La convergenza IT/OT nei sistemi di comando e controllo centralizzato delle linee metropolitane di Milano

IT/OT convergence in centralised command and control systems of underground lines in Milan

Dott. Ing. Stefano Pasetti[*]

Sommario - I sistemi di automazione industriale (identificabili con il termine "Operational Technology", OT), in particolar modo i sistemi SCADA utilizzati per il controllo e la supervisione degli impianti industriali e delle public utilities (energia elettrica, gas acqua, trasporti), sono sempre più pervasi da componentistica hardware e software proveniente dal settore dell'Information Technology (IT).

Questo processo di integrazione, conosciuto con il termine "convergenza IT/OT", è portatore di significativi benefici, sia in termini tecnici che gestionali. Si pensi ad esempio alla maggiore facilità con cui i sistemi di produzione possono essere interconnessi con le altre funzioni aziendali (approvvigionamenti, amministrazione, vendite, …), oppure alla possibilità di utilizzare hardware e software standard di mercato e largamente diffuso, abbandonando progressivamente i sistemi proprietari che hanno per tanto tempo caratterizzato il mondo OT.

Per contro, il continuo rinnovamento tecnologico del settore IT, spesso guidato da logiche di mercato più che da reali esigenze degli utilizzatori, non sempre risulta in linea con le primarie esigenze del settore OT, indirizzato tipicamente a garantire la stabilità e l'affidabilità dei propri impianti. Alcune criticità (sicurezza informatica, aggiornamenti software, cicli di vita dei componenti) vanno pertanto adeguatamente gestite per non inficiare i benefici effetti dell'integrazione.

Inoltre, la convergenza IT/OT non è rappresentabile esclusivamente come un processo di trasformazione tecnologica, ma riguarda anche azioni di "change management", organizzativo e culturale, di due settori che storicamente sono sempre stati distinti, sia per le diverse provenienze formative-professionali che per le differenti culture aziendali acquisite negli anni.

Summary - *Industrial automation systems (identifiable with the term "Operational Technology", OT), especially the SCADA systems used for the control and supervision of industrial plants and public utilities (electricity, gas, water, transport), are increasingly permeated with hardware and software components from the Information Technology (IT) field.*

This integration process, known as "IT/OT convergence" carries significant benefits, both in technical and management terms. For example, the increased ease with which production systems can be interconnected with other business functions (purchasing, administration, sales,...), or the ability to use standard market hardware and software and widely distributed, gradually abandoning proprietary systems that have for so long characterised the OT world.

By contrast, the continuous technological renewal of the IT industry, often driven by market logic rather than the real needs of the users, is not always in line with the primary needs of the OT sector, typically addressed to ensure the stability and reliability of its plants. Some criticalities (computer security, software updates, component life cycles) should be properly managed so as not to affect the beneficial effects of integration.

Moreover, IT/OT convergence is not exclusively representable as a technological change process, but also concerns organisational and cultural "change management" operations, of two sectors that historically have always been distinct, both for educational and professional backgrounds and for different corporate cultures acquired over the years.

The article presents these issues from the perspective of the maintenance manager of centralised command and control systems of subway lines in Milan, analysing the technological evolution of OT systems and the effects that

(*) Responsabile Direzione Sistemi Mobilità e Telecomunicazioni di ATM S.p.A.

(*) *Head of Mobility and Telecommunications Systems Department of ATM S.p.A.*

L'articolo presenta questi aspetti dal punto di vista del manutentore dei sistemi di comando e controllo centralizzato delle linee metropolitane di Milano, analizzando l'evoluzione tecnologica dei sistemi OT e gli effetti che tale processo di trasformazione ha portato all'interno dei reparti tecnici aziendali.

1. La convergenza IT/OT

Nel settore dell'automazione industriale, i sistemi di controllo e di supervisione (di seguito genericamente identificati con il termine OT, Operational Technology), sono utilizzati per garantire il funzionamento delle linee di produzione. Questi sistemi possono assumere differenti configurazioni, ma in genere sono costituiti da componenti di campo, sensori e attuatori, direttamente connessi alle linee di produzione, dai dispositivi elettronici di controllo (PLC – Programmable Locic Controller) e dai relativi sistemi di regolazione e supervisione centralizzata (SCADA - Supervision Control and Data Acquisition, DCS - Distribuited Control System, a seconda degli ambienti industriali in cui vengono utilizzati), che consentono di remotizzare il controllo e la supervisione degli impianti all'interno delle cosiddette "Sale Operative".

