche sono quindi necessarie per la generazione di dati aggregati e quelle usate più frequentemente sono:

- operazioni elementari (somma, differenza, moltiplicazione, divisione)
- elevazione a potenza
- estrazione di radice

8.3.2 Informazioni logiche

Le informazioni logiche che un sistema SCADA può generare corrispondono a quella serie di dati di tipo digitale che condensano in una serie di stati logici la valutazione degli stati di un insieme di dati primari o altri dati calcolati. In genere queste informazioni permettono di avere un'informazione equivalente ad una serie di informazioni che ne riassume il significato. Si faccia riferimento all'esempio dello scalo ferroviario di (cfr. sezione 7.2) che illustra chiaramente quanto un'unica informazione possa aiutare l'operatore nella scelta al momento di prendere una decisione.

La lista degli operatori logici più utilizzati per la generazione di questo tipo di dati è riportato nell'elenco seguente:

- operatore logico AND
- operatore logico OR
- operatore logico NOT

8.3.3 Informazioni statistiche

Le informazioni statistiche che un sistema SCADA può generare a partire da dati primari o dati calcolati costituiscono un insieme di informazioni che permettono di ottenere indicazioni circa l'evoluzione temporale del valore di un dato. Si pensi ad esempio alla necessità di conoscere non tanto il valore corrente di una grandezza, quanto la variazione nel tempo in modo da prevederne l'andamento nell'immediato futuro. A questa necessità risponde la possibilità di generare un dato calcolato che esprima il valore della derivata

nel tempo del valore del dato primario. Analogamente, valori che hanno variazioni ripetute nel tempo possono fornire un'indicazione migliore se se ne calcola la media in un certo intervallo. Per quanto riguarda dati di tipo digitale può essere comodo conoscere il numero di transizioni di stato nel tempo ed il tempo di permanenza medio in un dato stato.

I calcoli statistici sono sempre caratterizzati dall'applicazione di una funzione nel dominio del tempo. Le funzioni più utilizzate per la generazione di questo tipo di dati sono:

- calcolo del valore medio
- calcolo dell'integrale
- calcolo della derivata
- calcolo della distribuzione
- calcolo del numero di transizioni in un determinato stato logico
- calcolo del tempo di permanenza in un determinato stato logico

Capitolo 9

Interfaccia uomo-macchina

9.1 Caratteristiche

In un sistema SCADA la parte di interfaccia del sistema con l'operatore prende il nome di *interfaccia uomo-macchina*. A questo componente è demandata la gestione delle interazioni con l'uomo e quindi nella progettazione dello stesso si devono tenere in considerazione aspetti che riguardano la comunicazione con un essere umano piuttosto che caratteristiche di ottimizzazione tipiche delle macchine utilizzate. Se un calcolatore è insensibile, ad esempio, all'ordinamento di un insieme di informazioni un operatore umano trae grande giovamento dall'uso di elenchi ordinati (magari in ordine alfabetico).

Tutto quello che viene progettato per la realizzazione dell'interfaccia uomo macchina tiene conto del fatto che l'utente di questo componente è l'uomo e al centro dell'attenzione ci devono essere le sue esigenze. Non solamente gli aspetti più direttamente collegati alla restituzione delle informazioni all'utente, quindi, ma anche ogni aspetto che possa facilitare il compito dell'uomo nell'interazione con il sistema. Il sistema SCADA deve essere solo un mezzo per permettere all'uomo di gestire e controllare un processo e in questa attività esso deve risultare il più possibile "trasparente" per gli attori veri che sono l'operatore e il processo controllato. Responsabilità dell'interfaccia uomo-macchina è quella di agevolare il compito dell'operatore umano: più facile e intuitiva risulta l'interazione con il sistema SCADA, migliore sarà il risultato.

Curare l'usabilità del sistema SCADA corrisponde a mettere a proprio agio gli operatori anche con il secondo fine di ottenere un ampio utilizzo del sistema che sarà visto dagli operatori come un aiuto nello svolgimento delle attività di tutti i giorni. L'agevolazione di queste operazioni contribuisce a creare un senso di fiducia negli operatori tale che anche in situazioni critiche

essi potranno fidarsi delle risposte che il sistema fornisce, limitando situazioni di stress psicologico certamente non auspicabili in momenti critici. Anche la cura della semplicità delle operazioni e dei dispositivi attraverso i quali si attua l'interfaccia è motivo di studio per rendere efficace l'interazione con gli operatori. La riduzione e la semplificazione delle operazioni, l'automazione delle operazioni ripetitive, l'utilizzo di dispositivi ergonomici sono elementi che possono determinare il successo dell'adozione di un sistema SCADA.

Non si dimentichi che il processo di automazione delle aziende che vede nel sistema SCADA uno dei suoi strumenti fondamentali è spesso accompagnato da una diminuzione di impegno per il personale che proprio dal sistema di automazione si trova sostituito nello svolgere i compiti di controllo. Questo non sempre si risolve in una riduzione del personale che può essere ricollocato o riqualificato (disfarsi di personale qualificato ed esperto dovrebbe sempre essere motivo di preoccupazione per l'azienda) ma l'adozione di un sistema SCADA viene spesso vista con diffidenza da parte del personale. Questo anche per il fatto che una scelta di questo genere comporta un cambiamento di abitudini e una possibile perdita delle sicurezze accumulate nel corso della vita lavorativa. La diffidenza nei confronti delle conseguenze che l'adozione di un sistema di automazione comporta spesso si manifesta nella resistenza a questo tipo di novità e nel tentativo, nei casi peggiori, di denigrare le caratteristiche del sistema stesso al fine di giustificarne il mancato utilizzo. Anche per questi motivi un sistema che agevoli le operazioni di interazione con gli operatori si candida al successo più di altri in quanto in grado di far apprezzare gli aspetti positivi legati al suo uso.

9.2 Funzioni

La funzione principale dell'interfaccia uomo-macchina, come detto, è la gestione delle interazioni tra il sistema SCADA e gli operatori. Le informazioni che possono essere scambiate tra questi due attori sono distinguibili in:

- presentazione dei dati
- gestione dei comandi operatore

Come si vedrà nel dettaglio, spesso le tecniche utilizzate nella realizzazione di queste funzioni tengono presente quanto già detto riguardo le caratteristiche di semplicità e usabilità che sono alla base di questo componente.

9.2.1 Presentazione dei dati

La funzione di presentazione dei dati permette all'operatore di essere informato sullo stato del processo controllato attraverso la visualizzazione di una serie di informazioni (acquisite o calcolate dal sistema). La visualizzazione di queste informazioni può essere realizzata per mezzo delle seguenti modalità:

- rappresentazioni schematiche
- rappresentazioni tabellari
- diagrammi temporali

Rappresentazioni schematiche

L'interfaccia uomo-macchina deve permettere agli operatori residenti in una sala destinata al controllo di avere una “vista” sullo stato del processo. Il metodo usato per ottenere questa condizione è la realizzazione di una rappresentazione schematica degli impianti. Questa rappresentazione può essere sviluppata utilizzando diverse tecniche e nel corso degli anni ha subito un'evoluzione significativa, anche grazie al progresso tecnologico che ha messo a disposizione dei progettisti di sistemi SCADA possibilità e potenze di elaborazione via via crescenti.

Inizialmente la tendenza è stata quella di avere un “quadro mimico” a parete che rappresentasse tutto il processo suddiviso nelle sue parti principali. La necessità di rappresentare tutto il processo in un'unica vista ha comportato la schematizzazione dello stesso e la condensazione delle informazioni in pochi dati. Per ottenere completezza e chiarezza d'informazione da schemi caratterizzati da un alto livello di sintesi sono state definite rappresentazioni simboliche caratteristiche degli organi di campo e tipologie ristrette di presentazione delle informazioni associate. Ad esempio accanto al simbolo rappresentativo di un motore una lampadina stava a indicare lo stato di esercizio (in marcia se accesa o in arresto se spenta).

In figura 9.1 è riportato un esempio di schema utilizzato per la realizzazione dei quadri mimici. Osservando la figura è possibile notare che una rappresentazione del processo di questo tipo pur essendo corretta corrisponde ad un insieme incompleto di informazioni in quanto essa realizza una “vista” astratta di alto livello. D'altra parte l'aver a disposizione troppe informazioni contemporaneamente in un quadro mimico può comportare difficoltà nell'interpretazione da parte degli operatori. Affinché un operatore operi correttamente e tempestivamente è necessario che le informazioni che lo raggiungono siano poche ma significative e associate in modo univoco all'organo

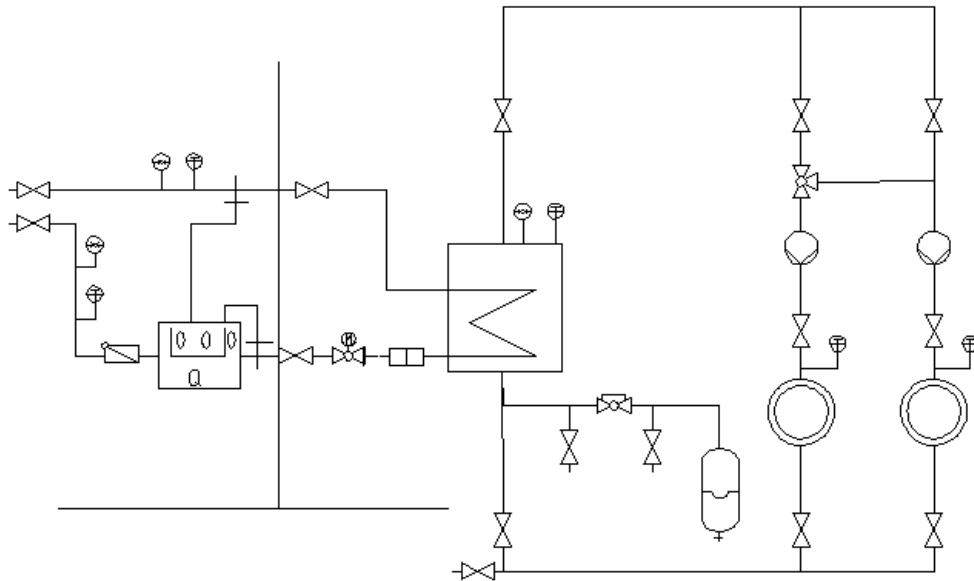


Figura 9.1: Esempio di rappresentazione tipica di un quadro mimico

corrispondente in modo da non introdurre ambiguità. Ecco perché ogni organo di campo è stato schematizzato con un simbolo che da solo consente di comprenderne la natura. La rappresentazione simbolica del processo controllato è stata regolata dalla nascita di simboli standardizzati che coprono la maggior parte delle realtà del mondo dell'automazione. Uno degli enti più attivi nella generazione di standard per la rappresentazione dei processi controllati è l'ISA (*International Standard Association*) a cui si deve la definizione dei simboli che prendono il suo nome.

L'evoluzione del quadro mimico è stato il "quadro a mosaico" che ha portato al superamento del problema dei costi da affrontare in caso di modifica degli schematici in corrispondenza dell'evoluzione delle realtà impiantistiche. Il passo successivo è stato compiuto con l'introduzione dei calcolatori. Questi hanno consentito la rappresentazione per mezzo degli schermi delle informazioni fino ad allora contenute dal quadro mimico.

L'introduzione dei computer ha dato un contributo fondamentale all'impegno profuso nella direzione del potenziamento delle funzionalità dell'interfaccia. Con l'uso del computer è stato possibile disporre di più pagine video per la rappresentazione del processo, associare a ogni pagina informazioni diverse permettendo di suddividere il processo in più sezioni e, quindi, avere rappresentazioni sempre più dettagliate. È divenuto possibile realizzare pagine sommario corrispondenti ai vecchi quadri mimici e poi suddividerle in aree specifiche per ogni impianto. Richiamando la pagina di un partico-

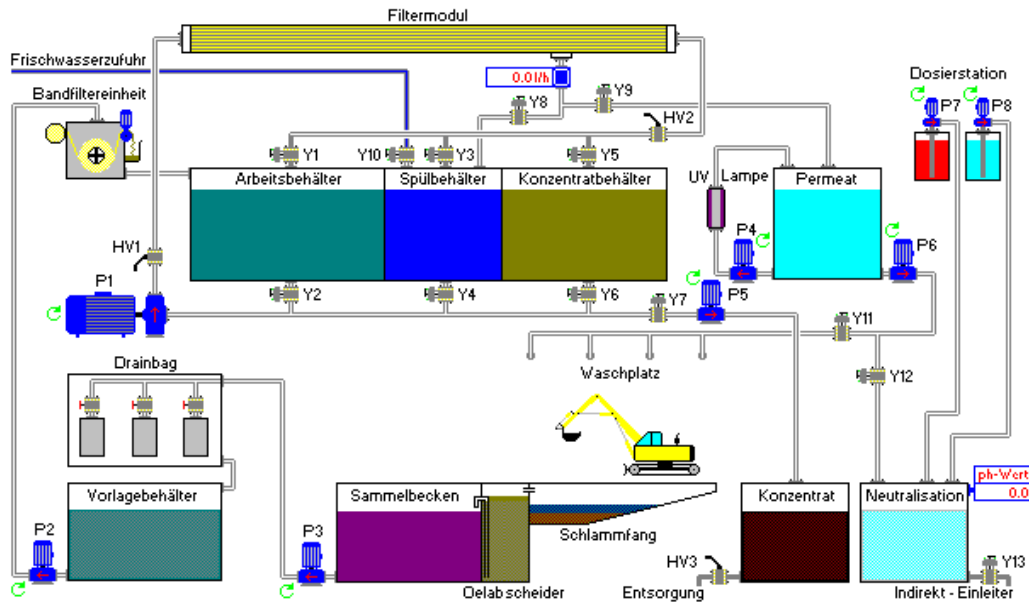


Figura 9.2: Esempio di rappresentazione del processo tipica di una pagina video

lare impianto si può visualizzare un dettaglio maggiore del dato impianto con informazioni che al livello superiore non vengono mostrate. Si può procedere con questa tecnica per passi successivi fino a ottenere un livello di dettaglio che permette a un operatore di concentrarsi su un singolo organo e ottenere tutte le informazioni delle quali il sistema dispone. Queste caratteristiche portano a un'efficacia dell'attività di supervisione altrimenti non raggiungibile poiché rendono possibili nuovi usi dell'interfaccia (si pensi al caso della segnalazione a una squadra di manutenzione del malfunzionamento di un organo di campo: una presentazione dettagliata dello stato dell'organo permette di realizzare un intervento efficace e tempestivo poiché una parte dell'analisi del malfunzionamento può essere condotta in sede di supervisione).

Sono state sviluppate tecniche che permettono di avere in vista su di un singolo schermo più immagini contemporaneamente, effettuare operazioni di ingrandimento o navigazione della singola pagina con contemporanea modifica delle informazioni mostrate, ecc. Ciò che non è cambiato nel passaggio dai quadri mimici agli schematici realizzati con il calcolatore sono le caratteristiche di immediatezza nella lettura delle rappresentazioni grafiche, cioè l'usabilità dell'interfaccia.

Un esempio di visualizzazione del processo o di parte di esso realizzata per mezzo degli strumenti di rappresentazione forniti dalle piattaforme software di sviluppo dei sistemi SCADA è riportata in figura 9.2 (cfr. [13]).

Rappresentazioni tabellari

Quando un insieme di informazioni collezionata da un sistema SCADA corrisponde a una serie di valori che non è conveniente inserire in una rappresentazione schematica può essere d'ausilio la rappresentazione di tipo tabellare. Questa modalità di rappresentazione permette di inserire in una tabella un insieme di valori tra loro correlati. È utile far uso di tabelle nei casi in cui si debba mettere in relazione due valori prelevati in punti diversi dell'impianto, oppure se si deve confrontare un valore con i limiti di funzionamento della grandezza che il valore rappresenta, o ancora se si vuole mostrare in un'unica pagina una serie di valori caratteristici del processo che ne diano una visione di immediata interpretazione.

Come modalità di rappresentazione si differenzia sostanzialmente dalla precedente perché riservata a operatori esperti che hanno una conoscenza dettagliata del processo e sono in grado di individuare un sottoinsieme di grandezze da osservare per avere un'idea dello stato di funzionamento corrente. Rispetto alla rappresentazione schematica si perde infatti la capacità di associare una grandezza al punto di prelievo della stessa; per contro un intero processo può essere tenuto sotto controllo da una serie di dati contenuti in un'unica pagina.

Diagrammi temporali

La capacità di rappresentare informazioni in diagrammi temporali offerta dall'interfaccia uomo-macchina di un sistema SCADA è una delle funzionalità più apprezzate da parte degli operatori. Avere la possibilità di inserire in un grafico tempo-valore una serie di dati significativi che danno una rappresentazione dello stato di funzionamento del processo controllato permette di avere informazioni sia sullo stato corrente che sull'evoluzione avvenuta nell'immediato pregresso, consentendo così l'elaborazione di un'idea su ciò che potrebbe avvenire nel prossimo futuro.

Quando si può visualizzare l'andamento nel tempo di un dato il grafico che ne risulta può avere un andamento che evoca curve tipiche che permettono di conoscere l'evoluzione del dato stesso. Tale andamento raramente corrisponde a quello di una funzione matematica nota, semplice o complessa che sia, ma nella maggior parte dei casi presenta elementi caratteristici che ri-

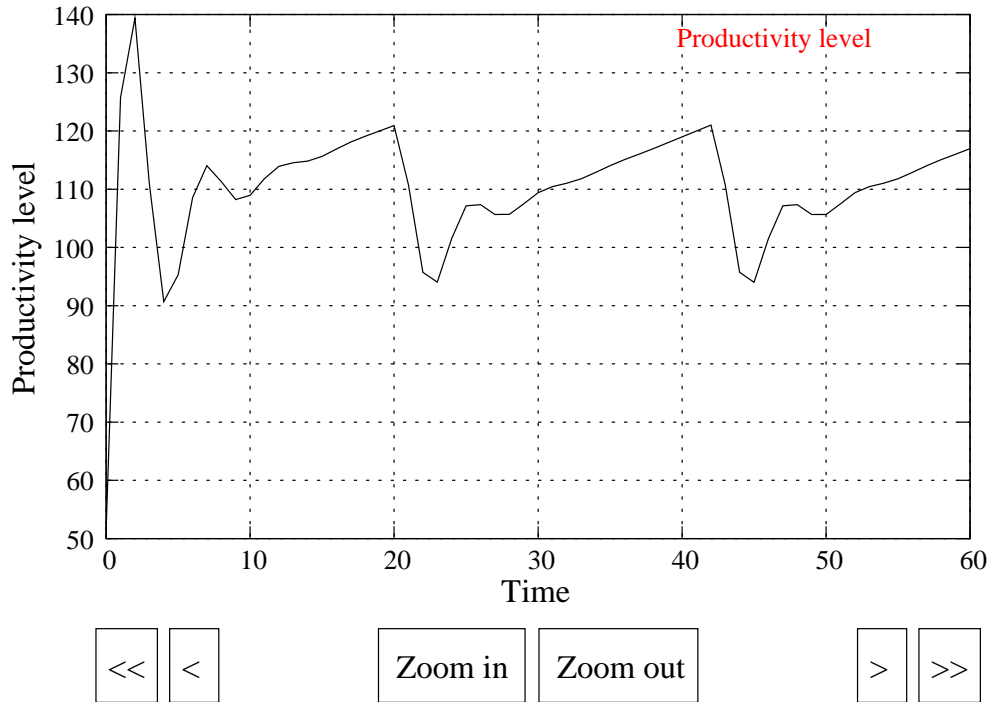


Figura 9.3: Esempio di diagramma valore-tempo di grandezze rappresentative del processo

chiamano alla memoria dell'operatore un comportamento conosciuto, quindi in qualche misura interpretabile. Non è raro vedere operatori di “sala controllo” che gestiscono processi anche complessi per mezzo di un insieme ristretto di diagrammi temporali costruiti su variabili fondamentali opportunamente scelte.

In alcuni sistemi SCADA una delle funzioni richieste è quella di seguire un certo comportamento preventivamente definito nell'evoluzione delle grandezze controllate. Niente di meglio che avere a disposizione in un unico diagramma temporale il valore di riferimento pianificato per la grandezza d'interesse e il suo valore reale. L'osservazione del diagramma permette all'operatore di sapere con impagabile immediatezza se il sistema SCADA sta rispondendo secondo le aspettative o se invece sono necessarie manovre per riportare sotto controllo il processo.

Gli strumenti di rappresentazione diagrammatica delle grandezze d'interesse hanno un aspetto simile a quello mostrato in figura 9.3.

9.2.2 Gestione dei comandi operatore

Una parte fondamentale dei sistemi SCADA è rappresentata dalla possibilità di inviare comandi. Sono già state trattate in precedenza le differenze tra comandi manuali (impartiti dagli operatori) e comandi automatici (ai quali provvede autonomamente il sistema). Questa sezione contiene una trattazione del supporto fornito dall'interfaccia uomo-macchina ad un operatore che si trovi a dover inviare comandi.

L'operazione di invio di un comando è un momento critico per l'operatore poichè richiede la determinazione di una procedura di controllo da adottare, l'attuazione di un'azione di condizionamento del processo controllato e la verifica degli effetti sortiti. Tutte le fasi della procedura di comando sono importanti per l'ottenimento di risultati positivi e l'interfaccia uomo-macchina deve fornire supporto a ognuna di queste.

Quando inviare un comando

L'attribuzione della responsabilità di valutare quando sia il momento opportuno per impartire un comando può portare a un impegno esclusivo dell'operatore oppure a una collaborazione tra operatore e sistema, essendo quest'ultimo chiamato a dare un contributo al processo decisionale.

Nel primo caso l'operatore, in base all'esperienza maturata nello svolgimento dell'attività di controllo o a piani di lavoro definiti, impartisce comandi senza supporto da parte del sistema che, in questo caso, opera come mero esecutore. Nel secondo caso il sistema aiuta l'operatore nella determinazione di una scelta di controllo e, perché no, si comporta da guida nella fase di esecuzione.

È noto che un operatore che si trovi a dover eseguire un'azione di comando è sottoposto a una significativa pressione psicologica. Se a questo si aggiunge anche la responsabilità di prendere la decisione di dover attuare il comando, è facile immaginare le possibili conseguenze negative frutto di tale stress. Un sistema SCADA che sia in grado di agevolare sia l'operazione di determinazione del momento opportuno per l'invio di un comando, sia le operazioni di esecuzione del comando, contribuisce a ridurre la pericolosità dell'attività di controllo e, quindi, ad accrescere la sicurezza dell'intero processo.

In tutti i casi in cui il sistema può essere in grado di suggerire decisioni all'operatore esso dovrebbe farlo. Ogni volta che l'operatore dovesse manifestare l'intenzione di attuare una procedura di comando il sistema dovrebbe chiederne conferma per evitare azioni intempestive. Per tutti i comandi che prevedono sequenze di operazioni facilmente determinabili il sistema dovrebbe

be provvedere a eseguirle autonomamente lasciando all'operatore il solo onere dell'avvio della procedura. In generale è possibile dire che l'aiuto che il sistema fornisce all'operatore si rivela fondamentale per l'innalzamento del livello di qualità e di sicurezza con la quale viene condotta la gestione del processo controllato.

Per assurdo si dovrebbe sempre pensare a quanto agevole sarebbe il compito di un operatore che disponesse di un sistema capace di prendere tutte le decisioni di comando in sua vece. Proponendo una sequenza di domande in corrispondenza di azioni da impartire il sistema lascerebbe all'operatore il solo onere di selezionare, quando necessario, un'opzione tra le poche plausibili presentate come alternativa a una prescelta. Ad assicurare la conservazione del controllo sul processo l'ultimo livello di giudizio rimarrebbe comunque agli operatori, ma le reazioni all'evoluzione del processo sarebbero guidate direttamente dall'intelligenza del sistema. L'operatore potrebbe avere come unica interfaccia di comando un "pulsante" (*il pulsante*) con il quale manifestare la sua intenzione di seguire o meno il consiglio del sistema. Ad esempio il sistema potrebbe porre domande del tipo: "La temperatura del trasformatore TR-1 ha superato il limite superiore. Attivo scambio TR-1 con TR-2?". A queste l'operatore potrebbe rispondere affermativamente semplicemente premendo il pulsante entro un certo intervallo di "timeout".

Attivazione di un comando

L'invio di un comando viene attivato dall'operatore agendo su oggetti di rappresentazione grafica che richiamano alla mente i dispositivi che l'operatore si troverebbe a manipolare nella realtà se dovesse attuare il comando direttamente sull'organo controllato. I simboli utilizzati sono in genere pulsanti, bottoni, manopole che danno l'effetto, anche con l'animazione che ne simula la pressione o il movimento, dell'avvenuta attivazione del comando. Più questi oggetti si comportano in maniera simile a quanto fatto dagli oggetti reali, maggiore è la convinzione per un operatore di aver effettivamente agito sull'organo da controllare.

Poiché l'attivazione di un comando è un'operazione potenzialmente pericolosa per il processo controllato, il sistema SCADA deve essere progettato per impedire che comandi indesiderati possano essere impartiti. Per far questo generalmente si utilizzano due tecniche: suddivisione dei compiti in base al ruolo degli operatori, richiesta di conferma dell'operazione al momento della sua attivazione.

La prima tecnica si realizza già a livello di configurazione del sistema SCADA. Si definisce un insieme di ruoli operativi e si associano ad ogni

ruolo le operazioni che possono essere compiute e quelle vietate. Definendo poi un profilo per ogni operatore che interagisce con il sistema, all'interno del quale è compreso il ruolo, automaticamente si stabilisce quali comandi un operatore può impartire e quali gli sono invece interdetti.

Ogni volta che un comando viene richiesto da un operatore il sistema controlla se l'operatore ha i presupposti per poter inviare il comando (meglio sarebbe se i comandi non fossero attivabili dagli operatori che non hanno la possibilità di inviarli). Una volta che questo controllo abbia dato esito positivo il sistema dovrebbe chiedere conferma della volontà di eseguire il comando richiesto. In questo modo l'operatore si troverebbe costretto a una doppia operazione per l'invio di un comando; solitamente si ritiene che questa tecnica sia sufficiente a escludere l'invio di comandi involontari. Per sistemi o comandi per i quali la volontà sia da verificare con certezza maggiore si possono prevedere procedure di complessità via via maggiori, in grado di assicurare l'identità dell'operatore sull'inoltro della richiesta (ad esempio introduzione di password, password caratterizzate da validità limitata nel tempo, ecc.).

Verifica dell'esecuzione di un comando

All'azione deve seguire una risposta da parte del sistema SCADA che mostri se il comando ha realmente prodotto gli effetti desiderati. Non è mai buona regola lasciare chi esegue un comando nell'incertezza rispetto all'avenuta esecuzione dello stesso. È bene ricordare che un comando impartito a bordo dell'organo manovrato restituisce immediatamente informazioni di esito percepite dai sensi dell'operatore in termini di rumori e movimenti tipici o atipici. Quando il comando viene inviato da una sala controllo non si può avere percezione della reale esecuzione della manovra richiesta. In questo caso è bene che il sistema SCADA mostri all'operatore almeno due stati: il sistema ha ricevuto il comando e sta procedendo all'esecuzione, il risultato dell'esecuzione del comando.

Ogni volta che l'operatore esegue un comando il sistema deve mostrare il fatto che lo ha preso in carico con segnalazioni del tipo "comando in corso" oppure con una modifica del simbolo grafico utilizzato. Quando il comando è stato eseguito il sistema deve riportare lo stato di avvenuta esecuzione, sia in caso di successo che in caso di fallimento. Per questo scopo potrebbero essere utilizzati messaggi simili a quello precedente, "comando eseguito" o "comando fallito", oppure rappresentazioni grafiche convenzionali. Nella definizione di come il sistema risponde alla richiesta di un comando da parte di un operatore si deve ricordare che un'informazione sintetica giunge con mag-

giore chiarezza all'operatore. Spesso l'utilizzo di una convenzione simbolica o luminosa fornisce un'indicazione migliore rispetto a una scritta che potrebbe risultare poco chiara o generica. Si pensi ad esempio alla necessità per un operatore di inviare più comandi in sequenza, oppure far corrispondere a un'unica azione l'invio di più comandi fisici. Avere una rappresentazione grafica dello stato di ogni singolo comando impartito, magari associato all'organo bersaglio, sicuramente corrisponde ad una più chiara fotografia dello stato corrente dei comandi eseguiti.

9.3 Evoluzione

Quanto descritto finora in questo capitolo riguarda le interfacce di interazione tra uomo e macchina che solitamente si trovano in un sistema SCADA. Al giorno d'oggi la maggior parte dei sistemi SCADA viene realizzato prevedendo delle postazioni operatore dotate di schermo, tastiera e dispositivo di puntamento (mouse o track-ball) che costituiscono l'insieme minimo sufficiente per permettere a un operatore di svolgere i normali compiti. A questa architettura a volte si accompagna un quadro mimico riassuntivo dell'intero processo in grado di rappresentare con un insieme ristretto di informazioni quanto necessario per avere un'idea dello stato del processo. Il quadro mimico può essere realizzato con tecniche quali quadri a mosaico oppure con proiettori a parete che riportano le stesse pagine video che sono visibili sul sistema.

Sebbene queste interfacce siano sufficienti per avere la possibilità di interagire con il sistema SCADA, in alcuni casi esse non rispondono completamente alle necessità di chi è demandato a controllare il processo. Non sempre infatti è richiesta una presenza continua degli operatori in "sala controllo", perchè il processo controllato non è così importante o pericoloso oppure perchè c'è la necessità di avere più punti di accesso alle informazioni collezionate dal sistema.

Sulla base di queste considerazioni è possibile introdurre un elemento giudicato come importante strumento di evoluzione dei sistemi SCADA tradizionali. Sempre più spesso le consuete interfacce videografiche vengono affiancate da interfacce che permettono di essere utilizzate da parte di operatori che non risiedono in una sala controllo. L'evoluzione delle tecnologie, soprattutto nell'ambito delle telecomunicazioni radiomobili, permette di avere sullo schermo di un terminale mobile, quale può essere un telefono cellulare, una serie di informazioni che consentono di tenere sotto controllo il processo.

Operatori dotati di terminali mobili possono essere sollecitati a intervenire

o semplicemente a verificare la presenza di eventuali anomalie direttamente dal sistema SCADA. In questo modo si possono attivare squadre di pronto intervento senza che queste siano impegnate nel presidio costante del sistema allestito nella sala controllo.

Un'altra area di evoluzione delle interfacce uomo-macchina riguarda la possibilità offerta dai sistemi di fornire informazioni non solamente attraverso l'uso di uno schermo. L'adozione di tecnologie multimediali anche nel mondo dei sistemi SCADA permette di disporre non più, o non solo, di rappresentazioni schematiche degli impianti, ma di rappresentazioni che ricalcano in tutto le reali forme degli impianti. Tornando all'esempio di una squadra di manutenzione si può dire che avere la segnalazione di un guasto su di un organo potendo osservare la situazione realmente in atto sul campo permetterebbe di semplificare l'intervento migliorandone tempi ed efficacia.

Capitolo 10

Eventi e allarmi

Uno dei compiti di un sistema SCADA è quello di avvertire nel più breve tempo possibile un operatore riguardo una condizione anomala che si sta verificando nel processo. In questo modo l'operatore può intervenire tempestivamente per prevenire situazioni potenzialmente pericolose per il processo, per l'ambiente o per l'uomo. In alcuni casi situazioni particolarmente pericolose sono gestite in modo autonomo direttamente dal sistema SCADA, proprio per garantire la correttezza delle operazioni e un intervento che sia il più rapido possibile.

Le informazioni che il sistema SCADA gestisce debbono essere trattate in maniera differente discriminandone la natura sulla base delle considerazioni fatte in precedenza. Infatti alcune informazioni sono semplici dati che il sistema presenta all'operatore, altre informazioni debbono essere elaborate con particolare tempismo e cura. In questo secondo caso si parla di *allarmi* e di *eventi*.

10.1 Differenza tra eventi e allarmi

Sia gli allarmi che gli eventi sono condizioni di funzionamento del processo controllato, o dei suoi componenti, che richiedono una elaborazione particolare da parte del sistema SCADA. Entrambi si riferiscono, generalmente, a condizioni di funzionamento anomalo e spesso richiedono una reazione, gestita automaticamente dal sistema SCADA o realizzata dall'operatore, per far tornare il processo in una situazione di controllo.

Anche se allarmi ed eventi possono sembrare la stessa cosa in effetti essi non lo sono. Un evento indica il verificarsi di una particolare condizione, un allarme indica lo stato di una particolare condizione. Un evento è associato all'istante in cui una condizione anomala si è verificata, l'allarme indica che

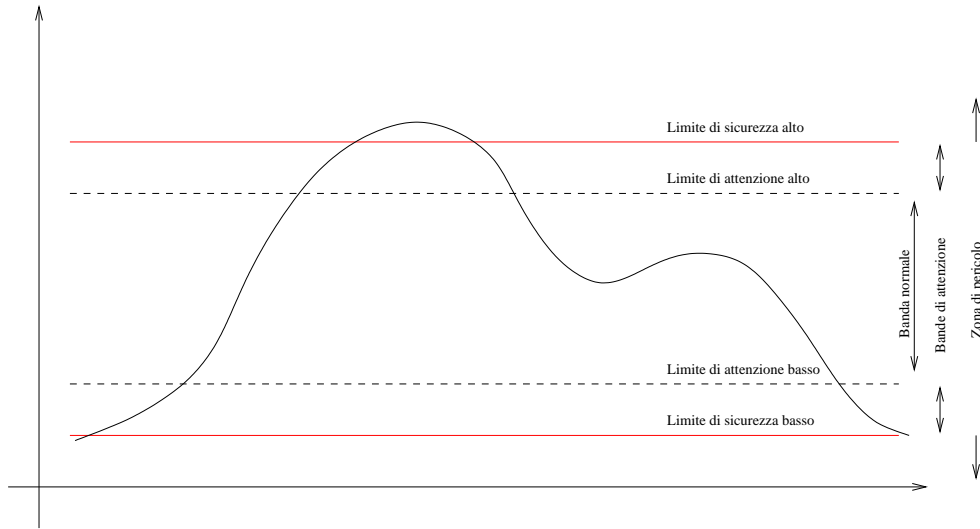


Figura 10.1: Soglie di allarme di una misura

il processo è in una condizione di funzionamento anomala. Una cosa che però accomuna gli allarmi e gli eventi è l'informazione temporale che il sistema SCADA associa ad entrambi per facilitarne la gestione.

Forse un esempio può contribuire a fare chiarezza. Si è visto nella parte di trattamento dati che a una misura possono essere associati dei limiti di funzionamento che ne definiscono una zona di normale funzionamento e altre zone in cui il valore della misura assume valori di attenzione o di pericolo (cfr. figura 10.1).

Se il valore della misura, trovandosi inizialmente nella banda normale, dovesse variare fino a portarsi nella banda di attenzione superiore il sistema dovrebbe segnalare quest'anomalia di funzionamento. La nuova condizione provocherebbe l'emissione sia della segnalazione di allarme che della segnalazione di evento. La condizione di allarme sarebbe data dal fatto che il valore si trova in una banda di attenzione mentre l'evento sarebbe dovuto al fatto che il valore ha cambiato banda di lavoro: dalla banda normale si è portato nella banda di attenzione. A questo punto se la misura subisse una nuova variazione che però non ne porta il valore al di fuori della banda di attenzione nessun evento sarebbe generato dal sistema, mentre la condizione di allarme permanerebbe. Se invece la misura subisse una variazione tale da portare il valore in un'altra banda, il sistema segnalerebbe nuovamente un evento, mentre l'allarme sarebbe generato solamente se la nuova banda fosse una banda di attenzione o di pericolo.

In definitiva l'evento indica l'istante in cui il valore di una misura passa da una banda all'altra. L'allarme invece è una condizione associata ad ogni

banda (tranne la normale): viene generato nel momento in cui la misura assume un valore che la porta nella relativa banda e permane per tutto il tempo in cui il valore rimane al suo interno.

10.2 Trattamento

La natura particolare delle informazioni eventi ed allarmi è tale che anche il trattamento che essi subiscono prevede una gestione particolare. Ogni volta che un allarme o un evento si genera l'operatore è chiamato ad effettuarne un riconoscimento. Riconoscere un allarme o un evento significa prendere visione della sua segnalazione e quindi della potenziale situazione di pericolo per il processo. Per facilitare il compito dell'operatore e metterlo in condizione di avere informazioni immediate su eventi e allarmi correntemente attivi il sistema utilizza una lista nella quale introduce una voce ogni volta che viene generato un evento o un allarme. Nel momento in cui la condizione anomala scompare e si ritorna al normale funzionamento il sistema segnala il ritorno da una condizione di allarme o da un evento. Se l'operatore aveva già effettuato il riconoscimento, l'allarme o l'evento viene rimosso dalla lista degli allarmi/eventi attivi, altrimenti vi rimane fino a che non sarà riconosciuto. Un sistema SCADA non dovrebbe consentire la cancellazione automatica dalla lista se non è stato eseguito il riconoscimento. Questa pratica infatti contrasterebbe con le motivazioni che hanno portato alla definizione di allarme o evento: condizione anomala che deve essere portata a conoscenza di chi gestisce il processo.

Questa lista deve essere consultabile dall'operatore per avere informazioni circa le situazioni critiche del sistema. Spesso la criticità delle situazioni che conducono alla generazione di un allarme o di un evento è tale che in ogni pagina che l'operatore ha a disposizione sono riportati gli ultimi allarmi/eventi accaduti. In sistemi SCADA che permettono di avere a disposizione una rappresentazione su più pagine video gli operatori solitamente hanno sempre in visualizzazione la pagina degli allarmi. Spesso a chi realizza il sistema si chiede di evidenziare la condizione di allarme con particolari rappresentazioni (ad esempio il valore che lampeggia) oppure di portare automaticamente alla vista dell'operatore la pagina che contiene la lista degli allarmi attivi. In figura 10.2 è riportato un esempio di come può apparire e di quali funzionalità dispone una pagina di gestione di eventi e allarmi.

Un'altra operazione che il sistema compie sulle informazioni di allarme/evento è l'associazione dell'etichetta "tempo". Ogni volta che un allarme/evento si genera, viene riconosciuto, viene cancellato, il sistema associa

possono suddividere eventi e allarmi per competenza e darne rappresentazione solo nelle postazioni operatore destinate alla loro gestione. Le informazioni di allarme relative alle grandezze di processo, ad esempio, potrebbero essere visualizzate nelle postazioni degli operatori di sala controllo, mentre le informazioni diagnostiche sullo stato degli impianti di acquisizione dati potrebbero essere visualizzate solamente nelle postazioni degli operatori di sistema.

In qualche sistema SCADA la categoria viene sostituita con il livello di allarme/evento. Il principio di funzionamento è lo stesso anche se con i livelli possono essere realizzati alberi gerarchici. In questo caso sarebbe possibile realizzare selezioni in relazione ad aggregazioni di allarmi/eventi. Infatti ad allarmi/eventi di primo livello sono collegati allarmi/eventi di secondo livello e a questi allarmi/eventi di terzo livello e così di seguito. Se venisse generato un allarme di terzo livello tutti i livelli soprastanti dai quali questo discende sarebbero portati dal sistema in uno stato di allarme. Associando ad esempio un allarme di primo livello a ogni impianto del sistema, uno di secondo livello a ogni organo di tale impianto e così per il livelli successivi, la semplice visualizzazione degli allarmi di primo livello potrebbe contenere informazioni di un allarme in un determinato impianto. Navigando nei livelli successivi si potrebbe poi conoscere l'allarme specifico.

10.2.2 Priorità

La priorità associata ad un allarme/evento permette di darne una classificazione in base al grado di importanza. Esistono condizioni di allarme che richiedono un intervento immediato, altre che possono essere considerate tollerabili per un breve periodo di tempo, altre ancora che richiedono interventi per i quali non è necessario agire con urgenza.

Spesso a gradi diversi di priorità si fanno corrispondere anche modalità di presentazione diverse. Ad esempio per allarmi a bassa priorità può essere sufficiente l'inserimento nell'archivio degli allarmi/eventi mentre allarmi a priorità medie oltre che nell'archivio vengono inseriti nella lista degli allarmi/eventi attivi che gli operatori hanno in vista; per priorità massime, oltre a quanto fatto per gli altri livelli, si procede all'attivazione di segnalazioni acustiche o visive (sirene, lampeggiatori) per sollecitare l'attenzione degli operatori.