Anche il settore delle utilities (energia elettrica, gas, acqua, trasporti), che eroga servizi vitali per il benessere e la sicurezza dell'intera collettività fa largo uso di questi sistemi, che al pari delle infrastrutture controllate, diventano essi stessi infrastrutture critiche: si pensi ad esempio alle reti di distribuzione elettrica, agli acquedotti, ai gasdotti e agli oleodotti, oppure alle reti di trasporto ferroviario o metropolitano e ai relativi sistemi di controllo che ne garantiscono il funzionamento e la sicurezza.

Originariamente i sistemi OT erano sistemi tradizionalmente "chiusi": i sensori e gli attuatori venivano direttamente cablati ai loro controllori e questi erano interconnessi alle control room attraverso linee dati (bus di campo o linee punto-punto) che utilizzavano protocolli proprietari e che risultavano completamente separate dalle altre reti dati aziendali, tipicamente LAN (Local Area Network) appartenenti al mondo dell'IT (Information Technology). Anche nelle Sale Operative spesso si utilizzavano sistemi e logiche elettromeccaniche per realizzare le interfacce uomo-macchina: un esempio tipico è costituito dai quadri sinottici a mosaico, con spie luminose per rappresentare gli stati ed i segnali di allarme e commutatori o pulsanti utilizzati per inviare comandi. Successivamente, anche con il progressivo diffondersi dei computer, i sistemi di controllo usavano elaboratori basati su protocolli e software proprietari, che di fatto li rendevano sistemi isolati. Conseguentemente, i reparti tecnici dedicati ai sistemi OT erano strettamente legati ai settori della produzione ed erano prevalentemente costituiti da personale orientato alla manutenzione degli impianti di campo, con estrazione tipicamente elettromeccanica, in quanto tale era la natura prevalente degli impianti di loro competenza.

this transformation process has brought within the corporate technical departments.

1. IT/OT convergence

In the industrial automation sector, control and supervision systems (hereinafter generically identified with the term OT, Operational Technology), are used to ensure the operation of production lines. These systems may take different configurations, but generally consist of field components, sensors and actuators, directly linked to production lines, by electronic control devices (PLC – Programmable Logic Controller) and their control and centralised supervision systems (SCADA Supervision Control and Data Acquisition, DCS - Distributed Control System, depending on the industrial environments in which they are used) that allow the remote control of industrial plants within the so-called "Operational Rooms".

Even the utilities sector (electricity, gas, water, transport), which provides vital services for the welfare and security of the whole community makes extensive use of these systems, which, like a controlled infrastructure, become themselves critical infrastructures: the electricity distribution networks, aqueducts, oil pipelines, gas pipelines and rail or metropolitan transport networks and their control systems that guarantee the functionality and safety thereof are an example.

Originally OT systems were traditionally "closed" systems: sensors and actuators were wired directly to their controllers and these were interconnected to control rooms through data lines (field buses or point to point lines) that used proprietary protocols and that were completely separate from other corporate data networks, typically Local Area Network (LAN) belonging to the world of Information Technology (IT). Even in Operational Rooms electromechanical and logical systems were often used to create human-machine interfaces: a typical example consists of the interlocking control panels, with warning lights to represent statuses and alarm signals and switches or buttons used to send commands. Subsequently, with the gradual spread of computers, control systems used computers based on protocols and proprietary software, which actually made them isolated systems. Consequently, technical departments dedicated to OT systems were closely linked to production areas and were mostly composed of field maintenance-oriented staff, with typical electromechanical extraction, as such was the prevailing nature of the systems of their competence.

Contacts with the enterprise IT sector were virtually absent or however greatly reduced.

Over the past decade there has been a gradual transformation of all the components constituting OT Systems: sensors and actuators have gradually become smarter, with greater intelligence and linked to their controllers no longer only through digital or Analogue Input/Output lines, but with more standard and faster field buses until becoming

I contatti con il settore IT aziendale erano praticamente assenti o comunque estremamente ridotti.