10.2.3 Disabilitazione dinamica

Si pensi ad un sistema SCADA che gestisce un insieme vasto di informazioni provenienti dal processo. È possibile che alcune situazioni portino il sistema

SCADA a generare un insieme di allarmi/eventi di dimensioni ragguardevoli. Spesso queste situazioni sono frutto di un evento scatenante al quale è possibile far risalire la responsabilità e altri eventi secondari derivati dal primo. Ad esempio l'apertura di un interruttore di ingresso a una cabina elettrica per intervento di una protezione comporta l'immediato arresto di tutti gli impianti derivati da quella cabina. Al verificarsi di questo evento l'operatore potrebbe ricevere una serie di allarmi tra i quali sono presenti sia gli allarmi causati dagli impianti che si sono fermati sia quello relativo all'intervento della protezione elettrica. In questo caso discriminare quale sia l'evento che ha originato il problema potrebbe essere difficile. Eppure è proprio l'intervento necessario a rimuovere la causa che ha generato l'evento primario che viene richiesto per riportare il processo sotto controllo.

Viene in aiuto la funzionalità di disabilitazione dinamica degli allarmi. Se la generazione degli allarmi relativi agli impianti che si sono fermati venisse disabilitata nel caso di intervento della protezione elettrica, l'operatore si troverebbe un solo evento al quale dover porre rimedio per ripristinare la condizione normale. Questa pratica è nota come *alarm overriding*.

Non sempre questa tecnica è gradita a chi gestisce il sistema SCADA in quanto potrebbe mascherare delle condizioni anomale quando invece esse potrebbero dover essere tenute in considerazione. Sistemi più moderni si avvalgono di tecniche evolute per la discriminazione di eventi primari e derivati. In questi sistemi l'operatore viene guidato dal sistema SCADA nella risoluzione del problema evitando di privarlo della conoscenza dettagliata di quanto è avvenuto.

10.2.4 Permessi operatore

Allarmi ed eventi sono informazioni che segnalano la necessità di una reazione al fine di scongiurare possibili situazioni di pericolo. Poiché la reazione deve garantire il ritorno a una situazione di normalità la preparazione richiesta agli operatori è specifica in relazione al tipo di allarme/evento accaduto. Non sempre le conoscenze di un operatore equivalgono quelle di un altro. Non sempre le competenze di un operatore sono tali da permettergli di operare su tutto il processo. In particolare per sistemi di medie o grandi dimensioni gli operatori vengono suddivisi per responsabilità e competenze.

Parallelamente per il trattamento degli allarmi/eventi vengono previste suddivisioni in base al ruolo degli operatori. Nell'esempio riportato in precedenza (cfr. sezione 10.2.1) il trattamento degli allarmi relativi alle grandezze di processo è riservato agli operatori di sala controllo, mentre il trattamento degli allarmi diagnostici è riservato agli operatori di sistema.

Ogni operatore sarà rappresentato all'interno del sistema SCADA con un determinato profilo. Di questo profilo fanno parte anche le informazioni che determinano la possibilità di operare sugli allarmi/eventi. Quest'ultima può essere data sulla base delle categorie di allarme o sulla loro priorità.

10.3 Evoluzione dei sistemi di avviso

L'evoluzione della tecnologia ha permesso di realizzare sistemi SCADA che possono autonomamente provvedere alla gestione di un processo senza richiedere la presenza di un operatore in sala controllo. I sistemi sono sempre più spesso capaci di lavorare e garantire il normale funzionamento del processo controllato senza l'intervento degli operatori. Questi invece sono necessari in particolari momenti, quando il processo entra in una condizione critica o quando c'è bisogno di operazioni di manutenzione.

In questi casi gli operatori debbono essere avvertiti dal sistema SCADA della necessità della loro presenza. Questo avvertimento non può seguire i normali canali dei sistemi SCADA tradizionali (segnalazione su stampante, su video, con sirena o lampeggiante). La comunicazione a distanza dell'allarme attivato deve passare attraverso l'utilizzo di mezzi di telecomunicazione che siano in grado di raggiungere operatori dotati di mobilità sul territorio. A questo scopo possono essere utilizzate vie di comunicazione che raggiungano l'operatore su un dispositivo radiomobile (telefono cellulare, cerca persone, computer portatili).

La scelta del mezzo di comunicazione deve essere fatta in maniera molto oculata e considerando tutte le caratteristiche del mezzo scelto. Il fatto che l'operatore non si trova nell'impianto non garantisce l'immediatezza della comunicazione e soprattutto del fatto che lo stesso venga effettivamente informato dell'evento, questo in contraddizione al principio di comunicazione immediata di situazione anomala che è alla base del concetto di allarme/evento. La scelta del messaggio di posta elettronica come strumento di comunicazione non è adeguata quando è necessario garantire la consegna, magari entro tempi soggetti a vincoli stringenti. In più non sarebbe garantito il fatto che il messaggio venga effettivamente letto dal destinatario.

Ogni volta che si deve realizzare una comunicazione a distanza di una situazione anomala si deve tenere in considerazione la gravità dell'informazione, la rapidità di intervento richiesto, la certezza che l'informazione raggiunga un operatore e che questo l'acquisisca, la possibilità di avere canali secondari in caso di indisponibilità del primo, la possibilità di avvertire più operatori.

In definitiva la possibilità di non presidiare l'impianto comporta un grande vantaggio per chi lo gestisce (permette di riservare risorse ad altri compiti assicurandosi al contempo la migliore gestione possibile del processo) ma al tempo stesso richiede uno sforzo organizzativo e progettuale notevole dovuto proprio al fatto che gli impianti non sono presidiati, cosa che comporta un notevole aumento dei rischi. Un dettagliato esame dei rischi potrebbe in qualche caso far recedere dall'idea di gestire un impianto da postazioni remote, o addirittura senza presidio.

Capitolo 11

Archiviazione

L'attività di un sistema SCADA comporta il trattamento di dati rappresentativi degli stati assunti dal processo nella sua evoluzione e delle condizioni di esercizio delle infrastrutture che costituiscono il sistema di controllo (sensori, attuatori, apparecchiature di acquisizione dati, sistemi di comunicazione, sistema di elaborazione). Le attività di supervisione e controllo fanno uso del database runtime nel quale sono presenti dati relativi all'istante in cui questi vengono osservati. Una volta divenuti inattuali i dati gestiti dal sistema non vengono perduti ma conservati in archivi detti "archivi storici" per ragioni e con modalità che sono descritte nel seguito del capitolo. Per una trattazione razionale e completa delle metodologie di gestione dei dati si suggerisce la consultazione di testi specializzati (cfr. [9], [1], [8], [3])

11.1 Perché archiviare i dati

Le ragioni che inducono alla realizzazione di una banca dati di archivio storico sono molte e molto diverse tra loro. Tra queste ce ne sono alcune che si ritrovano in molti sistemi e altre che, invece, sono valide in casi specifici. Le sezioni che seguono contengono una presentazione di alcuni dei motivi ricorrenti causa dell'impegno di archiviazione storica delle informazioni trattate dai sistemi di controllo.

11.1.1 Studio del processo

Una prima importante ragione per la quale si ritiene necessario equipaggiare i sistemi di supervisione e controllo con strutture di archiviazione dei dati è nel fatto che la disponibilità di serie storiche consente di realizzare analisi delle informazioni che conducono alla conoscenza dell'evoluzione del sistema. L'osservazione di rappresentazioni comunque raffinate e astratte rispetto alla

visione diretta dei dati grezzi ma pur sempre limitate allo stato attuale del processo controllato, a istantanee raffiguranti un fotogramma all'interno di un flusso continuo, non permette di comprendere alcuni aspetti fondamentali legati all'evoluzione. Aspetti che riguardano le relazioni di causa-effetto tra perturbazioni imposte al processo ed evoluzioni dello stato, la dinamica del processo in termini di variabilità nel tempo di grandezze significative, la correlazione tra grandezze del processo e, di conseguenza, le relazioni tra le evoluzioni di tali grandezze.

Lo studio dell'evoluzione del processo è esso stesso, in molti casi, scopo del sistema di supervisione. Un caso esemplare è quello dei sistemi di telerilevamento ambientale: l'analisi dei dati archiviati consente di giungere alla conoscenza dell'evoluzione di particolari fenomeni fisici e di metterla in relazione con l'evoluzione degli altri parametri registrabili, tutto ciò portando a una conoscenza altrimenti non raggiungibile.

11.1.2 Documentazione storica

L'archiviazione può essere il frutto di una scelta dettata dalla volontà di conservare memoria di quanto accaduto al processo nella sua evoluzione. Anche se non legata a necessità di studio o altre possibili cause di conservazione dei dati l'archiviazione può essere considerata utile per assicurarsi la disponibilità dei dati per scopi non ben definiti in fase di progetto ma che, l'esperienza insegna, prima o dopo emergono.

Un caso frequente di archiviazione dettata dalla necessità di documentazione storica è quello nel quale norme, regolamenti o leggi prevedono esplicitamente la conservazione dei dati. Tutti i sistemi che attuano supervisione e controllo su processi che sono di interesse pubblico sono di esempio per questo tipo di esigenza di archiviazione. I sistemi di telerilevamento ambientale realizzati e gestiti da enti pubblici di tutela dell'ambiente sono destinati a produrre informazioni e conoscenze che, opportunamente utilizzate dagli organi pubblici di governo, suggeriscono provvedimenti orientati alla conservazione o al recupero di uno stato dell'ambiente considerato compatibile con le attitudini spontanee del pianeta e dei suoi abitanti. I dati prodotti da questo tipo di sistemi sono portatori d'informazione e conoscenza ma anche di provvedimenti amministrativi o legislativi; essi hanno un impatto significativo sulla vita dei singoli cittadini, dell'industria, di tutte le attività umane che possono essere causa di turbamento dell'equilibrio ambientale e, per questo, per essi esiste un'adeguata regolamentazione che razionalizza la loro produzione e il loro trattamento anche in termini di metodi, strumenti e tempi di archiviazione.

Un altro esempio significativo di archiviazione dei dati regolata da norme specifiche è dato dall'attività dei sistemi di controllo del traffico aereo. Questi sistemi sono in grado di registrare l'attività del traffico osservato per mezzo dei complessi sistemi radar installati presso gli aeroporti. Si potrebbe essere portati a pensare che in normali condizioni di flusso del traffico aereo l'archiviazione dei dati sia soltanto un carico inutile per il sistema di controllo e che questa dovrebbe avvenire solo in casi di emergenza, magari su richiesta dei responsabili del traffico. In realtà quanto osservato dal sistema di controllo deve essere adeguatamente archiviato per permettere una corretta analisi del traffico realizzata a posteriori, analisi che per molte ragioni può essere richiesta dalla magistratura o da altre autorità competenti. La conservazione della storia del traffico aereo come l'archiviazione dei dati ambientali utilizzati per calcolare valori di parametri sui quali determinare scelte politiche rappresenta, infine, la garanzia di regolarità dell'attività delle strutture responsabili di tali dati e dell'uso che se ne fa o, se si preferisce, rappresenta la garanzia del fatto che la regolarità dell'attività può essere verificata.

11.1.3 Interesse statistico o contabile

L'attività dei sistemi di controllo è spesso legata all'automazione dei processi produttivi sviluppati nel mondo dell'industria nei quali i processi controllati corrispondono ai fenomeni fisici che realizzano gli obiettivi dell'impegno industriale. In questi ambienti i sistemi di controllo vengono in contatto, quando non sono la vera sorgente d'informazione, con i dati relativi alla produzione in termini quantitativi e qualitativi e rappresentano il naturale strumento di gestione dell'archiviazione. In ambienti di produzione evoluti questa caratteristica viene sfruttata non soltanto come strumento aggiuntivo per l'osservazione dell'attività produttiva ma anche come punto di osservazione accessibile ai settori gestionali dell'azienda. Il patrimonio di dati trattati dal sistema di controllo diventa così una base di riferimento sulla quale costruire un'informazione preziosa in termini tecnici e gestionali, la base dati relativa al motore della macchina industriale che è l'attività produttiva.

Esempi relativi alle esigenze di archiviazione di carattere statistico o amministrativo-gestionale possono essere presi, come detto, dal mondo della produzione industriale. Si consideri quindi una linea automatizzata quale può essere quella in dotazione a un impianto di produzione di flaconi di sapone liquido. Essa è presumibilmente gestita da un sistema di controllo che ne governa le attività elementari (moto del nastro trasportatore, disposizione dei flaconi sul nastro, introduzione del sapone nel contenitore, collocazione e fissaggio del tappo, ...) e da un'attività umana responsabile della predisposi-

zione delle condizioni di esercizio della linea (assicurazione della disponibilità del sapone liquido nei serbatoi dai quali la linea attinge, della disponibilità di flaconi e tappi, del prelievo del prodotto finito dalla sezione d'uscita della linea, ...). Un sistema del genere è in grado di fornire un insieme di dati fondamentali nell'analisi dell'attività della linea: numero di pezzi prodotti, tempi e cause di eventuali interruzioni della produzione, livelli di materia prima contenuta nei serbatoi. La semplice osservazione di questi dati è in grado di fornire elementi di analisi importanti, analisi che diviene veramente efficace se si dispone, oltre che dei dati attuali, delle serie storiche. È evidente che lo studio di questo tipo di dati volto a comprendere le cause e trovare i rimedi alle interruzioni di produzione dovute a guasti è un'attività d'interesse tecnico mentre le analisi dei dati più propriamente legati alle quantità (ad esempio il numero di pezzi) sono d'interesse gestionale. È altrettanto evidente che l'interesse per una attenta archiviazione dei dati è assolutamente giustificato e diventa un elemento per la valutazione della qualità del sistema di controllo.

11.2 Metodi e tecnologie

La realizzazione dell'archivio storico di un sistema SCADA comporta la risoluzione di alcuni problemi che inevitabilmente si presentano al progettista quando si deve decidere come organizzare i dati, come rappresentarli, quali strumenti utilizzare. Alcuni quesiti ricorrenti, e con essi possibili soluzioni, sono presentati nelle sezioni seguenti.

11.2.1 Organizzazione e modalità di archiviazione

Un primo importante passo verso la realizzazione di un archivio storico è la determinazione di un'adeguata organizzazione dei dati. Si intende per organizzazione il modello secondo il quale i dati appartenenti a diverse sezioni della banca dati sono in relazione tra loro e non i metodi con i quali il modello può essere definito. Si considera quindi come obiettivo del processo di modellazione una banca dati di tipo relazionale, essendo la modellazione la fase di analisi che ne determina la struttura. La predilezione per una struttura relazionale discende principalmente dalla necessità di allestire una banca dati che sia in grado di soddisfare esigenze di analisi provenienti da ambienti eterogenei per funzioni svolte, conoscenze e strumenti di lavoro. Scelte diverse possono essere prese in considerazione quando il patrimonio di dati è caratterizzato da un interesse limitato all'esercizio del sistema ma

la tendenza all'integrazione tra sistemi distinti, che fa dell'archivio storico la naturale interfaccia di comunicazione, induce a considerare questa opzione inefficiente e obsoleta. Il ruolo di strumento di comunicazione tra sistemi concorrenti svolto dall'archivio mette in evidenza la necessità di considerare l'organizzazione dei dati come parametro di qualità della base dati poiché da questa dipendono le caratteristiche dell'interoperabilità tra sistemi.

La specificità di un archivio storico contenente i dati relativi all'attività di un sistema SCADA risiede in due elementi caratteristici: il riferimento temporale che caratterizza ciascun elemento d'informazione e la mole di dati trattati. L'archiviazione dei dati di esercizio ha come obiettivo la conservazione di informazioni relative all'evoluzione del sistema, informazioni che possano essere utilizzate per riprodurre una fotografia dello stato in cui il processo si è trovato in un istante appartenente al passato. Per ottenere questo risultato è necessario realizzare una banca dati nella quale il singolo elemento d'informazione conservi la nozione del tempo, sia qualificato con un'etichetta temporale corrispondente all'istante nel quale il dato è stato acquisito. L'archivio prende così la forma di un insieme di dati rappresentativi di immagini dello stato di esercizio, fotogrammi che costituiscono il percorso evolutivo che il sistema ha seguito nella propria attività.

Quanto detto suggerisce un metodo di archiviazione in grado di condurre a una banca dati contenente tutto il necessario per una ricostruzione completa degli stati attraversati dal processo. Questo corrisponde all'archiviazione su base periodica della totalità dei dati "grezzi" trattati dal sistema con periodicità tale da intercettare tutte le variazioni avvenute nel tempo. Il metodo è in contrasto, però, con i vincoli imposti dal secondo elemento di specificità degli archivi storici, cioè la mole dei dati. L'allestimento dell'archivio e l'obiettivo di renderlo effettivamente utilizzabile, quando non semplicemente realizzabile, comporta la definizione di un insieme di dati da archiviare che può essere un sottoinsieme di quello caratteristico del database runtime, un nuovo insieme costruito sulla base di calcoli in linea che producono grandezze aggregate o una combinazione tra elementi dei due tipi di dati. La definizione dell'insieme di dati destinati all'archiviazione è, evidentemente, un'attività nella quale è necessario prestare attenzione alle caratteristiche del processo del quale si vuole riprodurre lo stato a posteriori, alle esigenze di analisi di tutti i destinatari dei dati individuabili al momento della progettazione del sistema, a usi non ancora previsti che possono essere fatti dell'archivio. La scelta dei dati grezzi da archiviare deve condurre a un insieme in grado di evidenziare elementi determinanti nella comprensione delle condizioni di esercizio del sistema mentre per gli aspetti quantitativi è possibile affidarsi

a grandezze aggregate quali possono essere le medie orarie, giornaliere, settimanali. Spesso la definizione di dati aggregati di questo genere è prescritta da specifiche di sistema derivate dallo studio del processo o è la risposta a esigenze di analisi quantitativa coincidenti con le stesse ragioni per le quali il sistema deve essere realizzato. Quest'ultimo è il caso, ad esempio, in cui le grandezze aggregate vengono utilizzate per la contabilizzazione o la fatturazione.

L'uso di questo tipo ibrido di archivio, costituito in parte da dati grezzi e in parte da grandezze aggregate, è molto frequente poiché risponde alle esigenze che solitamente emergono in fase di progettazione. Naturalmente esistono sistemi, ad esempio quelli destinati a funzioni di rilevamento, per i quali l'unica soluzione adeguata coincide con l'archiviazione di tutti i dati grezzi acquisiti. In questi casi la progettazione dell'intero sistema deve essere realizzata in considerazione del vincolo imposto sull'archivio. Eventuali limiti non possono essere superati con la definizione di un sottoinsieme dei dati trattati appena considerata ma con l'individuazione di una frequenza di archiviazione minore rispetto a quella di acquisizione, compatibilmente con le risorse disponibili e con le esigenze di archiviazione.

Le soluzioni proposte al problema sollevato dalla gestione di ingenti quantità di dati da archiviare introducono una perdita d'informazione nel passaggio dal database runtime all'archivio storico. L'archiviazione parziale dei dati grezzi non consente di conservare immagini complete degli stati attraversati dal processo nella sua evoluzione comportando la necessità di introdurre meccanismi di salvataggio per la gestione di casi particolari. Malfunzionamenti del sistema, evoluzioni atipiche del processo, lo studio di particolari stati di esercizio sono esigenze alle quali solitamente si risponde con procedure che salvano in archivio l'insieme completo di dati trattati dal sistema in intervalli di tempo comprendenti l'istante di attivazione delle procedure medesime. L'attivazione può essere comandata dagli operatori per mezzo dell'interfaccia uomo-macchina oppure da procedure automatiche attive nel sistema. La dimensione dell'intervallo di tempo considerato, o il valore limite tollerato, deve essere definito in fase di progetto.

11.2.2 Strumenti

Nelle sezioni precedenti è specificato il fatto che la struttura dei dati si fonda in ogni caso sul modello relazionale. Questa precisazione non determina la scelta degli strumenti di gestione dell'archivio anche se la strada privilegiata conduce ai sistemi di gestione dei database detti RDBMS (*Relational DataBase Management System*). Strada che non sempre è in discesa poiché

spesso la frequenza di acquisizione e la mole dei dati comportano flussi che le sovrastrutture introdotte dalla gestione delle banche dati non riescono a trattare nei tempi imposti dal sistema di controllo. È noto che i sistemi di gestione dei database sono caratterizzati da elevati tempi di trattamento dei dati a causa delle operazioni di controllo finalizzate a garantire l'integrità della banca dati.