Nel corso dell'ultimo decennio si è assistito ad una progressiva trasformazione di tutti i componenti costituenti i sistemi OT: i sensori e gli attuatori sono via via diventati sempre più smart, dotati di maggiore intelligenza e connessi ai loro controllori non più solamente attraverso linee di Input/Output digitale o analogico, ma con bus di campo sempre più standard e veloci, fino a diventare vere e proprie reti locali. Il protocollo TCP/IP (Transmission Control Protocol/Internet Protocol, identifica la suite di protocolli più utilizzata nell'ambito delle reti locali) non è più di pertinenza esclusiva delle reti office aziendali ma si è ormai diffuso nel mondo delle reti dei sistemi OT. Anche i calcolatori utilizzati, sia a livello di server che di postazioni operatore, così come i sistemi operativi ed i data base, sono diventati gli stessi di quelli utilizzati dall'IT aziendale per l'erogazione dei servizi di corporate: back office, amministrazione, acquisti, vendite.

I sistemi operativi VMS o UNIX su cui erano stati costruiti tanti sistemi SCADA degli anni '90 sono stati progressivamente sostituiti dai sistemi Microsoft Windows e ultimamente anche da sistemi opensource, Linux based. Le reti OT, inizialmente isolate dal resto delle reti dati aziendali, sono ora naturalmente predisposte per essere collegate con le reti office aziendali e attraverso Internet, con il mondo esterno.

Si viene così a realizzare quel processo di convergenza tecnologica, conosciuto con il termine "convergenza IT/OT", portatore di notevoli benefici, sia dal punto di vista della flessibilità e dell'ottimizzazione dei costi complessivi di gestione (possibilità di uniformare i contratti con i fornitori di software e di hardware, unificazione di reparti tradizionalmente separati), sia per la possibilità di integrare i dati di produzione con le altre funzioni di corporate e per creare sistemi di Business Intelligence sempre più completi.

2. Punti di attenzione

Se da un lato la progressiva introduzione di soluzioni IT all'interno dei settori della produzione industriale presenta evidenti aspetti positivi, è in ogni caso opportuno analizzare alcune criticità che parallelamente si sono venute a creare, e che spesso non risultano altrettanto evidenti, per poterle adeguatamente gestire senza fermare il benefico processo di integrazione sopra descritto.

2.1. Sicurezza

In primo luogo, occorre evidenziare che l'isolamento in cui originariamente si venivano a trovare i sistemi OT, essenzialmente legato alle loro caratteristiche costruttive, li rendeva intrinsecamente sicuri e protetti.

real local networks. The TCP/IP protocol (Transmission Control Protocol/Internet Protocol, identifies the most used protocol suite within local networks) is no longer exclusive to corporate office networks but has now spread into the world of OT system networks. Even computers used both at server and operator stations, as well as operating systems and databases, have become the same as those used by corporate IT to provide corporate services: back office, administration, purchases, sales.

VMS or UNIX operating systems on which many SCADA systems in the 90's were built, were gradually replaced by Microsoft Windows systems and more recently by opensource, Linux based systems. OT networks, initially isolated from the rest of the corporate data networks, are now naturally predisposed to be connected with corporate office networks and through the Internet, with the outside world.

Thus the process of technological convergence is realised, known by the term "IT/OT convergence", carrier of substantial benefits, both from the point of view of flexibility and optimisation of total management costs (possibility to standardise contracts with software and hardware vendors, unification of traditionally separate departments), and for the possibility to integrate production data with other corporate functions and create more and more complete Business Intelligence systems.

2. Points for Attention

Although the progressive introduction of IT solutions within the industrial production sectors clearly has positive aspects, it is in any case advisable to analyse some criticalities that have come about, and that often are not equally obvious, in order to adequately manage them without stopping the beneficial integration process described above.

2.1. Safety

First, it should be pointed out that the isolation, in which OT systems were originally found, essentially linked to their construction characteristics, made them inherently safe and protected.

Or rather, their reliability and integrity was basically controllable through tested mechanisms: redundant power systems, implementation of physical protection systems such as system segregation, production areas access control systems, etc..

The deployment of Windows based systems and connection of OT networks to office networks and Internet network made OT Systems vulnerable subjecting them to security issues, typical of IT systems [1].