Una soluzione alternativa consiste nella rinuncia all'uso di sistemi che garantiscono la gestione dei dati, rinuncia che comporta la perdita di tutta la potenza resa disponibile dall'uso di RDBMS e la realizzazione di meccanismi di archiviazione che si limitano alla memorizzazione su supporto stabile delle informazioni di archivio (che conservano un'organizzazione di tipo relazionale). In particolare si tratta di memorizzare i dati da archiviare su file opportunamente formattati e rimandare al momento in cui si verifica la necessità di accedere alle informazioni l'attività di trasferimento dei dati dai file a una banca dati relazionale gestita da RDBMS.

Le due soluzioni possono essere adottate anche di concerto in modo da avere immediatamente disponibile un insieme limitato di dati conservando la possibilità di recuperare da archivi gestiti a livello di filesystem le informazioni che dovessero risultare necessarie alle strutture di analisi. Questo metodo può essere visto come una tecnica di ottimizzazione delle risorse ed è molto diffuso nella pratica poiché permette di ottenere elevate prestazioni senza pregiudicare la completezza dell'informazione contenuta negli archivi storici. L'adozione di questo metodo di solito comporta la realizzazione di strumenti per la configurazione dinamica dei due insiemi di dati, quelli destinati direttamente al database e quelli archiviati in file dati.

La disponibilità dell'informazione nella forma di banche dati gestite da RDBMS ha un importante significato dal punto di vista dell'interoperabilità tra sistemi concorrenti. Questo in virtù del fatto che i sistemi di gestione delle banche dati espletano la doppia funzione di gestori, occupandosi di organizzazione, integrità e quant'altro, e di fornitori di meccanismi d'interrogazione, per mezzo di un linguaggio di interrogazione definito secondo uno standard consolidato, il noto *Structured Query Language* o *SQL*. L'eleganza e la potenza del linguaggio SQL garantiscono la massima accessibilità possibile alle basi di dati senza compromettere l'efficacia delle transazioni, anche quando le strutture dei dati sono molto complesse. Le caratteristiche di linguaggio definito come standard sia dall'ANSI (*American National Standards Institute*) che dal mercato del software lo qualificano come protocollo di comunicazione per l'interoperabilità dei sistemi diffuso e stabile. Gli strumenti software per la fruizione dei dati basata su interrogazione via linguaggio SQL sono

a loro volta sufficientemente consolidati e possono essere raggruppati in due categorie:

1. sistemi aperti di connettività
2. *API (Application Program Interface)* specifiche del RDBMS e del linguaggio di programmazione

Alla prima categoria appartengono i software comunemente classificati come *drivers*, cioè strati intermedi interposti tra RDBMS e applicativi. Questi traducono le query provenienti dagli applicativi in comandi comprensibili al RDBMS e i risultati delle query in forme comprensibili agli applicativi. Il più importante e diffuso driver, detto ODBC (*Open DataBase Connectivity*), fa riferimento a un metodo definito dallo *SQL Access group* nel 1992 ed è lo strumento prediletto per la realizzazione di applicazioni che non sono soggette a vincoli prestazionali e di affidabilità particolarmente stringenti. Una caratteristica importante del metodo ODBC è nel fatto che i driver che lo realizzano definiscono un'interfaccia standard indipendente dal RDBMS, lasciando agli applicativi che accedono alle informazioni il solo onere di conoscere la struttura dei dati. Le *API* sono librerie software rese disponibili dai produttori di software RDBMS nei principali linguaggi di programmazione utilizzati per lo sviluppo di software applicativi (C, C++, ...). Con queste è possibile realizzare un controllo completo su instaurazione, uso e distruzione dei collegamenti tra applicativi e RDBMS, il tutto fatto con grande riguardo per le prestazioni e l'affidabilità delle transazioni.

Capitolo 12

Analisi dei dati

Il presente capitolo tratta un aspetto dei sistemi che nel corso degli anni ha subito un'evoluzione tale da renderlo protagonista di una significativa spinta verso l'integrazione tra sistemi di controllo concorrenti e, cosa ancor più significativa, tra ambienti di controllo e strutture di supporto alla decisione. L'analisi dei dati è stata l'evoluzione naturale di sistemi che nel tempo si sono rivelati capaci di diventare depositari di dati essenziali per la comprensione dei processi sottoposti a supervisione e controllo. Sistemi progettati a scopo di supervisione, quali sono i sistemi di rilevamento per lo studio delle attività sismiche, dell'inquinamento ambientale, delle variabili d'interesse meteorologico, hanno mostrato profonde analogie con sistemi di controllo per l'industria destinati alla contabilizzazione di alcune grandezze fisiche caratteristiche del processo controllato o all'analisi delle stesse finalizzata a produrre previsioni e a valutare prestazioni. Le due categorie di sistemi sono chiamate a svolgere un compito per il quale è indispensabile allestire strutture di archiviazione e analisi dei dati. Le sezioni che seguono contengono un'introduzione agli strumenti comunemente utilizzati in fase di analisi, quelli che solitamente sono integrati nelle funzionalità del sistema di elaborazione e quelli che ben presto lo saranno.

12.1 Trend Storici

Uno strumento di analisi considerato, a ragione, come parte integrante di un sistema di supervisione e controllo è il *trend storico*. Si tratta di uno strumento di elaborazione grafica che consente di rappresentare su un diagramma cartesiano l'evoluzione di una grandezza sottoposta a osservazione in funzione di un'altra grandezza acquisita dal sistema o, come accade comunemente, del tempo. Nella maggior parte dei casi il trend storico viene integrato nel-

l'interfaccia uomo-macchina e proposto come strumento a disposizione degli operatori ma il compito di rappresentare l'andamento di grandezze d'interesse per l'attività del controllo viene svolto da un altro tipo di trend (cfr. sezione 9). Il trend storico ha l'obiettivo di rendere disponibile uno strumento grafico di indagine del comportamento che una grandezza ha avuto in un intervallo di tempo che appartiene al passato. Questa funzione è volta a supportare l'analisi con una rappresentazione grafica che in molti casi è in grado di fornire in forma diretta e immediatamente leggibile informazioni nascoste dal linguaggio criptico delle serie numeriche.

L'uso che può essere fatto dei trend storici dipende fortemente dal tipo di processo controllato e, di conseguenza, di sistema. Se il processo controllato è l'attività sismica di un'area territoriale il trend deve permettere la rappresentazione dell'intensità rilevata in uno o più punti in funzione del tempo. Quando le variabili osservate sono indicatori della presenza di fattori inquinanti nell'aria deve essere possibile rappresentare il comportamento di tali fattori su scala temporale. L'andamento delle temperature, comprese massime e minime, dell'intensità delle precipitazioni, del grado di umidità e della pressione sono solo alcuni esempi di casi nei quali una rappresentazione grafica permette di rendere immediata la lettura delle variabili meteorologiche fondamentali.

Nel caso di sistemi di controllo l'osservazione dei trend costruiti su opportune variabili del sistema consente di osservare il comportamento dello stesso sistema favorendo, a volte, l'individuazione degli anelli deboli della catena e il miglioramento delle prestazioni del sistema e del processo. Per comprendere meglio questo aspetto e al tempo stesso mettere in evidenza l'efficacia del trend come strumento di analisi è possibile fare un esempio. Si consideri il problema di realizzazione di un inseguitore di una grandezza variabile nel tempo con l'andamento del dente di sega. Una volta realizzato l'algoritmo di inseguimento è necessario individuare il valore dei parametri di progetto che consentono di ottenere un risultato adeguato alle aspettative. Per far questo si possono analizzare i dati prodotti dall'algoritmo e confrontarli con l'andamento della grandezza di riferimento. Un modo per affrontare il problema è analizzare i valori per come si presentano selezionando un intervallo di tempo per l'osservazione. Le serie numeriche che seguono corrispondono ai primi valori acquisiti dalle due grandezze riportate in figura 12.1.

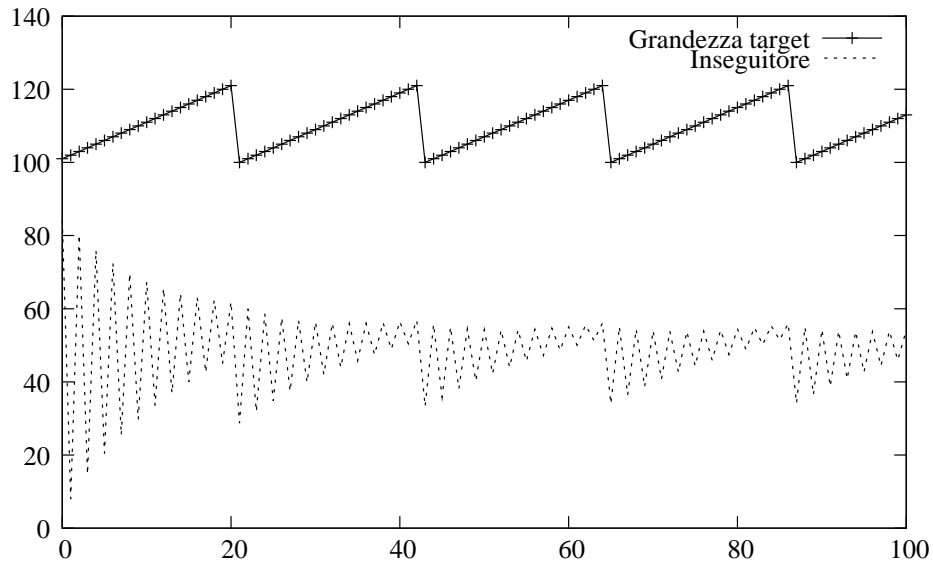


Figura 12.1: Primo esempio di output di un algoritmo di inseguimento di un dente di sega

Ciclo di calcolo	Grandezza target	Inseguitore
0	101.000000	84.840004
1	102.000000	7.950398
2	103.000000	80.197830
3	104.000000	14.739515
4	105.000000	75.995728
5	106.000000	20.449774
6	107.000000	72.490807
7	108.000000	25.404125
8	109.000000	69.640518
9	110.000000	29.740192
10	111.000000	67.354362
11	112.000000	33.554535
12	113.000000	65.548141
13	114.000000	36.926460
14	115.000000	64.149429
15	116.000000	39.922909
16	117.000000	63.096630
17	118.000000	42.600670
18	119.000000	62.337444
19	120.000000	45.007927
20	121.000000	61.827465

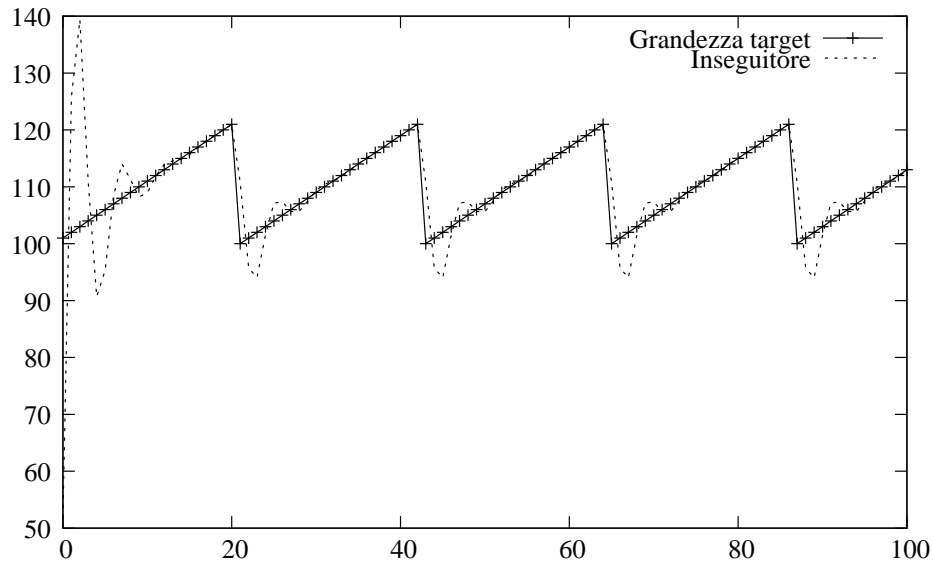


Figura 12.2: Primo esempio di output di un algoritmo di inseguimento di un dente di sega

La sfida alla quale chiunque è chiamato a rispondere è procedere per passi successivi alla variazione dei parametri di progetto e alla verifica del comportamento dell'inseguitore fatta sulla base delle serie numeriche, fino all'ottenimento di un algoritmo in grado di produrre una risposta confrontabile con quella riportata in figura 12.2. Il procedimento utilizzato per ottenere questo risultato è lo stesso proposto tranne che per il metodo di verifica utilizzato. Con l'osservazione dei trend è stato possibile ottenere il comportamento sperato in quattro passi di *tuning* dell'algoritmo.

Quanto detto evidenzia l'importanza dello strumento di generazione di trend storici e dà un esempio di come questo possa essere utilizzato come mezzo per la comprensione di caratteristiche relative sia al processo che al sistema di controllo.

12.2 Diagrammi e tabulati

Diagrammi (istogrammi, diagrammi a torta, ...) e tabulati sono strumenti comunemente utilizzati per tipi di analisi che non appartengono al mondo della supervisione e del controllo in senso stretto. L'uso di tabulati non è del tutto estraneo alla pratica del controllo ma questo ha avuto spazi di applicazione che hanno quasi sempre rappresentato la risposta a una esigenza d'interpretazione dei dati altrimenti disattesa. È possibile notare, però, l'introduzione nelle piattaforme di sviluppo SCADA di accessori che hanno

lo scopo di rendere disponibili strumenti di rappresentazione dei dati storici nella forma di diagrammi e tabulati.

Il motivo per il quale è stata dedicata una sezione a questo tipo di strumenti è nel fatto che esprimono necessità provenienti dai settori gestionali e di ricerca sempre più spesso codificate in termini di specifiche di progetto. L'evoluzione tecnologica ha permesso di giungere alla formalizzazione di un'esigenza che a oggi può essere formulata in termini di integrazione tra sistemi di controllo e sistemi di analisi dei dati. Questo è il vero tema della presente sezione e deve essere affrontato con l'obiettivo di individuare le interfacce tra sistema SCADA e sistemi concorrenti candidate all'interazione tra due mondi che debbono iniziare a scambiarsi informazioni.

Prendendo a riferimento il modello di sistema fin qui presentato la risposta al quesito posto è scontata. Il punto di accesso privilegiato alle informazioni residenti in un sistema è il database relazionale contenente l'archivio storico dei dati trattati. Questo punto d'accesso deve essere costruito per essere in grado di fornire tutti i dati necessari alle elaborazioni condotte per mezzo di strumenti di analisi; deve quindi essere progettato come elemento di un sistema che ha confini al di fuori del sistema di controllo. Per fare questo è importante indagare sulle caratteristiche dei sistemi di analisi ai quali sono destinate porzioni rilevanti dell'archivio storico.

12.3 Strumenti specifici di analisi

Gli ambienti gestionali e di ricerca ai quali si è fatto riferimento nelle sezioni precedenti sono caratterizzati da metodi, strumenti e tecnologie che hanno seguito uno sviluppo completamente indipendente da quello dei sistemi SCADA. Gli strumenti di analisi utilizzati sono molti e molto diversi tra loro, essendo stati pensati, realizzati e sviluppati in funzione di esigenze specifiche di settori per nulla affini. Un obiettivo di un progettista di sistemi SCADA, o più propriamente di piattaforme di sviluppo SCADA, deve essere la comprensione delle richieste provenienti dall'esterno e la risposta con soluzioni adeguate. Esistono casi in cui gli stessi strumenti comunemente utilizzati nell'analisi dei dati risultano inadeguati e la realizzazione passa per soluzioni specifiche. In questi casi debbono essere individuate correttamente le caratteristiche del problema in termini tecnologici e organizzativi. Se le responsabilità di sviluppo del sistema di controllo e di analisi dei dati sono distinte le soluzioni possibili comportano un'attenta definizione delle interfacce d'interazione tra le due attività. Le interfacce debbono permettere l'instaurazione di flussi di dati caratterizzati da moli e velocità di trasferi-

mento adeguate alle esigenze e possono non rispondere a canoni standard di comunicazione. Parallelamente deve essere definito il contenuto del flusso informativo in entrambe le direzioni. Se le responsabilità di sviluppo non sono distinte l'analisi dei dati può essere vista come frutto di procedure integrate nel sistema di controllo e la sua realizzazione ricondotta allo sviluppo di componenti del sistema medesimo. Questo genere di problemi si presenta quando le attività di analisi dei dati richiedono tempi di esecuzione molto bassi e dati aggiornati allo stato di esercizio attuale, cioè quando l'archivio storico non è l'unica sorgente di dati.

Un esempio di sistema chiamato a una fornitura dati finalizzata ad analisi realizzate con strumenti specifici è dato dall'esperienza dei sistemi di telerilevamento ambientale. Questi sistemi hanno il compito di acquisire dati relativi a variabili fisiche e renderli disponibili agli ambienti di analisi. Questi ultimi possono procedere all'elaborazione numerica dei dati da rappresentare successivamente nelle opportune forme oppure utilizzarli direttamente per produrre rappresentazioni in grado di arricchire la conoscenza del processo. Esempi di rappresentazioni utilizzate negli studi dei fenomeni ambientali sono le cartografie tematiche. Con queste vengono rappresentate caratteristiche di alcune variabili d'interesse, quale può essere la concentrazione di una sostanza, in relazione al territorio preso in esame. Il risultato dell'analisi può essere, ad esempio, una carta che riproduce in saturazione o intensità di un colore scelto la concentrazione di monossido di carbonio sul territorio metropolitano di una città. Sulla scia di questo esempio è possibile comprendere che la banca dati del sistema di acquisizione deve essere in grado di fornire dati qualificati con i parametri fondamentali (valore, codice di qualità, istante di acquisizione) utilizzati in un qualsiasi sistema SCADA ma anche con parametri caratteristici del sistema come le coordinate geografiche del sensore che ha acquisito il dato. Allo stesso modo è possibile comprendere come il processo che conduce dall'acquisizione dei dati all'archiviazione nel sistema di elaborazione è un sottoinsieme delle funzionalità tipiche dello SCADA mentre l'analisi di dati relativi a grandezze chimiche e fisiche nel contesto dell'indagine di qualità ambientale è un'attività che non può essere commissionata a un sistema di calcolo e nulla ha in comune con l'esperienza del controllo. Un'ultima considerazione riguarda gli strumenti utilizzati per l'analisi. La produzione di cartografie tematiche è opera di strumenti software complessi destinati a usi specifici verso i quali il sistema di acquisizione e archiviazione dei dati deve preoccuparsi di esporre interfacce efficienti e dati qualificati. È questo un confine che insieme a molti altri rappresenta la porta verso un'integrazione che non è logico continuare ad attendere e irragionevole pensare di cancellare.

Capitolo 13

Sicurezza del sistema

Il modello di sistema SCADA presentato contiene elementi strutturali che possono essere soggetti a problemi di sicurezza. Osservando la figura 7.1 da questo punto di vista è possibile individuare gli elementi sensibili nei seguenti:

1. interfaccia di accesso ai dati
2. interfaccia di comunicazione con le apparecchiature di campo
3. interfaccia uomo-macchina
4. infrastrutture tecnologiche che realizzano il sistema

I primi due punti evidenziano la necessità di predisporre sistemi di protezione delle infrastrutture di comunicazione utilizzate per le connessioni tra porzioni di sistema fisicamente distinte; il terzo si riferisce alle caratteristiche dell'interfaccia uomo-macchina e alla gestione degli accessi alle funzionalità del sistema di controllo. L'ultimo riguarda la protezione fisica alla quale debbono essere sottoposte tutte le strutture tecnologiche costituenti il sistema per evitare che intrusioni indesiderate portino a eventi di manomissione o danneggiamento.

Il modello di sistema inattaccabile è un obiettivo indicato dall'esperienza come un'utopia che può essere di aiuto per la definizione di politiche precauzionali. Pratiche di protezione dei sistemi sono presentate nelle sezioni seguenti come esempi di provvedimenti possibili finalizzati alla protezione di sistemi dotati di una struttura confrontabile con quella fin qui descritta. Quanto riportato deve essere considerato come introduzione a un tema vasto e complesso per il quale sono forniti riferimenti bibliografici che possono condurre a una conoscenza teorica e operativa appropriata.