Moreover, some special features of OT systems, first and foremost the need to operate 24/7 with "real time" performance" or "near real time ", make some good safety practices disseminated in the IT world, frequently impractical, or at least difficult to implement, such as the adop-

O meglio, la loro affidabilità e integrità era sostanzialmente controllabile attraverso meccanismi collaudati: sistemi di alimentazione ridondati, messa in atto di sistemi di protezione fisici quali segregazione degli impianti, controllo degli accessi alle aree di produzione, ecc..

La diffusione dei sistemi Windows based e la connessione delle reti OT alle reti office e alla rete Internet ha reso vulnerabili i sistemi OT, sottoponendoli alle problematiche di sicurezza tipiche dei sistemi IT [1].

Peraltro, alcune particolarità dei sistemi OT, prima fra tutte la necessità di operare h24 con prestazioni di tipo "real time" o "near real time", rendono frequentemente inattuabili, o perlomeno di difficile attuazione, alcune buone pratiche di sicurezza diffuse nel mondo IT, come ad esempio l'adozione di tecniche di rilevazione dei tentativi di accesso non autorizzati e di antintrusione (IDS/IPS, Intrusion Detection System/Intrusion Protection System), l'utilizzo esteso di protezioni antivirus e di politiche di aggiornamento software (patch management) [2], [3].

2.2. Livelli di servizio

Le problematiche di continuità operativa di una linea metropolitana, di una rete ferroviaria o di un aeroporto sono differenti da quelle di un sistema IT aziendale. In prima battuta, la differenza fondamentale risiede nel fatto che eventuali discontinuità nel funzionamento dei sistemi OT spesso comportano impatti e/o danni fisici rilevanti, come ad esempio tempi di ripartenza estremamente critici (si pensi ad esempio ad un fermo e alla successiva ripartenza di un impianto di distillazione di una raffineria), danneggiamenti ad apparati o a linee di produzione, anche in questo caso con tempi di ripristino non dipendenti solamente dal tempo di ripristino del corrispondente sistema di controllo, ma fortemente correlati ai danni subiti dagli impianti controllati, danni ambientali e alle persone, in forme più o meno gravi.

Tutto questo perché i sistemi OT sono costituiti da componenti (i dispositivi di campo) che sono direttamente connessi al mondo fisico per rilevarne le condizioni e controllarlo, a differenza dei tradizionali sistemi IT che elaborano ed archiviano dati logici, che per quanto complessi e fondamentali per il corretto funzionamento di un'azienda, causano generalmente inefficienze organizzative e nei casi peggiori perdite economiche e/o di reputazione, ma difficilmente sono la causa di danni fisici.

In aggiunta, le priorità dei settori preposti a garantire il funzionamento dei sistemi IT aziendali e dei sistemi OT sono, per loro natura, differenti [4]:

– l'integrità dei dati e la privacy costituiscono di norma gli obiettivi primari dei settori IT di Corporate, secondo una strategia chiaramente "data oriented";
– l'affidabilità degli impianti, il loro funzionamento esente da guasto, in alcuni casi realizzato con sistemi fail-safe, rappresentano certamente gli obiettivi pri-

tion of techniques for detecting unauthorised access attempts and intrusion detection (IDS/IPS, Intrusion Detection System/Intrusion Protection System), extensive use of antivirus protections and software update policies (patch management) [2], [3].

2.2. Service levels

The problems of operational continuity of a metro line, railway network or airport are different from those of a corporate IT system. In the first instance, the fundamental difference lies in the fact that any discontinuity in the operation of the OT systems often involves significant impacts and/or physical damage, such as extremely critical restart times (think for example of a downtime and the subsequent reboot of a distillation system of a refinery), damage to equipment or production lines, again with recovery times not only depending on the recovery time of the corresponding control system but strongly related to damages suffered by controlled installations, damage to the environment and to people, in more or less severe ways.

All this because OT systems consist of components (field devices) that are directly related to the physical world to detect and control conditions thereof, unlike traditional IT systems that process and store logical data, that no matter how complex and critical to the successful operation of a company, generally cause organisational inefficiencies and at worst economic and/or reputation losses but are hardly ever the cause of injury.