13.1 Canali di comunicazione

L'analisi del livello di sicurezza dei canali di comunicazione è importante nel caso in cui le comunicazioni fanno uso di infrastrutture pubbliche o, più semplicemente, condivise con altri sistemi. In questi casi il traffico dati viene veicolato da canali di comunicazione accessibili anche a entità che non appartengono al sistema di controllo. Per questo motivo è importante realizzare le comunicazioni con meccanismi di protezione i quali altro non sono che algoritmi di criptaggio da applicare al flusso dei dati (cfr. [2]). Le forme con le quali è possibile realizzare questi sistemi sono molte come molti sono gli strumenti disponibili. Esempi di strumenti per la realizzazione di canali di comunicazione criptati sono il *Secure Socket Layer* e il *Transport Layer Security* (rispettivamente SSL e TLS, cfr. [4]). Questi protocolli consentono di stabilire connessioni autenticate e trasmissioni criptate con il metodo della doppia chiave (pubblica e privata) riducendo considerevolmente il rischio di interazioni indesiderate tra sistema di controllo ed entità estranee a esso. Il livello di sicurezza che può essere ottenuto dipende dal contesto nel quale si sviluppano le comunicazioni. In caso di comunicazioni su infrastrutture chiuse accessibili a un numero limitato di entità controllabili l'uso di protocolli sicuri è probabilmente un provvedimento eccessivo mentre l'uso di canali di trasporto pubblici lo rende spesso insufficiente.

I due protocolli criptati ai quali si è fatto riferimento rappresentano la risposta data ai problemi di sicurezza emersi con l'uso della rete internet, una realtà che fino a oggi è stata considerata estranea al mondo dei sistemi di controllo. Considerando l'uso dei canali di comunicazione pubblici, però, ci si riferisce alle infrastrutture di rete (realizzate solitamente in tecnologia TCP/IP) che i gestori pubblici rendono disponibili alle utenze come risorse condivise. Nei sistemi di controllo di dimensioni geografiche sono rari i casi nei quali risulta possibile realizzare una rete di campo privata, *ad hoc*, e l'uso di risorse pubbliche è una soluzione praticata. Quando questo avviene è necessario considerare il fatto che la protezione fornita con il servizio di trasporto non può essere ritenuta sufficiente per due ragioni fondamentali. In primo luogo essa ha carattere generalista nel senso che è pensata per servire utenze che hanno esigenze molto diverse tra loro e potrebbe essere inadatta ai vincoli imposti dal sistema di controllo. La seconda ragione discende dal fatto che la gestione del servizio di sicurezza di regola è a carico dello stesso fornitore del servizio di trasporto e comunque non dei responsabili della gestione del sistema di controllo. Tutto ciò comporta una minore specificità della protezione e la dispersione delle responsabilità di controllo imponen-

do la realizzazione di efficaci politiche di protezione in aggiunta a quelle di carattere commerciale.

L'importanza di una corretta gestione della sicurezza delle comunicazioni può essere considerata anche dal punto di vista dell'uso di tecnologie emergenti o consolidate ma non utilizzate nel settore dei sistemi di controllo. Un esempio è dato dalle tecnologie di radiocomunicazione, affermatesi in modo sorprendente con l'introduzione dei sistemi di telefonia radiocellulare. Sono molti i casi in cui il mancato uso di sistemi di comunicazione radio, dovuto alla intrinseca inaffidabilità dei medesimi, comporta soluzioni inefficienti per sistemi di controllo distribuiti. L'uso di adeguati strumenti di gestione della sicurezza permetterebbe, invece, di rivalutare il canale radio con grande vantaggio per l'efficienza e, non di rado, per l'economicità dei sistemi di controllo.

13.2 Strumenti d'interazione con il sistema

Il capitolo 9 ha trattato gli aspetti funzionali e tecnologici che riguardano la realizzazione degli strumenti d'interazione tra operatori e sistema di controllo. I problemi sollevati dall'interfaccia uomo-macchina in termini di sicurezza del sistema meritano senza dubbio un approfondimento. Gli elementi che caratterizzano l'interfaccia uomo-macchina come sicura o infida possono essere ricondotti a due categorie: l'accessibilità alle funzionalità del sistema e l'ambiguità delle stesse. In questa sezione viene affrontato il problema dell'accessibilità in considerazione del fatto che l'ambiguità delle funzionalità è tema affrontato in sede di descrizione delle buone pratiche di progettazione e realizzazione dei sottosistemi d'interazione uomo-macchina.

La gestione dell'accessibilità alle funzionalità del sistema consiste innanzitutto nella determinazione di “chi” può disporre di una sessione del sottosistema HMI, di “come” questi è autorizzato a farlo e, se possibile, di “quando” permetterglielo. Questa fase definisce le politiche di accesso che debbono essere realizzate in termini tecnologici dal sistema di controllo. Troppo spesso accade che il rapporto di causalità sia invertito e le politiche di accesso definite in base ai meccanismi che le piattaforme di sviluppo scelte mettono a disposizione degli sviluppatori. Questo diffuso fenomeno di adozione di metodologie “predefinite” di controllo degli accessi ha avuto momenti di grande fortuna ma è stato anche causa di gravi problemi di fronte ai quali il tema della sicurezza ha generato nuove e attente analisi. In particolare è stato un criterio efficace nei casi in cui gli strumenti utilizzati si sono rivelati validi

mentre ha portato a inquietudine e insicurezza quando le tecnologie hanno mostrato limiti metodologici o di realizzazione.

Il controllo degli accessi si fonda sui principi di autenticazione e autorizzazione e la sua forma più comune è il sistema basato sulla coppia “nome utente” e “parola chiave” (*username* e *password*) realizzato in tutti i sistemi operativi che aspirano a essere qualificati come sicuri. La decisione di uniformarsi a questo modello suggerisce l’adozione di strumenti che, inclusi nell’interfaccia utente, facciano uso del sistema di autenticazione integrato nel sistema operativo per sfruttare il livello di complessità, e quindi di sicurezza, raggiunto da questi. La soluzione può essere considerata molto efficiente e affidabile soprattutto nel caso in cui la piattaforma di sviluppo (intesa in questa fase come struttura costituita da sistema operativo, piattaforma di sviluppo di sistemi SCADA, software di gestione dei database, ...) risulta caratterizzata da un impianto realizzativo generale di qualità e orientato alla soluzione di problemi di sicurezza. Forse non è opportuno considerare sottintesa l’importanza della scelta della piattaforma operativa per la realizzazione dei sistemi di controllo; in questo senso il problema della sicurezza è solo uno dei molti da affrontare in sede di sviluppo se le basi sulle quali costruire un sistema che svolge funzioni molto delicate vengono individuate in una piattaforma inadeguata.

L’accesso controllato con il metodo di autenticazione e autorizzazione risolve soltanto il problema della determinazione di “chi” può accedere al sistema. Anche se questo in molti casi può bastare è interessante considerare la possibilità di controllare anche “come” e “quando” permettere gli accessi. I due controlli possono essere risolti, ancora una volta, utilizzando in maniera efficace gli strumenti di gestione delle utenze integrati nei sistemi operativi. Una personalizzazione raffinata di queste regole di accesso richiede, però, sovrastrutture da realizzare in sede di sviluppo dell’interfaccia utente. Per comprendere quest’ultimo punto è opportuno considerare il caso in cui si voglia permettere a un utente del sistema di operare su un insieme ristretto di pagine video; se l’interfaccia HMI viene realizzata come unico processore applicativo responsabile della produzione e della gestione di tutte le pagine video costituenti l’interfaccia utente è indispensabile realizzare un meccanismo di selezione che metta in relazione le immagini con l’utenza. Questo meccanismo di selezione non può essere realizzato se non come elemento interno all’applicativo che implementa l’interfaccia.

13.3 Infrastrutture

La sicurezza delle infrastrutture tecnologiche che realizzano il sistema è un problema che comporta riflessioni a vari livelli di analisi. Si può affrontare il tema in termini di protezione dalle intrusioni o di gestione degli eventi di guasto e in entrambi i casi fare considerazioni di carattere tecnologico, organizzativo o affrontare il problema in una visione complessiva. Il problema delle intrusioni indesiderate negli ambienti che ospitano le infrastrutture tecnologiche, problema comune a tutti i sistemi elettronici e informatici, deve essere affrontato soprattutto in termini organizzativi e deve condurre all'adozione di adeguate misure di protezione quali possono essere servizi di vigilanza, barriere architettoniche che regolano gli accessi e quant'altro. Il contributo che può essere dato dal progetto del sistema al raggiungimento di livelli di sicurezza accettabili coincide con l'attuazione delle politiche di gestione degli accessi alle funzionalità presentati in precedenza.

Un discorso diverso vale per la protezione intesa come realizzazione di sistemi che godono di predefiniti livelli di immunità dagli eventi di guasto (cfr. [6]). In questo caso il problema deve essere affrontato in termini sia tecnologici che organizzativi; esso coinvolge la scelta delle tecnologie, sia hardware che software, da utilizzare per la realizzazione del sistema ma al tempo stesso deve essere affrontato valutando correttamente le risorse infrastrutturali, umane e organizzative a disposizione del sistema costruendo. Il contributo della tecnologia al *disaster recovery*, questa è l'espressione comunemente utilizzata per identificare il problema, si basa sui concetti di ridondanza delle componenti, sia hardware che software, del sistema di controllo e di disponibilità di procedure e strumenti di "recupero" delle funzionalità rese indisponibili da eventi di danneggiamento.

La ridondanza consiste nella realizzazione di meccanismi che rendono le infrastrutture tra loro intercambiabili in modo trasparente alle funzionalità. Essa viene realizzata solitamente per le componenti più esposte al rischio di danneggiamento quali possono essere le apparecchiature periferiche, spesso collocate in ambienti in cui sono presenti elementi ostili a una corretta conservazione, i calcolatori che ospitano il sistema di elaborazione, le apparecchiature di gestione delle reti di comunicazione. Naturalmente la ridondanza non si realizza con il semplice allestimento di infrastrutture duplicate ma richiede una adeguata progettazione del sistema, finalizzata alla corretta realizzazione dei meccanismi responsabili della interoperabilità delle componenti "parallele". Molto spesso ciò che appare semplice a dirsi risulta essere problema complesso fin dalle prime fasi della progettazione: è bene tenere

a mente che la ridondanza appare cosa semplice a causa di una valutazione superficiale del problema e che una sua corretta realizzazione passa per una progettazione che la tenga adeguatamente in considerazione a tutti i livelli di analisi.

Accanto alle contromisure che possono essere adottate per evitare che il sistema di controllo possa andare incontro a interruzione del servizio è importante considerare l'importanza dell'allestimento di strumenti e procedure con le quali intervenire nel caso in cui il peggio dovesse accadere. Per far questo è importante analizzare il sistema in tutte le sue parti: infrastrutture architettoniche e tecnologiche, risorse umane e materiali. Sulla base di un'attenta analisi tecnica e organizzativa del sistema e delle risorse che contribuiscono al suo funzionamento è importante individuare i punti deboli e definire procedure di recupero che tengano in considerazione tutto quanto necessario a ricondurre a normalità lo stato di esercizio delle componenti danneggiate. In questo senso sono senza dubbio di aiuto soluzioni molto efficaci da valutare in fase di scelta delle apparecchiature hardware, un elevato livello professionale degli operatori coinvolti dalle procedure e l'efficienza delle procedure software di installazione e gestione delle risorse.

Parte IV
Conclusioni

Capitolo 14

Strumenti e competenze

In questa parte vengono introdotti gli strumenti e le competenze necessarie a una corretta progettazione e un efficace esercizio di un sistema SCADA. La trattazione ha carattere descrittivo e ha lo scopo di svolgere considerazioni di principio che possono essere prese a riferimento in sede di analisi dei metodi da utilizzare. Quanto riportato di seguito è il frutto dell'esperienza sviluppata nell'ambito della progettazione e realizzazione di sistemi SCADA e non rimanda a testi specializzati poiché questo genere di argomenti non è stato ancora affrontato in modo organico dalla letteratura tecnica. Questo stesso testo è nato come risposta alla evidente mancanza di pubblicazioni dedicate al mondo dei sistemi SCADA. La ragione principale per la quale questo tipo di sistemi non è oggetto di approfondimenti è nel fatto che essi sono il frutto di tecnologie introdotte soltanto di recente nel mondo dell'industria. Questo comporta la mancanza di metodi sperimentati e documentati di progettazione e, di conseguenza, errori progettuali che spesso diventano causa del fallimento delle realizzazioni, circostanza che ha prodotto anche una certa diffidenza nei confronti della loro efficacia.

Le difficoltà incontrate dai progettisti nella definizione del sistema SCADA costruendo sono indipendenti dal campo di applicazione del sistema anche se alcune caratteristiche da tenere in considerazione sono tipiche del processo che deve essere sottoposto a controllo. Nel seguito sono descritti alcuni aspetti fondamentali della progettazione di un sistema SCADA, aspetti che possono essere considerati come un percorso di riferimento per la progettazione. È bene ricordare, però, che la definizione di un metodo di progetto non è in grado di sostituire le esperienze personali dei progettisti, i quali continuano a essere fondamentali per la buona conduzione del progetto e per la validità del sistema. L'impossibilità di prescindere dall'aiuto di un esperto può essere considerata anche come limite all'introduzione dei sistemi SCADA nel mondo industriale e non, ma proprio questa necessità deve far riflettere

sulla possibilità che prodotti preconfezionati, cioè semplicemente da adattare alla propria realtà, siano in grado di garantire la realizzazione di un sistema SCADA efficiente. L'esperienza porta a dire che per la realizzazione di sistemi SCADA è meglio servirsi di un buon sarto che sia in grado di confezionare il *vestito su misura*, quello che si adatta alle caratteristiche fisiche particolari, piuttosto che acquistare un abito confezionato, anche se di qualità, nella speranza che si adatti perfettamente al corpo. Questa necessità deve essere valutata soprattutto nei casi in cui il processo da controllare sia un processo importante e particolare, oppure quando il sistema SCADA è destinato a integrarsi in un ambiente di lavoro ben definito nel quale non si vogliono produrre scostamenti dalle abitudini consolidate.

14.1 Definizione dei requisiti

Un'attività essenziale per la corretta progettazione di un sistema SCADA è la definizione di tutti i requisiti del sistema. I requisiti sono le richieste che il sistema deve soddisfare. I requisiti definiscono il sistema nel suo modo di comportarsi e costituiscono l'accordo tra il committente del sistema SCADA e chi lo realizza. Nel seguito il termine cliente definirà l'utente finale del sistema mentre il termine fornitore chi è chiamato a realizzarlo. Nella realtà questi attori non sono sempre rappresentati da un'unica entità, spesso sono presenti anche altre figure professionali che a vario titolo prendono parte alla definizione dei requisiti; la presenza di più attori, comunque, non impedisce di trattare l'argomento con un buon grado di generalizzazione.

Il modo migliore per iniziare un progetto è ottenere la definizione dei requisiti prima di iniziare la progettazione del sistema SCADA in quanto le scelte progettuali dovrebbero essere compiute in funzione delle richieste e non viceversa. Purtroppo questa "regola" viene spesso disattesa e la definizione procede in corso d'opera. Nel primo caso si può essere quasi certi che il sistema risultante sarà, nella migliore delle ipotesi, non aderente alle necessità dell'utente e il secondo caso, in alcune circostanze, potrebbe essere l'unico modo per poter procedere. In tutti i casi in cui il committente non ha una conoscenza dettagliata dei problemi che deve affrontare, quando il sistema si classifica come sistema sperimentale perché inserito in un ambito in cui esperienze pregresse non sono disponibili, quando si voglia procedere a una introduzione graduale del sistema SCADA, risulta necessario definire i requisiti in fasi successive. Questo modo di procedere, seppur possibile, per risultare efficace richiede uno sforzo nella fase di progettazione che deve

coinvolgere anche il cliente in quanto solo così si può riuscire a far convergere le necessità e le possibilità realizzative.

Che si possa procedere alla definizione dei requisiti in una unica fase iniziale oppure si debba procedere alla loro definizione in corso d'opera, il metodo più comune è avere una serie di incontri tra cliente e fornitore in modo da chiarire da una parte e dall'altra cosa si vuole ottenere e cosa si otterrà. Spesso le richieste del cliente debbono essere tradotte in linguaggio tecnico da parte del fornitore in modo da poter essere interpretate, così come le proposte del fornitore debbono essere tradotte in linguaggio comprensibile al cliente. Questa necessità di utilizzare un linguaggio comune fa nascere nel fornitore l'esigenza di coinvolgere per questa fase di definizione dei requisiti (ciò che è interessante analizzare in questo frangente) personale che sia in grado di mediare tra le richieste del cliente e quello che il fornitore è in grado di offrire, con lo sguardo rivolto a questioni non soltanto tecniche (ad esempio il contenimento dei costi entro limiti accettabili per il cliente). La cosa più importante in questo caso è non considerare nulla come scontato, sottinteso, non ben definito. La chiarezza deve essere la base di partenza per poter procedere alla definizione dei requisiti in modo che nessuno possa essere all'oscuro di quanto si richiede o si fornisce. Ciò è maggiormente importante se si considera che il periodo di realizzazione del sistema spesso trascorre senza contatti tra cliente e fornitore, contatti che si riattivano nel momento in cui il sistema è completo e pronto per essere installato.

Nel seguito sono elencati alcuni degli aspetti principali da definire come requisiti di base. È importante ricordare la natura del tutto generale dell'elenco proposto e il fatto che esso deve essere integrato con quanto l'esperienza del progettista può suggerire.

14.1.1 Definizione dei punti da sottoporre a controllo

La prima cosa che deve emergere nella definizione dei requisiti è il numero e la natura dei punti da controllare. Spesso si identificano questi punti con i punti di I/O (input/output), cioè i punti da prelevare direttamente dal processo. La definizione dei punti da prelevare e delle modalità di esecuzione di comandi e regolazioni è materia specifica degli esperti di processo. A questa fase deve quindi necessariamente partecipare una figura di questo tipo pena una errata interpretazione delle caratteristiche del processo da controllare. Altra figura professionale che potrebbe essere necessaria alla definizione dei punti di I/O è il progettista elettrico. Infatti i punti di I/O sono gestiti da dispositivi di acquisizione dati che sono in grado di interagire con processo e sistema per mezzo di segnali elettrici.

La definizione dei punti di I/O è fondamentale poiché da una parte permette di scegliere quali informazioni utilizzare per tenere sotto controllo il processo, dall'altra fornisce una prima, grossolana idea della dimensione del sistema. A volte, anche se con un grado di approssimazione non sempre accettabile, il numero dei punti di I/O viene fornito come unica informazione per la valutazione della complessità del sistema. La produzione di un'offerta economica per la realizzazione di un sistema SCADA sulla sola base di questa informazione, come risulterà chiaro nel seguito, non è possibile anche se non è raro trovare clienti che per scelta o per inesperienza non forniscono altre nozioni sulla natura del processo. In questi casi il consiglio è di insistere affinché si possano ottenere informazioni di maggior dettaglio in quanto l'offerta prodotta, o peggio il sistema fornito, sarebbe sicuramente inaccettabile.

14.1.2 Definizione funzionale

Una volta definiti i punti di I/O, l'informazione da ottenere dal cliente è come ritiene che il sistema debba funzionare per poter svolgere le sue funzioni. Questa definizione funzionale è di fondamentale importanza poiché attraverso di essa il cliente descrive cosa si aspetta che il sistema debba essere in grado di fare. Se le funzioni sono descritte in modo dettagliato, il cliente riuscirà a ottenere quanto si aspetta e il fornitore sarà in grado di scegliere il modo migliore per realizzare le funzioni desiderate.

Tra le funzioni che debbono essere definite ci sono sicuramente le procedure automatiche, le logiche di automazione, l'interazione del sistema con l'operatore, le informazioni che debbono essere oggetto di rapporti periodici, ecc. La conoscenza di queste informazioni permette al progettista di definire la tipologia degli apparati periferici e le funzioni che questi debbono essere in grado di svolgere. Anche il sistema centrale, per quanto riguarda la configurazione hardware, software, le risorse, il sistema operativo, ecc. è soggetto a scelte che possono essere determinate in base alle funzioni del sistema SCADA.

Alla fase di definizione funzionale del sistema, dalla parte del cliente, devono partecipare l'esperto di processo, gli operatori che giornalmente interagiscono con il sistema, i destinatari dei dati di riepilogo, ecc.

14.1.3 Definizione delle modalità di trasmissione dati

La definizione delle modalità di trasmissione dati in relazione alle caratteristiche del vettore di comunicazione è stata descritta in un capitolo dedicato. In questa parte si vuole invece identificare il problema di definizione della

trasmissione dati in relazione alle distanze, alla quantità di dati, alla disponibilità dei medesimi (intesa sia come periodo di acquisizione che come estensione temporale). La definizione di queste caratteristiche è un'attività che spesso può essere svolta con un certo grado di autonomia dal fornitore in quanto il cliente non sempre ha la capacità per entrare nel merito di aspetti estremamente tecnici. In alcuni casi invece le necessità esplicitate dal cliente sono indicative della soluzione da adottare (ad esempio può porre vincoli sulla posa di cavi e imporre l'uso di vettori radio). In ogni caso il cliente deve essere adeguatamente informato della scelta effettuata o, nel caso siano plausibili più alternative, delle caratteristiche positive e negative delle soluzioni proposte. Tutto questo ha lo scopo di essere il più possibile trasparenti in merito a quanto verrà realizzato.

14.1.4 Definizione delle informazioni da archiviare

Una volta che sono stati definiti i punti da acquisire e le funzioni del sistema, dovrà essere determinato l'insieme delle informazioni che debbono essere archiviate al fine di consentire la conservazione della storia del processo. La scelta delle informazioni da archiviare deve essere curata perché da essa dipende la scelta del sistema di archiviazione e delle risorse da destinare allo stesso. Si è visto in precedenza che l'adozione di un data base relazionale è scelta obbligata per realizzare il motore di archiviazione. Si tenga presente però che ogni motore DBMS ha le sue caratteristiche peculiari e un costo a esse associato. È inutile dimensionare il sistema SCADA con l'intenzione di archiviare tutti i dati trattati con la frequenza tipica dell'acquisizione. Procedere su questa strada farebbe arrivare facilmente ad avere un sistema di archiviazione che da solo occuperebbe la maggior parte del sistema SCADA sia economicamente sia in termini di risorse destinate. Per poter dimensionare correttamente il sistema di archiviazione si dovrebbe prima di tutto definire cosa fare con i dati archiviati: servono per avere un riepilogo del funzionamento del sistema? servono per poter ricreare degli scenari fuori linea per permettere lo studio a posteriori di eventi? servono per ragioni legali? Ognuna di queste domande porta a soluzioni diverse da caso a caso che solamente l'esperienza permette di definire. Dalla parte del cliente è necessario che l'esigenza finale dell'archiviazione dei dati sia esplicitata. Per fare questo le figure interessate potrebbero essere i gestori del sistema e il settore gestionale dell'azienda (che potrebbe aver bisogno di questi dati per svolgere il proprio lavoro).

14.1.5 Definizione delle criticità

Una delle parti più importanti nella fase di definizione dei requisiti è la definizione delle criticità del sistema. Le criticità del sistema, comprensibilmente, definiscono in massima parte capacità che il sistema SCADA deve avere e che non possono prescindere dalle caratteristiche del processo controllato. Se ad esempio si deve realizzare un sistema SCADA in ambito petrolchimico si devono prevedere delle misure di sicurezza che in altri ambiti sono del tutto superflue. È caratteristica specifica di ogni processo controllato la definizione delle criticità, ma gli argomenti che debbono essere presi in considerazione sono comuni a tutti i sistemi. In funzione del sistema specifico saranno poi associati dei gradi di importanza ad ogni singola voce.

In generale gli aspetti critici da tenere in considerazione nella definizione dei requisiti possono essere riassunti nell'elenco seguente:

- sicurezza intrinseca (MTBF, SO)
- ridondanza
- disponibilità
- permessi operatore

Le professionalità da coinvolgere nella definizione di questi aspetti sono tutte quelle che a qualsiasi titolo hanno responsabilità nella definizione del processo di controllo; si va quindi dall'esperto di processo al responsabile degli operatori, dal responsabile dei sistemi informatici al responsabile della manutenzione, della produzione fino al responsabile di stabilimento.

14.1.6 Definizione dell'interoperabilità con sistemi esterni

È stato più volte fatto cenno al fatto che il sistema SCADA sempre più spesso viene visto come un componente di un più complesso sistema necessario alla gestione di processi che dal singolo processo industriale possono arrivare a interessare la funzione gestionale e di definizione delle strategie aziendali. In quest'ambito la definizione dell'interoperabilità con altri sistemi è parte fondamentale per il successo del sistema SCADA. Se si vuole avere un sistema che sia il più possibile integrabile con altri sistemi aziendali si deve tenere in considerazione che il sottosistema di interazione può essere sviluppato in due modi: con l'uso di sistemi proprietari integrati tra loro o con l'adozione di sistemi che espongono interfacce standard.

Nel primo caso si potrebbe avere la possibilità di sfruttare la facilità di integrazione di prodotti che sono stati pensati per interagire. Con l'utilizzo di questa soluzione c'è sicuramente un vantaggio in termini di semplicità e velocità di realizzazione, vantaggio che però comporta una notevole dipendenza da un unico fornitore. Questa dipendenza, oltre a tutti gli aspetti negativi che sono facilmente comprensibili, comporta anche un altro aspetto che a volte non viene adeguatamente valutato. Il fornitore unico potrebbe avere dei prodotti ottimi per alcuni dei componenti dell'intero sistema, ma per altri componenti potrebbero essere disponibili prodotti di altri fornitori dotati di caratteristiche migliori di quello proposto. Seguendo questa strada difficilmente si riuscirebbe ad avere il meglio per ogni componente.

Meglio quindi utilizzare prodotti che abbiano interfacce standard e integrare tra loro prodotti di fornitori diversi. La standardizzazione delle interfacce è un problema che sempre più spesso trova una risposta nei fornitori che aderiscono a standard comuni. Gli standard possono essere definiti in base a quanto il mercato fa emergere come standard (i cosiddetti *standard de-facto*), oppure perché istituti preposti alla loro definizione ne hanno creati (*standard de-iure*). Comunque sia, l'adesione a standard, possibilmente aperti, da parte dei fornitori è garanzia del fatto che un prodotto valido rappresenta una scelta potenzialmente più efficace rispetto all'uso di un prodotto "chiuso". Sulla base di queste considerazioni si può dire che è sempre opportuno progettare prodotti che siano il più possibile aperti. Il fornitore di sistemi che segue questa regola è in grado di rispondere alle esigenze del cliente facendo leva su esperienza e abilità, elementi di garanzia per il futuro del fornitore e per la soddisfazione del cliente.

La definizione delle necessità di interoperabilità è compito che interessa tutti i settori di un'azienda in quanto le informazioni che possono essere estratte da un sistema SCADA potrebbero essere utilizzate proficuamente in moltissimi ambiti aziendali.

14.2 Fase di definizione dell'architettura

Una volta definiti tutti requisiti si può passare alla fase progettuale vera e propria. Durante questa fase tutte le indicazioni ottenute a livello di analisi e definizione dei requisiti devono trovare una soluzione nella scelta dell'architettura del sistema. Con architettura del sistema si intende l'insieme di componenti che lo costituiscono. I macro componenti di un sistema SCADA sono stati già ampiamente descritti in tutto l'arco di questa trattazione; ora si definiscono nel dettaglio i singoli componenti (a partire dai macro

componenti fino ad arrivare a quelli più piccoli) avendo cura di assicurare che:

- ogni requisito del sistema sia preso in adeguata considerazione
- le interfacce tra i vari componenti siano definite e consistenti

È questa la fase di progettazione del sistema SCADA vera e propria, dove la competenza, l'esperienza, ma anche la fantasia del progettista trovano sfogo e determinano le soluzioni a tutti i requisiti del sistema. In questa fase il contatto tra il progettista e il cliente del sistema è meno intenso in quanto il cliente verrà interessato nella fase finale del progetto, quando il fornitore andrà a presentare la soluzione ideata per una sua approvazione formale. Il coinvolgimento del cliente in questa fase, sia per ragioni storiche sia per ragioni di autonomia progettuale, è sempre vista come un rallentamento della fase creativa e in qualche caso anche come un ostacolo vero e proprio. Questa convinzione, invece, dovrebbe essere vista con sospetto poiché un coinvolgimento del cliente nelle prime fasi di definizione dell'architettura del sistema è un costume che l'esperienza suggerisce di adottare.

Tra gli obiettivi del progetto, accanto a quelli che sono gli obiettivi formali (fornitura adeguata alle richieste, rispetto dei tempi e dei costi), il fornitore deve avere anche la soddisfazione del cliente. Spesso quest'aspetto viene trascurato correndo il rischio che sistemi perfettamente adeguati e rispettosi delle specifiche di progetto siano rigettati dal cliente. Questo perché può accadere che le richieste del cliente non rispecchiano le sue reali esigenze (magari perché formulate male) e impediscono al fornitore di produrre una soluzione corretta. Ma anche da parte del fornitore vengono commessi errori che portano a realizzazioni inadeguate. Ad esempio spesso si tenta di forzare i clienti a recepire come adeguata la fornitura di una soluzione che in realtà non lo è (magari perché per il fornitore è comodo offrire qualcosa di cui già dispone e che in qualche modo fornisce la risposta a un sottoinsieme significativo di requisiti). Accade che il fornitore pensi di poter partire da una soluzione di carattere generale che sia adattabile a tutte le circostanze e poi invece si trova di fronte a richieste talmente particolari da non essere trattabili con una soluzione generalista (o trattabili a costo di soluzioni economicamente non convenienti, poco eleganti o addirittura non del tutto funzionanti).

Per ovviare a questi errori è necessario coinvolgere il cliente già nelle prime fasi di progettazione del sistema, anche se questo può essere visto come uno sforzo inutile. Lo "sforzo inutile" compiuto per non sentire, a progetto finito, le comprensibili lamentele del cliente che chiede l'aggiunta

di una piccola funzione che aveva dimenticato di chiedere come requisito e che non immagina possa comportare la revisione dell'intera architettura del sistema.

Certo, il coinvolgimento del cliente richiede uno sforzo anche da parte sua, sforzo che non sempre è disposto a fare. Certo, i tempi di progettazione potrebbero allungarsi oltremodo. Certo, il gruppo di progetto deve avere la capacità di confrontarsi con figure professionali che non sono in grado di parlare lo stesso linguaggio e un'opera di mediazione tra le parti deve essere messa in conto. Ma a fronte di questo costo iniziale quante discussioni, contestazioni, rivalse potrebbero essere risparmiate! Il mondo dei sistemi SCADA è un mondo particolare, che si occupa di una materia che si può ritenere ancora giovane, con una storia non sufficientemente lunga da consentire che siano chiari i problemi da affrontare e che per essi già sia stata realizzata una soluzione adeguata. Se a questo si unisce il fatto che un sistema SCADA spesso si inserisce in realtà industriali che già dispongono un metodo di lavoro, che da questo nuovo oggetto non deve essere sconvolto, si capisce che si è di fronte all'esigenza di fornire un *vestito su misura* e non un abito preconfezionato buono per tutte le esigenze. Quando anche il cliente è in grado di apprezzare i vantaggi di una soluzione di sartoria rispetto a un abito da confezione tutte le parti in gioco ne traggono benefici. È necessario però che il fornitore si faccia carico anche dell'opera di convincimento nei confronti di clienti meno propensi, facendo leva su argomentazioni quali ad esempio il fatto che il cliente ottiene un sistema vicino alle sue esigenze e di cui ha conoscenza anche negli aspetti più nascosti (in virtù della sua partecipazione alla progettazione). Il fornitore da parte sua può guadagnare la fiducia del cliente e realizzare un sistema in grado di consolidare il rapporto commerciale.

Metodi specifici da utilizzare per la fase di progettazione, sia che questa venga fatta con il metodo tradizionale, sia che segua quanto detto in precedenza, non ce ne sono. Di base rimane il fatto che il progetto migliore è quello che parte dalla definizione minuziosa dei requisiti. Non ci si deve spaventare del fatto che la fase progettuale possa andare per le lunghe, non si deve cedere al prurito del programmatore che vuole scontrarsi il prima possibile con il codice. D'altra parte non si può neanche allungare la fase progettuale oltremodo e anzi spesso il cliente ha bisogno di vedere dei prototipi di quanto si sta analizzando in modo da avere un riscontro oggettivo delle ipotesi formulate. Il consiglio che può derivarne è cercare di realizzare il sistema per gradi, costruendo l'architettura dal basso in modo da poter vedere nel più breve tempo possibile come si presenterà il sistema finito. Questa immediatezza del risultato potrebbe da una parte suggerire al cliente che quanto il

fornitore afferma ha anche un risultato pratico (evitando considerazioni del tipo “finora ho visto solo carta, quando mi farete vedere qualcosa di funzionante?”), dall’altra offrire al fornitore un riscontro diretto della correttezza delle scelte progettuali adottate. In questo modo errori progettuali potrebbero essere individuati e risolti tempestivamente, cioè quando ancora questo non richiederebbe uno sforzo eccessivo. Perché tutto ciò sia realizzabile è necessario spingere l’acceleratore sulla fase di test del sistema la cui descrizione è oggetto della seguente sezione.

14.3 Fase di verifica

I metodi classici di realizzazione di un sistema informatico prevedono che la fase di definizione dei requisiti sia seguita dalla fase progettuale alla quale seguirà poi la fase di realizzazione. Solamente al termine di questa fase si procederà alla realizzazione di test del sistema (alla presenza del cliente). Questo metodo, detto *waterfall* in quanto ogni fase inizia solo quando la precedente è terminata, prevede che il sistema sia verificato alla presenza del cliente per mezzo dei test di accettazione. Questi test sono costituiti da procedure volte alla verifica del rispetto di tutti i requisiti richiesti, che quindi costituiscono il limite contrattuale di fornitura. La fase di definizione delle procedure di test dovrebbe essere cura del cliente in quanto attraverso i test egli accetta il sistema dichiarandolo adeguato a quanto richiesto. Più realisticamente si può dire che il fornitore produce delle procedure di test e le sottopone al cliente che si riserva di accettarle. Come già detto i test servono a verificare che il sistema abbia recepito tutti i requisiti. Così come la cura nella definizione dei requisiti è di interesse di entrambi (cliente e fornitore), anche la fase di definizione delle procedure di test è fondamentale per tutte le parti coinvolte. L’accuratezza, la completezza, la varietà delle procedure di test deve essere garanzia che nessun aspetto del sistema venga tralasciato. Dal lato del cliente questo garantisce che il sistema sia realmente adeguato a quanto richiesto, dal lato del fornitore il test deve essere visto come il momento in cui si verifica che quanto realizzato non contenga errori sfuggiti al controllo. Un approccio superficiale ai test da parte del fornitore può comportare l’installazione e la messa in esercizio di sistemi contenenti errori o lacune che può essere molto difficile affrontare una volta reso operativo il sistema.

In generale quindi la definizione dei test è operazione importante perchè garanzia del buon funzionamento del sistema. Ma come si può essere certi che il sistema sia verificato nel suo reale comportamento? Quando il siste-

ma andrà in esercizio si troverà a lavorare in condizioni simili a quelle nelle quali è stato verificato? È noto che in molti casi l'ambiente di test può essere influente sull'oggetto del test tanto da comprometterne il funzionamento. Come si può scongiurare questa ipotesi in un sistema SCADA? In realtà non c'è un modo per ovviare a questi problemi. Si procede considerando che il miglior modo per verificare il funzionamento di un sistema è farlo in un ambiente che sia il più possibile simile a quello nel quale si troverà a funzionare. Per far questo si dovrebbe vedere il sistema SCADA come una scatola nera e inserirla in un contesto che sia il più possibile rappresentativo della realtà fisica nella quale si troverà a operare. Questo può essere fatto realizzando simulatori del processo, delle infrastrutture di comunicazione e quant'altro rimane al di fuori della scatola nera. L'adozione di simulatori il cui funzionamento è ben noto permette di avere indicazione delle risposte fornite dal sistema SCADA anche in condizioni limite. Infatti si possono realizzare simulatori in grado di creare un carico di sistema ben preciso e verificare il comportamento del sistema in risposta a questo carico, verificare come questo comportamento varia al variare del carico, definire i limiti del sistema anche in relazione alla sua scalabilità. La realizzazione di simulatori è attività che spesso non viene adeguatamente considerata nella fase di realizzazione del sistema SCADA, ma è fondamentale per tutte queste ragioni. Essi svolgono la parte del leone nella fase di verifica del sistema e spesso sono presi anche come metro di giudizio. Come giudicare un fenomeno se il metro che uso non fornisce un'indicazione chiara e riproducibile della misura effettuata?

Il termine riproducibile non è stato utilizzato a caso. La riproducibilità dei test effettuati è fondamentale per la verifica della reazione del sistema sottoposto ad una determinata procedura di test. È fondamentale che il sistema sottoposto agli stessi stimoli reagisca nella stessa maniera. Se così non fosse non si potrebbe definire deterministico il suo comportamento, che quindi dovrebbe essere considerato inaccettabile (discorso diverso va fatto per i sistemi esperti che modificano le loro risposte in base alla storia delle situazioni osservate in precedenza).

Le procedure di test sono svolte sostanzialmente in due fasi distinte: in una prima fase il cliente verifica il sistema presso il fornitore, in una seconda fase il sistema viene installato presso il cliente e i test vengono ripetuti nella sede definitiva. La prima fase prende il nome di FAT (*Factory Acceptance Test*), la seconda prende il nome di SAT (*Site Acceptance Test*). L'unica differenza che esiste tra le due fasi è il fatto che il sistema in un caso si trova nell'ambiente in cui è stato sviluppato, nell'altro si trova nell'ambiente nel quale opererà normalmente. Entrambe le fasi vengono realizzate alla

presenza del cliente e del fornitore e producono evidenze formali dei risultati dell'esecuzione di ogni procedura di test. Si concludono solamente quando il cliente riterrà superato il test con risultati accettabili (rispetto a quanto richiesto). Ogni volta che l'esecuzione di una procedura di test non dovesse presentare risultati soddisfacenti a causa di malfunzionamenti del sistema, questi debbono essere corretti al fine di realizzare quanto richiesto. In base alla gravità del malfunzionamento presentato, il singolo test o l'intera fase di test di accettazione dovrà essere sospesa in attesa della correzione. Dopo ogni correzione si dovrà procedere alla riesecuzione della procedura di test incriminata (o dell'intero set di procedure) fino a quando tutti i risultati saranno considerati accettabili. Al termine della fase SAT, il sistema è pronto per l'installazione e l'avvio della fase di utilizzo.

Quanto fin qui descritto aderisce a quello indicato come metodo waterfall di produzione di un sistema informatico. Senza addentrarci nelle motivazioni è necessario dire che questo metodo, nel corso degli anni, si è rivelato inefficace. Principalmente si è osservato che il metodo non coincide con quanto in realtà avviene nei rapporti usuali tra fornitore e cliente. Non è possibile lavorare su fasi di progetto chiuse che non prevedono interazioni con le altre e che debbono fornire risultati ottimi pena il buon esito delle fasi successive. La realtà ci parla di sistemi che sono spesso in divenire e lo sforzo per rappresentare questi sistemi con il metodo descritto è tale da far ritenere lo sforzo da compiere sproporzionato rispetto al risultato da raggiungere.

Si è detto che il cliente deve essere coinvolto direttamente, il più possibile, in tutte le fasi del progetto. Non è esente da questa considerazione la fase di verifica del sistema. Già nella fase di progettazione si è parlato della necessità di fornire in tempi brevi soluzioni, anche di tipo prototipale, che siano in grado di allineare le richieste con quanto si andrà a fornire. La verifica di queste soluzioni può essere vista come la realizzazione della fase di accettazione del sistema da parte del cliente, non in un unico passo compiuto al termine della realizzazione del sistema ma durante la fase di realizzazione stessa, in modo da avere riscontri immediati sulla validità delle scelte compiute. Cambia l'importanza dei test. Essi diventano funzionali all'assicurazione di livelli misurabili di qualità della fornitura. Cambia anche l'approccio ai test troppo spesso vissuti come se fossero esami essendo, al contrario, parte integrante del processo di progettazione e realizzazione. Garantirsi la possibilità di confrontare immediatamente quanto realizzato con quanto richiesto è un modo efficace per prendere tempestivamente contromisure se attese e risultati non coincidono; in più permette di superare tutte le naturali difficoltà che possono rivelarsi gravissime, o addirittura insormontabili, se affrontate

con eccessivo ritardo.