In addition, the priorities of the sectors involved ensuring the functioning of enterprise IT systems and OT systems are, by their nature, different [4]:

– *data integrity and privacy are usually the primary targets of Corporate IT sectors, according to a clearly "data oriented" strategy;*
– *plant reliability, their fault-free operation, in some cases performed with failsafe systems, are certainly the primary objectives of the OT sector according to more process-oriented strategies.*

Even design and organisational arrangements to address the conditions of degradation and failure are often different, as well as the organisation and planning of scheduled maintenance activities. Hence the differences in the relevant operative and maintenance facilities.

In a corporate IT system, if properly managed (through capillary alerts to users and provided early enough), it can be a custom to plan a downtime of systems for maintenance activities also during the hours that such systems should be generally used (office hours).

In an OT system one normally tries to avoid production downtime at times when this must be done by providing for alternative scenarios, with more or less degraded operating conditions, but that allow in any case to keep systems active, or intervening in times when production is already stopped, due to corporate planning.

mari del settore OT, secondo strategie maggiormente orientate al processo.

Anche le modalità progettuali ed organizzative per affrontare le condizioni di degrado e di guasto sono spesso differenti, così come l'organizzazione e la pianificazione delle attività di manutenzione programmata. Da qui le differenze nelle corrispondenti strutture operative e di manutenzione.

In un sistema IT aziendale può essere consuetudine, se opportunamente gestita (mediante avvisi agli utilizzatori, capillari e forniti con sufficiente anticipo), pianificare un fermo dei sistemi per attività di manutenzione anche durante le ore in cui tali sistemi dovrebbero essere generalmente utilizzati (orari ufficio).

In un sistema OT di norma si cerca invece di evitare il fermo della produzione negli orari in cui questa deve essere effettuata, prevedendo scenari alternativi, con condizioni di funzionamento più o meno degradate, ma che consentono in ogni caso di tenere attivi gli impianti, oppure intervenendo in periodi in cui la produzione, per programmazione aziendale, risulta già ferma.

La progressiva integrazione dei due settori, IT e OT, può così indurre ad una unificazione dei livelli di servizio normalmente ad essi associati, assolutamente da evitare in quanto si avrebbe o un impiego non necessario di risorse su servizi o infrastrutture che possono comunque tollerare tempi più o meno significativi di indisponibilità o, nel caso contrario, una riduzione dei livelli di servizio su sistemi o infrastrutture che invece richiedono alti indici di disponibilità e di affidabilità.

2.3. Il ciclo di vita della componentistica di un sistema OT

I sistemi OT sono costituiti oggi da un mix di componenti provenienti in parte dal mondo IT ed in parte dai settori dell'automazione industriale e più in generale dell'elettromeccanica, come ad esempio nel caso di PLC, sensori, attuatori e quadri elettrici.

I cicli di vita della componentistica IT, sia essa hardware che software, sono notoriamente molto veloci. I PC dopo 3 - 5 anni diventano obsoleti, così come anche i sistemi operativi.

Per contro, la componentistica dei PLC ed in generale quella elettromeccanica è caratterizzata da cicli di vita molto più lunghi, spesso dell'ordine delle decine di anni.

Può succedere quindi che, dopo un aggiornamento, il sistema operativo di una workstation non sia più in grado di gestire un driver obsoleto di comunicazione oppure che un nuovo PC, installato in un quadro di automazione di campo, non disponga della corretta tipologia di porta seriale necessaria per connettere un vecchio PLC ancora in esercizio.

I differenti cicli di vita che caratterizzano le varie componenti degli attuali sistemi OT comportano la neces-

The progressive integration of the two IT and OT areas, can lead to a unification of service levels normally associated with them, that must absolutely be avoided as there would either be unnecessary use of resources on services or infrastructures that can more or less tolerate significant times of unavailability or, otherwise, a reduction in the levels of service on systems or infrastructures that require high availability and reliability.

2.3. Life cycle of OT system components

Today OT systems are made of a mix of components coming partly from the IT world and partly from the industrial automation fields and more generally of electro mechanics, such as PLCs, sensors, actuators and electrical panels.

The life cycles of IT components, either hardware or software, are known to be very fast. After 3-5 years PCs, as well as operating systems become obsolete.

On the other hand, PLC and in general electromechanical components are characterised by much longer life cycles, often of the order of tens of years.