14.4 Fase di installazione

Una volta che il sistema ha raggiunto una fase di maturazione tale da consentire il suo utilizzo, si inizia la fase di installazione in campo. Quando il grado di maturazione può definirsi accettabile? Semplicemente quando le funzionalità minime indispensabili per l'utilizzo del sistema sono state realizzate e verificate con il cliente. Il consiglio è di non iniziare la fase di installazione fino a quando il sistema presenta problemi che ne compromettono l'usabilità. I problemi che non si risolvono prima dell'installazione sono sempre difficili da risolvere durante questa fase e nelle successive. Spesso l'installazione e l'avvio dell'esercizio del sistema impediscono l'allestimento di ambienti di simulazione mirati alla riproduzione dei problemi emersi, precludendo la possibilità di un'analisi efficace e tempestiva del malfunzionamento. Inoltre l'inizio della fase di installazione comporta tempi di correzione dei malfunzionamenti ridotti a causa delle crescenti aspettative del cliente che vede il proprio obiettivo a portata di mano. È noto che la fretta non aiuta a trovare la soluzione ottimale dei problemi. Anche l'installazione può essere sorgente di malfunzionamenti che vanno a sommarsi a quelli noti. Il continuo presentarsi di problemi, unitamente alla difficoltà che si incontra nella loro risoluzione, stimola nel cliente la percezione che il sistema non sia adatto, percezione che può degenerare in malcontento dell'utilizzatore e manifestarsi in ulteriori pressioni nei confronti del fornitore. Si genera quindi un circolo vizioso che non è certamente quanto si ci si attende quando la tranquillità e i nervi saldi possono essere determinanti nella soluzione dei problemi incontrati.

Per evitare tutto questo è necessario essere sicuri che tutto quello che si andrà ad installare sia pronto per essere portato in ambiente di integrazione. La valutazione di quando si è in grado di installare deve necessariamente tenere in considerazione fattori quali la stabilità del sistema, le prestazioni, la disponibilità, la sicurezza. Il limite temporale che viene stabilito contrattualmente non è stato incluso tra i fattori discriminanti in quanto si sta facendo un'analisi qualitativa del prodotto fornito, ma non c'è dubbio che dovrà essere tenuto nella dovuta considerazione (in ogni caso c'è sempre qualcuno pronto a ricordarci che siamo soggetti a scadenze contrattuali). Il rispetto dei tempi contrattuali non deve essere messo in secondo piano rispetto agli altri fattori. Deve anzi essere considerato anch'esso indice della qualità del prodotto. Il consiglio è di dare la giusta importanza a tutti i fattori e non valutare il rispetto religioso dei tempi quale indice della capacità produttiva (cosa che

invece viene spesso osservata nei rapporti tra cliente e fornitore). Quando l'approssimarsi della scadenza di consegna genera una eccessiva pressione nel gruppo di progetto può accadere che piccoli problemi vengano ingigantiti e nuovi problemi creati. Inoltre la fretta spesso viene usata a giustificazione di una fase di analisi dei problemi che potrebbe risultare lacunosa tanto da produrre soluzioni inefficaci (per cui un problema deve essere affrontato più volte senza mai trovare la soluzione definitiva) o addirittura dannose (in quanto altre parti del sistema risultano danneggiate dalla soluzione adottata). In ogni caso la fretta nella risoluzione di un problema è un problema a propria volta che accresce il rischio di ritardi nella consegna (cioè esattamente quello che si voleva evitare). Tutto ciò senza considerare l'impatto psicologicamente negativo che un sistema malfunzionante ha nei confronti sia del gruppo di progetto che nel cliente.

Comunque, senza entrare nello specifico, è bene considerare che quanto più il sistema viene verificato prima di essere installato, minore sarà il tempo di installazione. Considerando che l'installazione è un'attività per sua natura costosa (si svolge presso il cliente e quindi si debbono considerare i costi di trasferta del personale interessato), si comprende che dovrebbe essere interesse di tutti condividere questa considerazione.

La capacità di valutare in situazione di contingenza quale parametro sacrificare in vista di un miglioramento complessivo, non è cosa che possa far parte di trattazioni di questo tipo. Solamente l'esperienza può portare a valutare caso per caso quale contromisura adottare nell'ottica di raggiungere i risultati migliori. E proprio in questa considerazione nasce la definizione delle competenze necessarie in fase di installazione. La complessità delle situazioni da affrontare, il fatto che si lavora spesso con tempi stretti, fuori sede, senza la disponibilità degli strumenti migliori, la necessità di integrarsi con altri fornitori e quindi di affrontare situazioni non previste, suggerisce di utilizzare personale esperto. Il gruppo di installazione può essere composto anche da personale inesperto se guidato da un coordinatore esperto.

Dal punto di vista degli interventi in campo è bene cercare di seguire una filosofia che permetta di procedere per passi successivi in modo da suddividere l'impegno di installazione in diverse aree. Ad esempio si potrebbe procedere all'installazione degli apparati periferici e, per ognuno di essi, alla verifica della corrispondenza dei dati acquisiti con quelli previsti. Questa attività che prende il nome di *battitura del campo* consente di verificare che a livello di informazioni acquisite ci sia corrispondenza tra quanto progettato e quanto realizzato in campo. Avere la sicurezza che un dato sia esattamente quello che ci aspettiamo è fondamentale per assicurare il funzionamento del sistema

(si pensi a cosa può succedere se l'invio di un comando ad un dato organo corrisponda in realtà comandarne un altro!). Qualche volta semplici errori di cablaggio sono facilmente individuabili a livello di apparato di acquisizione dati, mentre diventano quasi impossibili da individuare a livello di sistema centrale.

Al termine della battitura del campo, si può procedere con la fase di collegamento degli apparati periferici con il sistema centrale. In questa fase il controllo si concentra sulla parte di telecomunicazione che permette l'interazione tra sistema centrale e periferico. In questo caso è bene attivare un singolo apparato periferico alla volta e verificare che tutte le funzioni siano correttamente eseguite. Per consentire l'esecuzione di prove senza rischio di effettuare comandi è utile utilizzare meccanismi realizzati con lo scopo di evitare che i comandi impartiti dal sistema raggiungano gli organi di campo. In questo caso si parla di *prove in bianco* il cui fine è quello di assicurare che lo scambio dati tra sistema centrale e periferia avvenga correttamente. Una volta superata questa fase si ha la certezza che ogni dato gestito dal sistema e che ogni comando impartito corrisponderà con quanto desiderato. Non resta che mettere in servizio il sistema e verificare che tutto funzioni regolarmente.

14.5 Fase di messa in servizio

La fase di messa in servizio non è altro che l'attivazione del sistema e l'uso per le normali operazioni quotidiane. È possibile che in una prima parte di questa fase sia richiesta la presenza di personale della ditta fornitrice con il compito di introdurre gli operatori all'uso del sistema. Questa richiesta viene fatta soprattutto quando le dimensioni del sistema sono ragguardevoli o quando il passaggio dalla gestione tradizionale al controllo automatizzato può risultare traumatico. In qualche caso questa fase inizia con la fase d'installazione, nella quale può accadere che alcune componenti del sistema si rendano disponibili prima che l'intero sistema lo sia. Gli utenti possono prendere confidenza con queste parti di sistema avvalendosi di indicazioni sul funzionamento che possono essere fornite dal personale destinato all'installazione.

In qualche caso è richiesto un periodo di dimostrazione della disponibilità del sistema al fine di accertare la capacità di funzionare con continuità. Questo periodo viene definito come un monte ore nelle quali il sistema deve comportarsi secondo quanto richiesto e nel quale ogni intervento di manutenzione o aggiornamento deve essere adeguatamente giustificato. In particolare si possono evidenziare due tipi di problemi che richiedono l'intervento da parte del fornitore: problemi di tipo *bloccante* e problemi di tipo *non bloccante*.

Al primo tipo fanno capo tutti quei problemi che non consentono l'utilizzo del sistema fino a che un provvedimento risolutivo non venga attuato. Si tratta di problemi gravi che richiedono l'intervento immediato e la soluzione in tempi brevissimi. Dal manifestarsi del problema fino alla sua risoluzione il periodo di dimostrazione viene sospeso. Di solito si stabilisce un tempo massimo di intervento trascorso il quale, se il problema persiste, la sospensione dell'esercizio si trasforma in interruzione. Per riportare il sistema in attività sarà necessario eliminare i malfunzionamenti, procedere alle opportune verifiche e riavviare l'esercizio in regime di verifica della disponibilità. In questo caso il periodo di dimostrazione riparte dall'inizio. Se invece il problema viene risolto nel tempo massimo fissato, si ricomincia a utilizzare il sistema senza che il tempo speso per la soluzione del problema venga tenuto in conto per il calcolo della disponibilità.

Nel caso di problemi non bloccanti, il manifestarsi di uno di questi non comporta la sospensione del periodo di dimostrazione, ma semplicemente il tracciamento del problema manifestato per una sua soluzione in tempi che non sono preventivamente determinati (il sistema è in grado di funzionare anche senza che il problema sia risolto). In qualche caso si fissa un numero massimo di problemi non bloccanti aperti contemporaneamente. Superato questo numero i problemi vengono considerati di tipo bloccante e si procede secondo quanto già descritto.

Il periodo di dimostrazione è un periodo molto importante sia dal punto di vista del cliente che da quello del fornitore. In questo periodo il cliente deve avere assicurazione del corretto funzionamento del sistema in tutte le sue funzioni. Per il fornitore è invece l'esame che porta al primo giudizio complessivo sul valore del prodotto. Anche la capacità del fornitore di affrontare con efficacia e rapidità i problemi che dovessero emergere è motivo di valutazione della qualità della fornitura (intesa come sistema e servizi accessori), in particolare rispetto ai requisiti di manutenibilità definiti in fase progettuale. Non si deve mai sottovalutare la facilità di intervento sul sistema fornito né rispetto alla risoluzione dei problemi né rispetto all'implementazione di nuove funzioni richieste dal cliente.

La particolare natura di questa fase suggerisce al fornitore di disporre di un gruppo di lavoro che conosca il sistema nel dettaglio, pena l'inefficacia e la lentezza degli interventi. È bene non disperdere le conoscenze del sistema una volta iniziata la fase di installazione ma mantenere vivo il gruppo di progetto (magari riducendolo alle sole figure chiave) anche per un primo periodo di esercizio. L'esperienza porta a dire che la maggior parte degli interventi di manutenzione, correzione, aggiornamento realizzati su un sistema si verifica

nella prima parte della sua vita operativa. Le competenze che il gruppo di supporto all'installazione e alla messa in esercizio deve avere sono tali e tante da coprire tutti gli ambiti nei quali il sistema si muove. Importantissime in questa fase sono quelle figure professionali che hanno una visione d'insieme del sistema, della sua architettura e delle sue funzioni. Spesso le ragioni di successo di un sistema risiedono nella capacità del fornitore di offrire soluzioni rapide alle richieste del cliente e figure che conoscano nel dettaglio il sistema si possono rivelare indispensabili allo scopo.

14.6 Fase di esercizio e manutenzione

La fase di esercizio coincide con l'utilizzo del sistema per le funzioni che ne hanno determinato la realizzazione. La manutenzione è l'attività con cui si garantisce il funzionamento ottimale del sistema. Questo per mezzo della risoluzione dei problemi, dell'evoluzione delle funzioni implementate e dell'introduzione di nuove funzioni. In questa fase, che si svolge lungo l'intero corso della vita del sistema, il cliente può avvalersi o meno del fornitore. Solitamente il supporto del fornitore viene richiesto quando le dimensioni del sistema impedirebbero una manutenzione realizzata con i mezzi a disposizione del cliente. Per sistemi di piccole dimensioni il tema della manutenzione viene affrontato come un costo inutile. Il consiglio è di non considerare mai inutile questo supporto e, quale che sia la volontà di avvalersene, di creare una struttura interna in grado di intervenire sul sistema. Questo tipo di struttura consente al proprietario del sistema di ottenere due importanti risultati. In primo luogo una maggiore conoscenza delle caratteristiche attuali e potenziali del sistema e del patrimonio di conoscenza che esso è in grado di creare e gestire, il tutto al riparo da sguardi indiscreti che inevitabilmente il fornitore porta con sé. In secondo luogo l'indipendenza dal supporto del fornitore, frequente causa di vincoli sull'evoluzione e sulla personalizzazione del sistema.

Da parte del fornitore, se coinvolto nella fase di esercizio e manutenzione, è bene mantenere un gruppo interno che si occupi della gestione di questa fase. Le capacità che il gruppo deve esprimere sono analoghe a quelle utilizzate nella fase di messa in servizio in quanto il grado di conoscenza del sistema ha effetti diretti sul livello di qualità della gestione. In questo caso i tempi di intervento per la soluzione dei problemi o per la realizzazione di nuove funzioni non sono stringenti, quindi si può lavorare anche per la formazione di nuovo personale. Lo stesso personale sarà riutilizzabile dall'azienda nel caso di fornitura di altri sistemi o di rifacimento dello stesso.

La manutenzione non deve essere percepita né dal cliente né dal fornitore come una fase in cui si attende la comparsa di un problema per procedere all'intervento risolutivo. In questa fase dovrebbero essere realizzate tutte le modifiche necessarie al raggiungimento del livello ottimale di efficienza e usabilità. Modifiche che possono trovare le loro richieste solo dopo che gli operatori ne abbiano fatto conoscenza grazie all'uso quotidiano. In definitiva un sistema in esercizio non deve essere visto come un'infrastruttura che bisogna solamente mantenere in vita. Il sistema deve essere visto come un'entità della quale alimentare una crescita funzionale al potenziamento dell'efficacia del processo controllato e dell'attività del personale coinvolto nel controllo. Perché questo possa avvenire è necessario che si stabilisca un rapporto di fiducia tra il cliente e il fornitore, rapporto che deve manifestarsi in una collaborazione mirata al miglioramento del sistema.

Il miglioramento delle funzioni del sistema, l'introduzione di nuove funzioni, l'osservazione e il miglioramento delle prestazioni sono attività da ricondurre alla fase di manutenzione. Tra queste alcune possono essere svolte soltanto osservando il comportamento del sistema in esercizio, altre possono essere svolte soltanto in ambienti distinti da questo. Ciò che risulta opportuno è l'allestimento di un sistema in tutto simile a quello in servizio, tranne che per l'interazione con il processo controllato. Si tratta di un ambiente di test gemello del sistema in linea per il quale il processo da controllare è sostituito da un sottosistema di simulazione. Una soluzione di questo genere viene vissuta, naturalmente, come un inutile costo da sovrapporre a quello affrontato per la realizzazione del sistema. Un modo per contenere il peso del costo di un ambiente di test è collocare questo ambiente all'interno dei provvedimenti da adottare per la definizione delle procedure di *disaster recovery*, infatti la dotazione di una copia fedele del sistema in esercizio può essere un valido strumento per la definizione di tali procedure.

Capitolo 15

Evoluzione dei sistemi SCADA

Nel corso della trattazione è stato fatto più volte cenno a possibili evoluzioni dell'architettura e delle funzionalità dei sistemi SCADA. Queste hanno preso forma nel corso degli anni, e continuano a emergere, grazie allo sviluppo delle tecnologie e a un diverso modo di interpretare il significato dei sistemi di controllo nell'ambito dei sistemi informativi aziendali. Il sistema SCADA segue linee di trasformazione che lo stanno conducendo a una integrazione sempre maggiore con sistemi affini, con i sistemi di gestione e di supporto alla decisione. Allo stesso tempo l'uso di nuove tecnologie consente di definire architetture con le quali è possibile realizzare nuove funzionalità o perfezionare quelle esistenti, fino a giungere alla formulazione di una nuova definizione dei sistemi SCADA che consideri l'acronimo realmente rappresentativo di funzionalità e non di un tipo di sistema, funzionalità rese disponibili nella forma di servizi personalizzati erogati da un "provider".

La trattazione che segue ha lo scopo di introdurre elementi di riflessione sul significato dei sistemi SCADA nel panorama tecnologico attuale secondo i caratteri appena delineati. È bene sottolineare che alcuni aspetti dell'evoluzione trattati nel seguito del capitolo si riferiscono a fenomeni d'integrazione tra sistemi che pur essendo in atto da molti anni non hanno ancora condotto alla definizione di modelli evoluti di progettazione. La causa di questo ritardo non risiede nel limite imposto dalle tecnologie ma da un'analisi superficiale delle esigenze che emergono dai settori aziendali che non realizzano i processi produttivi intesi in senso fisico. In sintesi si può dire che i produttori di sistemi e piattaforme di sviluppo SCADA non hanno ancora compreso in modo compiuto il ruolo dei sistemi informativi e l'importanza che rivestono all'interno di questi i sistemi di controllo. L'inerzia con la quale il mondo dei sistemi SCADA affronta questi temi è in parte giustificata dal fatto che al già elevato livello di complessità che caratterizza la realizzazione di sistemi di controllo si vanno aggiungendo nuovi elementi di complessità. Per questi

è necessario ricorrere a competenze e strumenti di progettazione e sviluppo estranei al mondo dei sistemi di controllo e a tecniche di progettazione che permettano di instaurare la collaborazione tra i diversi settori aziendali con lo scopo di definire un modello d'integrazione che sia frutto di una visione d'insieme.

15.1 Controllo di processo e sistemi informativi aziendali

Il primo elemento sul quale procedere per dare una descrizione delle linee evolutive seguite dai sistemi SCADA è l'integrazione con sistemi concorrenti finalizzata alla realizzazione di sistemi informativi aziendali evoluti. In realtà una sezione dedicata all'integrazione intra-aziendale prende posto anacronisticamente in un capitolo dedicato all'evoluzione dei sistemi di controllo. Ciò che deve essere visto come ancora in fase di sviluppo è il metodo di progetto da utilizzare quando uno degli obiettivi è l'integrazione dei sistemi. È necessario iniziare a considerare concretamente la necessità di dedicare risorse fin dalle prime fasi di progettazione all'analisi delle esigenze d'integrazione che altrimenti sono destinate a emergere a cose fatte. L'analisi deve condurre alla definizione delle interfacce, delle strutture dati, delle informazioni da scambiare, degli strumenti da utilizzare ma anche del personale che deve essere coinvolto in questa attività e in quella successiva di esercizio del sistema. Autorizzazioni, competenze, responsabilità, potenzialità e limiti del sistema, risorse logistiche sono elementi che richiedono un impegno di analisi al quale è bene iniziare a dedicare attenzione.

L'obiettivo di un impegno di questo genere è un sistema SCADA in grado di interagire con sistemi di controllo concorrenti e con sistemi comunemente classificati come "gestionali". Un esempio di architettura alla quale è possibile giungere seguendo questa strada è riportato in figura 15.1. La figura mostra sistemi per i quali sono state definite modalità d'interazione con il risultato di giungere alla realizzazione di un unico sistema informativo aziendale. Quest'ultimo si comporta come sistema di supervisione e controllo dal punto di vista del processo ma allo stesso tempo opera come strumento d'interazione tra il processo medesimo e le strutture di gestione aziendale.

Stabilita la comunicazione tra le entità riportate in figura è possibile capire quale sia la portata del passo compiuto analizzando le funzioni svolte solitamente da un sistema di gestione aziendale, in particolare quelle che richiedono la disponibilità dei dati trattati dal sistema SCADA. Uno dei motivi per i quali vengono allestiti i sistemi gestionali è l'automazione della gestione

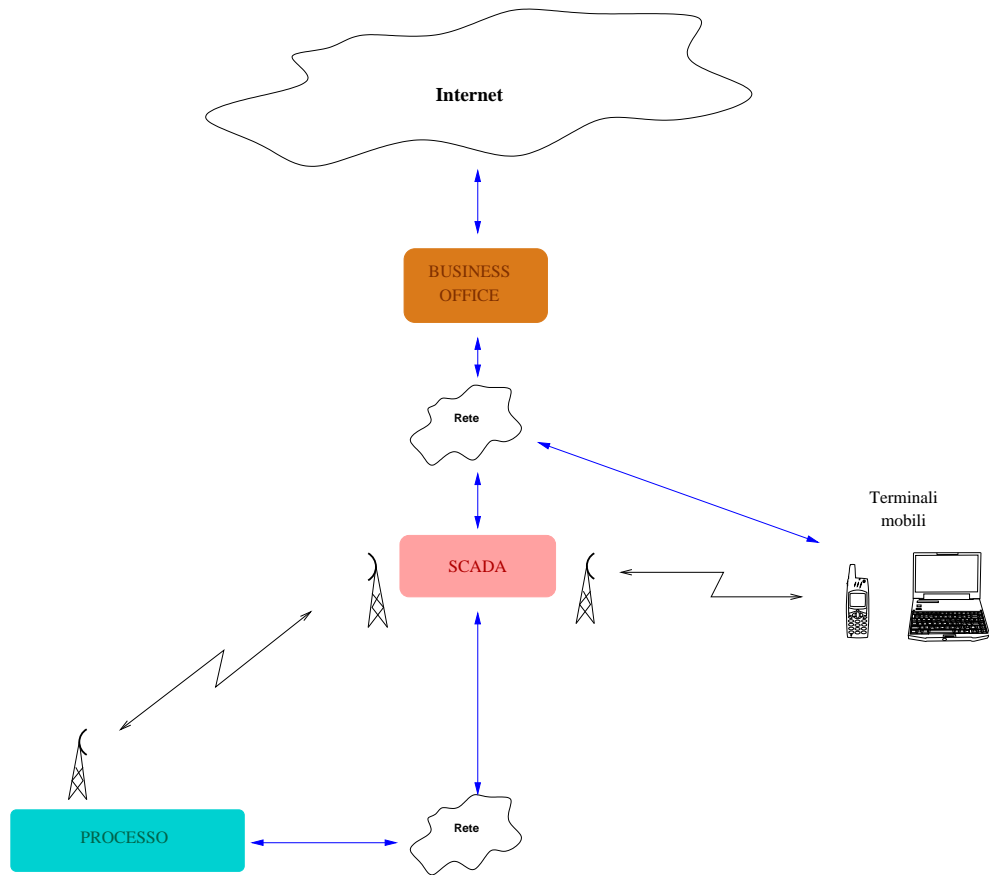


Figura 15.1: Architettura di sistema integrato di controllo, gestione e fornitura di servizi

del magazzino. In un'azienda di produzione che abbia in magazzino materie prime e prodotto finito può essere utile rendere disponibile al sistema gestionale le informazioni relative all'evoluzione del processo produttivo che consentono una valutazione delle quantità che escono dal magazzino sotto forma di materia prima e di quelle che vi entrano nella forma di prodotto finito. Ciò che viene fatto dal sistema gestionale per l'interazione tra azienda e mondo esterno (fornitori e clienti) può essere fatto per l'interazione tra magazzino e processo produttivo. Qualcuno direbbe "deve essere fatto" poiché la determinazione automatica delle dimensioni dei flussi di materia prima e prodotto finito è una funzione che ha carattere sia organizzativo che contabile e può contribuire in modo determinante all'innalzamento dell'efficienza aziendale. La disponibilità di queste informazioni unita alla disponibilità di dati relativi agli stati di esercizio del processo produttivo, inclusi gli stati di fermo, permette di condurre analisi di carattere statistico finalizzate alla conoscenza dell'effettivo livello di produttività dell'azienda. Se gli stati di fermo vengono qualificati opportunamente secondo classificazioni dei diversi guasti possibili, e delle attività accessorie degli operatori, è possibile determinare l'influenza che ha sulla produzione il sopraggiungere di un particolare tipo di guasto e contenere i danni con l'allestimento di opportune contromisure.

I guasti, al pari dell'ordinaria manutenzione, comportano l'interruzione dell'attività del processo e l'impegno di operatori competenti per il ripristino delle funzioni. Il doppio effetto prodotto da guasti e manutenzioni è l'interruzione della produzione unita all'impegno di personale: due elementi di interesse vitale per un'azienda. Rendendo disponibili al sistema gestionale le informazioni relative allo stato del processo, includendo quelle relative agli stati di fermo, è possibile giungere a una corretta gestione dei fermi in termini di impegno del personale (i sistemi gestionali vengono utilizzati anche per organizzare turni, formazione del personale, ...) e di materiale necessario alle attività di ripristino delle funzioni del processo. Ciò fatto rimarrebbe poco da aggiungere per ottenere quanto necessario a una gestione programmata degli interventi di manutenzione, coordinata con la normale attività lavorativa degli operatori e con la disponibilità del materiale necessario agli interventi. A quanto detto si unisce il fatto che una corretta gestione dei dati aziendali conduce alla disponibilità di informazioni che possono essere opportunamente archiviate e utilizzate in fase di analisi per la comprensione di fenomeni che riguardano la vita dell'intera azienda su intervalli di tempo che possono coprire l'intera durata dell'impegno produttivo realizzato.

Considerazioni del tutto analoghe a quelle presentate finora valgono per gli aspetti dell'attività aziendale che riguardano i rapporti stabiliti con il

mondo esterno per mezzo delle tecnologie offerte dalla rete internet. L'erogazione di servizi per mezzo delle tecnologie web (vendita, ordinazioni, assistenza, ...) può essere affrontata soltanto quando lo consente il livello raggiunto nell'integrazione tra i sistemi di controllo delle attività produttive e quelli destinati alla gestione aziendale. A titolo di esempio può essere considerato il servizio di vendita "online" nel quale un aggiornamento costante della disponibilità dei prodotti offerti permette al sistema di vendita di soddisfare in modo adeguato le esigenze dei clienti. Allo stesso modo un corretto uso dei dati relativi alle ordinazioni e di quelli riguardanti l'attività produttiva consentono ai settori gestionali di compiere le scelte migliori in fase di pianificazione delle attività.

Per quel che riguarda gli effetti causati dall'evoluzione tecnologica sullo sviluppo dei sistemi SCADA si può dire che il contributo più significativo è stato dato dalle tecnologie di telecomunicazione. La diffusione e il perfezionamento di reti basate sullo standard *IEEE 802*, detto "ethernet", ha consentito di disporre di infrastrutture di comunicazione affidabili, flessibili, modulari e gestibili per le quali sono stati definiti protocolli di comunicazione specifici dei diversi ambiti del controllo di processo. L'introduzione di questo tipo di reti è stato un fattore determinante soprattutto nello sviluppo dei sistemi di dimensioni geografiche, per i quali è possibile sfruttare la tecnologia TCP/IP per mezzo delle infrastrutture rese disponibili dai fornitori di servizi di telecomunicazioni. Un significato altrettanto importante sembra che lo avranno i servizi di radiocomunicazione. I sistemi radiocellulari per le comunicazioni tra entità remote di un sistema di dimensioni geografiche e le reti *wireless* per le comunicazioni locali si stanno imponendo, anche se ancora soltanto sulla carta, come soluzioni efficienti a problemi di connettività che a dire il vero sono già affrontati con successo. Quello che la telefonia cellulare ha consentito di realizzare è un nuovo insieme di funzioni che in qualche modo cambia l'organizzazione del lavoro. Oggi è possibile associare a stati del sistema di controllo per i quali è necessario l'intervento di un operatore l'invio di messaggi *sms* di richiesta d'intervento. Questo consente di realizzare sistemi non presidiati capaci di richiamare l'attenzione di operatori impegnati in altre attività su stati di esercizio che non possono essere gestiti con procedure automatiche.

Tornando al modello di sistema integrato riportato in figura 15.1 è opportuno ripetere che un sistema integrato dovrebbe essere progettato tenendo in considerazione tutte le componenti che lo costituiscono, per evitare di commettere tutti gli errori che vengono compiuti quando si sceglie di rimandare l'analisi dei requisiti dell'integrazione al momento in cui la realizzazione delle

singole parti è completata. La complessità di un sistema integrato e la difficoltà di coordinare il lavoro di settori aziendali molto diversi tra loro porta, solitamente, a resistenze che impediscono una corretta e tempestiva analisi dei requisiti d'integrazione, pregiudicando la possibilità di ottenere una realizzazione valida dal punto architeturale ed efficiente dal punto di vista pratico. Queste resistenze possono essere più o meno forti e la loro intensità fornisce una misura della capacità delle aziende di affrontare un percorso che non si limita all'automazione aziendale ma coinvolge l'intera struttura con lo scopo di razionalizzare le attività e, se possibile, migliorarle in termini di efficienza e di qualità del lavoro.

15.2 Dai sistemi ai servizi SCADA

La direzione presa dall'evoluzione delle tecnologie informatiche, delle telecomunicazioni e dei dispositivi di campo ha condotto alla formulazione di ipotesi di architetture dei sistemi SCADA, in qualche caso tradotte in realtà industriali, caratterizzate dalla trasformazione dell'impegno di realizzazione di un sistema di controllo nella soddisfazione di esigenze di carattere funzionale. L'approccio tradizionale al problema della supervisione è basato sulla realizzazione di sistemi dedicati, per i quali la responsabilità di gestione è a carico dei responsabili del processo controllato. Il percorso che conduce al compimento del progetto di automazione parte dall'individuazione di esigenze di controllo per giungere all'installazione del sistema. Le fasi intermedie comportano la definizione dei requisiti funzionali, di affidabilità, disponibilità e sicurezza, la determinazione delle caratteristiche dell'architettura tecnologica, la realizzazione delle componenti software, la configurazione (programmazione e installazione) delle apparecchiature periferiche, la messa in esercizio. Il coinvolgimento del committente è necessario in tutte le fasi nelle quali debbono essere compiute scelte di tipo funzionale, tecnologico, logistico, organizzativo. Il committente è costretto a essere protagonista di fasi di realizzazione per le quali potrebbe essere sollevato dall'impegno in virtù di un uso più intelligente delle tecnologie e di una diversa concezione del sistema di controllo.

Questa diversa concezione si basa sulla possibilità di rendere disponibili funzionalità fruibili dal committente senza che questi sia costretto a realizzare impianti tecnologici dedicati. L'impegno dei responsabili di processo può essere limitato alla definizione delle specifiche (funzionali, prestazionali, di affidabilità, ...), alla gestione dei problemi di carattere organizzativo generati dall'introduzione del sistema di controllo, al compimento delle scelte

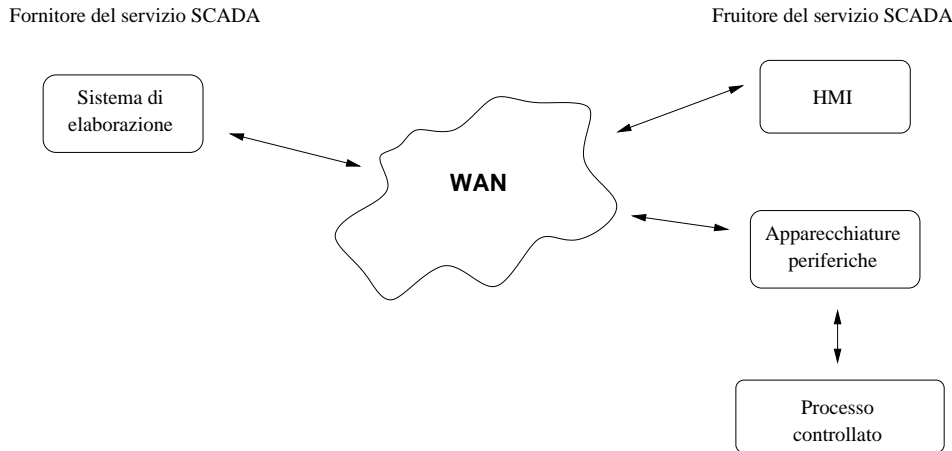


Figura 15.2: Architettura per l'erogazione di servizi SCADA

logistiche legate all'installazione delle apparecchiature periferiche. La responsabilità delle scelte architettoniche, della progettazione hardware e software, della realizzazione, della messa in esercizio e della manutenzione del sistema di elaborazione può essere assunta dal solo fornitore. Il sistema SCADA si sposta dal committente al fornitore e da sistema di controllo si trasforma in erogazione di servizi per la realizzazione di attività di controllo. L'unico elemento di intrusione del sistema nella realtà del processo che continua a sopravvivere è l'infrastruttura delle apparecchiature periferiche. Per queste è comunque possibile sollevare il committente da impegni di gestione, soluzione ampiamente praticata nel mondo dell'industria. Una rappresentazione della struttura necessaria alla realizzazione di servizi SCADA è riportata in figura 15.2.

La rete di campo, realizzata in prossimità del processo, è accessibile per mezzo dei canali di comunicazione comunemente utilizzati nei sistemi di controllo distribuiti. L'uso di servizi di trasporto pubblici, di servizi basati su comunicazioni radio o di altri tipi di canali comporta le stesse considerazioni fatte nell'analisi delle soluzioni adottate dai sistemi tradizionali. Il sistema di elaborazione viene realizzato e gestito per mezzo di infrastrutture tecnologiche di proprietà del fornitore il quale, dovendo fornire un servizio e non un prodotto, è tenuto a onorare il contratto in termini di funzioni erogate e prestazioni garantite. L'elemento che chiude la catena di controllo è l'interfaccia uomo-macchina che deve essere resa disponibile al committente nelle sedi da questo destinate all'attività di supervisione e controllo.

Un sistema dotato di queste caratteristiche differisce da un'installazione tradizionale per alcuni importanti elementi. Il primo riguarda la realizzazione dell'interfaccia uomo-macchina che in questo caso risulta vincolata a

tecnologie di scambio dati tra entità remote. Prestazioni, sicurezza e affidabilità sono aspetti che debbono essere analizzati con particolare attenzione. Il secondo riguarda la gestione dei dati acquisiti e prodotti dal sistema. L'adozione di un servizio SCADA da parte di un committente comporta la condivisione con il fornitore dell'accesso ai dati. Il fornitore risulta essere addirittura il depositario, in senso fisico, di un patrimonio di conoscenza che in molti casi può essere considerato come elemento strategico nell'attività che ha portato alla realizzazione del sistema. Un altro elemento da tenere in considerazione riguarda la perdita di competenze interne all'azienda o all'ente che commissiona un servizio di questo tipo. Ciò che inevitabilmente accade è l'allontanamento degli addetti a supervisione e controllo dalla realtà del processo e dei sistemi e la conseguente incapacità di giudicare con adeguato senso critico il livello di qualità del controllo attuato dal sistema e dei servizi che lo realizzano. Un'ultima importante considerazione attiene l'interesse che committenti e fornitori hanno nei confronti dei servizi SCADA. I primi hanno la necessità di realizzare un sistema che sia in grado di soddisfare le esigenze di controllo del processo del quale sono responsabili. I secondi hanno l'interesse di ottenere la massima soddisfazione del cliente sia in termini di servizio erogato che di costi esposti. Gli interessi delle due parti trovano un punto d'incontro soddisfacente fin quando il fornitore risulta in grado di realizzare un servizio adeguato alle esigenze del committente all'interno di economie di scala realizzate per mezzo della definizione di servizi standard. Quando il processo presenta caratteristiche poco comuni o non gestibili con i servizi erogati, accade che l'incontro tra domanda e offerta porta alla personalizzazione del servizio soltanto se questa viene considerata come un'evoluzione che può essere integrata nell'offerta di servizi complessiva (la quale ha inevitabilmente carattere generalista).

Glossario

affidabilità (in inglese *reliability*) capacità di un sistema di operare correttamente espressa come percentuale del tempo di esercizio

alarm overriding metodo di gestione automatica degli allarmi prodotti da un sistema che prevede l'inibizione della generazione degli allarmi nei casi in cui le condizioni al contorno la rendono inutile o dannosa

banco di controllo banco dotato di tasti, leve e bottoni per mezzo dei quali gli operatori possono impartire comandi per il controllo del processo

database runtime base dati di supporto all'attività del sistema di controllo solitamente caratterizzata da tempi di accesso molto bassi

DCS (*Distributed Control System*) sistema di controllo affine al sistema SCADA ma caratterizzato da un elevato livello di decentramento delle funzioni

disponibilità percentuale di tempo per la quale deve essere assicurato l'esercizio del sistema

HMI (*Human-Machine Interface*, interfaccia uomo-macchina) insieme di strumenti di interazione tra operatore e sistema

pagine video rappresentazioni dello stato del processo realizzate per mezzo di strumenti software; queste hanno sostituito la tecnologia del quadro mimico

PID componenti hardware o software che realizzano logiche di controllo costituite da azioni proporzionali, derivate e integrali; sono il primo e più semplice risultato della teoria dei controlli automatici

PLC (*Programmable Logic Control*) dispositivi di acquisizione dati dotati di strumenti per la programmazione finalizzati alla realizzazione di logiche di controllo

porta punto di accesso di un sistema di elaborazione o di un dispositivo per mezzo del quale è possibile attivare uno scambio dati per la fruizione di un servizio

quadro mimico componente dell'interfaccia uomo-macchina che permette la rappresentazione dello stato del processo per mezzo di schemi realizzati con strumenti elettromeccanici

quadro sinottico vedi quadro mimico

RDBMS (*Relational Database Management System*) sistema di gestione di basi di dati organizzate secondo il modello relazionale

realtime attributo di un sistema capace caratterizzato da tempi di elaborazione trascurabili se confrontati con le caratteristiche dinamiche del processo controllato

trend storici diagrammi cartesiani di tipo *tempo/valore* rappresentativi dell'andamento che ha caratterizzato variabili del sistema in periodi di esercizio che appartengono al passato

video wall matrice di schermi o display che realizza un sistema di visualizzazione di dimensioni configurabili in funzione di esigenze specifiche; nel caso dei sistemi di controllo raggiunge, solitamente, le dimensioni delle pareti interne agli ambienti nei quali è allestito il centro di controllo

Bibliografia

- [1] Camil Demetrescu, Irene Finocchi, Giuseppe F. Italiano. *Algoritmi e strutture dati*, volume 1. McGraw-Hill, 2004.
- [2] D. Welsh. *Codes and Cryptography*, volume 1. Oxford University Press, 1988.
- [3] Daniela Dorbolò, Andrea Guidi. *Guida a SQL*, volume 1. McGraw-Hill, 2 edition, 2004.
- [4] Eric Rescorla. *SSL and TLS: Designing and Building Secure Systems*, volume 1. Addison-Wesley Professional, 2000.
- [5] G.F. Franklin, J.D. Powell, A. Emami-Naeini. *Feedback Control of Dynamic Systems*, volume 1. Addison-Wesley, 4 edition, 2002.
- [6] Michael Wallace, Lawrence Webber. *Disaster Recovery Handbook, The: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets*, volume 1. AMACOM, 2004.
- [7] N.S. Nise. *Control Systems Engineering*, volume 1. Wiley and Sons Inc, 3 edition, 2000.
- [8] Paolo Atzeni, Stefano Ceri, Stefano Paraboschi, Riccardo Torlone. *Basi di dati - Modelli e linguaggi di interrogazione*, volume 1. McGraw-Hill, 2002.
- [9] Raghu Ramakrishnan, Johannes Gehrke. *Database management system*, volume 1. McGraw-Hill, 3 edition, 2003.
- [10] R.C. Dorf, R.H. Bishop. *Modern Control Systems*, volume 1. Addison-Wesley, 2001.
- [11] S. Gai, P.L. Montessoro, P. Nicoletti. *Reti locali: dal cablaggio all'internetworking*, volume 1. SSGRR, L'Aquila, 1997.

- [12] Andrew S. Tanenbaum. *Reti di Computer*, volume 1. Prentice Hall International, 3 edition, 1997.
- [13] VISUAL Project. VISUAL web-enabled open source SCADA and HMI software for LINUX. sourceforge.net/projects/visual.

Parte V
Appendici

Appendice A

GNU Free Documentation License

Version 1.2, November 2002

Copyright ©2000,2001,2002 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document free in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of copyleft, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The **Document**, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as **you**. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A **Modified Version** of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A **Secondary Section** is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The **Invariant Sections** are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The **Cover Texts** are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A **Transparent** copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or

discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not Transparent is called **Opaque**.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The **Title Page** means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, Title Page means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section **Entitled XYZ** means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as **Acknowledgements**, **Dedications**, **Endorsements**, or **History**.) To **Preserve the Title** of such a section when you modify the Document means that it remains a section Entitled XYZ according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute.

However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling

the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled History, Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled History in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network

locations given in the Document for previous versions it was based on. These may be placed in the History section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

- K. For any section Entitled Acknowledgements or Dedications, Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled Endorsements. Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled Endorsements or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled Endorsements, provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled History in the various original documents, forming one section Entitled History; likewise combine any sections Entitled Acknowledgements, and any sections Entitled Dedications. You must delete all sections Entitled Endorsements.

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an aggregate if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled Acknowledgements, Dedications, or History, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License or any later version applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright ©YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled GNU Free Documentation License.

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the with...Texts. line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.