It can happen that, after an update, a workstation's operating system is no longer able to manage an out-dated communication driver or that a new PC, installed in a field automation panel, does not have the correct type of serial port required to connect an old PLC still in operation.

The different life cycles that characterise the various components of existing OT systems need to address the issue of updates and system patches[1] with the utmost attention, possibly since the planning phase, or parts of the same.

Again we can see different styles of approach to the problem.

The OT field has always tried to avoid, or at least minimise, system updates, which have always been among the top "best practices" in the IT world and that must in any case be absolutely maintained, albeit with the necessary precautions [5].

The reluctance to updates typical of the OT industry is essentially due to the complexity that often distinguishes validation activities of a new system baseline. For such systems stringent guarantees of non-regression are frequently required; for some of them (failsafe systems) complex validation and certification procedures are required for any update, performed by third parties responsible for attesting the maintenance of original safety requirements, throughout the lifecycle.

---

[1] The term "patch" in computer science is used to indicate the action of updating a programme (software), usually specified by the same producers, imposed by the need to quickly resolve a malfunction or a flaw of security and protection mechanisms, without having to wait for the release of a new (baseline) version of the software in question.

sità di affrontare con la massima attenzione, possibilmente sin dalla fase di progettazione, la questione degli aggiornamenti e delle patch[1] di sistema, o di parti di esso.

Anche in questo caso si possono notare differenti stili di approccio al problema.

Il settore OT ha sempre cercato di evitare, o perlomeno di ridurre al minimo indispensabile, gli aggiornamenti di sistema, che invece sono sempre stati tra le principali "buone pratiche" del mondo IT e che vanno in ogni caso assolutamente mantenuti, seppur con le necessarie precauzioni [5].

La ritrosia agli aggiornamenti tipica del settore OT è essenzialmente dovuta alla complessità che spesso contraddistingue le attività di validazione di una nuova baseline di sistema. Per tali sistemi sono frequentemente richieste stringenti garanzie di non regressione; per alcuni di essi (i sistemi fail-safe) sono obbligatorie per qualsiasi aggiornamento, complesse procedure di validazione e di certificazione, svolte da soggetti terzi preposti ad attestarne il mantenimento dei requisiti di sicurezza originari, per l'intero ciclo di vita.

La complessità viene ulteriormente incrementata se si pensa che i sistemi SCADA e/o DCS sono di norma sistemi verticali e proprietari ed il rapporto che viene frequentemente a stabilirsi fra cliente-utilizzatore del sistema OT ed il corrispondente fornitore è regolato da un contratto che spesso attribuisce al fornitore, una volta realizzato e attivato il sistema, anche i compiti di provvedere integralmente alle attività di manutenzione correttiva e specialistica, lasciando ai reparti interni di manutenzione i compiti di assistenza tecnica di primo livello e di pronto intervento.

Pertanto, oltre alle patch e agli aggiornamenti dei software applicativi originariamente prodotti da un determinato fornitore (o installatore certificato), anche le patch e gli aggiornamenti dei sistemi operativi ed in generale del middleware[2] dell'infrastruttura informatica, parte integrante del sistema OT (come ad esempio i Data Base e le piattaforme di virtualizzazione), devono generalmente essere eseguite a cura del fornitore, pena la decadenza della garanzia e degli obblighi di mantenimento dei livelli di disponibilità contrattualmente concordati [6].

Anche in questo caso è evidente l'approccio completamente differente da quello normalmente in uso nel settore IT di corporate, dove il carattere trasversale dell'infra-

Complexity is further increased if we think that the SCADA and/or DCS systems are usually vertical and proprietary systems and the relationship that is frequently established between client-OT system user and the corresponding supplier is regulated by a contract that once the system is created and activated, often attributes to the vendor even the duties of providing full corrective and specialist maintenance activities, leaving internal maintenance departments the tasks of top-level technical assistance and emergency services.

Therefore, in addition to patches and application software updates originally produced by a particular manufacturer (or certificate installer), even patches and operating systems and middleware in general updates[2] of the IT infrastructure, an integral part of the OT system (such as Data Bases and virtualisation platforms) must generally be performed by the supplier, failure the loss of warranty and maintenance obligations of the contractually agreed levels of availability [6].

Also in this case the completely different approach from the one normally in use in the corporate IT infrastructure is clear, where the transversal nature of the hardware infrastructure and processing, storage and network software means that the same infrastructure is normally completely transparent to applications and IT services provided by these, until reaching the ethereal consistency of cloud computing architectures[3] that characterise the industry trend in recent years.

Table 1 summarises the points of attention previously analysed.

3. ATM case

The Azienda Trasporti Milanesi S.p.A. (ATM) is the company that since 1931 is responsible for Local Public Transport in the metropolitan area of Milan.

Over the years it has extended its activities from surface lines (buses, trolley buses and trams) to the metro lines, with the inauguration of the first section of Line 1 in 1964, to date, with the management of 4 underground lines of the Milan area, including line 5, fully automated, with driverless trains. In the international it field also runs the Metro in Copenhagen.

In addition to local public transport, ATM manages other services related to mobility, including parking on the

[1] Il termine "patch" (rattoppo) in informatica viene utilizzato per indicare l'azione di aggiornamento di un programma (software), di norma specificata dagli stessi produttori, dettata dalla necessità di risolvere rapidamente un malfunzionamento o una falla dei meccanismi di protezione e sicurezza, senza dover attendere il rilascio di una nuova versione (baseline) del software in questione.

[2] Letteralmente "software di mezzo", indica un insieme di programmi specificatamente realizzati per consentire ad altri programmi di comunicare fra loro o di accedere a funzionalità, tipicamente di basso livello, senza conoscerne i dettagli costruttivi; è utilizzato in architetture informatiche complesse.

[2] Literally "middle software," is a set of programmes specifically designed to allow other programmes to communicate with each other or to access functionalities, typically of low level, without knowing the construction details thereof; it is used in complex computer architectures.)

[3] The term "cloud computing" refers to the ability to access computer processing and data storage services using just Internet network connectivity (through subscription of specific subscriptions), without having to have the IT hardware and software infrastructure that provides such services at the company facilities.

TABELLA 1 – *TABLE 1*

Punti di attenzione nella convergenza IT/OT
Points of attention in IT/OT convergence

Convergenza IT/OT - *Convergenza IT/OT*		
Punti di attenzione ***Points for attention***	**Sistemi IT** ***IT systems***	**Sistemi OT** ***OT systems***
Sicurezza ***Safety***	– Best practices consolidate e diffuse – *Consolidated and disseminated best practices*	– Originariamente garantita dalla "segregazione" dei sistemi OT. – *Originally guaranteed by "segregation" of the OT systems.* – L'interconnessione dei sistemi OT con il resto delle reti aziendali e con Internet impone misure di protezione tipiche del mondo IT che vanno in ogni caso preventivamente valutate. – *The OT systems niterconnection with the rest of corporate networks and the Internet requires protection measures typical of the IT world that must in any case be previously evaluated.*
Livelli di servizio ***Service levels***	Orientamento ai dati: *Orientation to data:* – integrità dei dati; – *data integrity;* – privacy; – *privacy;* – accessibilità. – *accessibility.*	Orientamento al processo: *Orientation to the process:* – affidabilità, – *reliability,* – gestione del degrado, – *management of degradation,* – sicurezza intrinseca. – *intrinsic safety.*
Aggiornamenti e cicli di vita ***Updates and life cycles***	– Frequenti aggiornamenti dei sistemi operativi. – *Frequent updates of the operating systems.* – Rapida obsolescenza della componentistica hardware (PC, LAN switch). – *Rapid obsolescence of the hardware components (PC, LAN switches).* – Separazione fra le infrastrutture IT di base e le applicazioni software che le utilizzano (virtualizzazione, cloud computing). – *Separation between the basic IT infrastructures and software applications that use them (virtualisation, cloud computing).*	– Il rilascio di un sistema OT è di norma sottoposto ad un accurato ciclo di verifiche iniziali (nei sistemi fail safe spesso è richiesta la certificazione di enti terzi). – *The release of an OT system is normally subjected to a careful loop of initial tests (often failsafe systems must be certified by third parties).* – La ripetizione di tali verifiche, in occasione dei frequenti aggiornamenti imposti dalla componentistica proveniente dal mondo IT, risulta di difficile attuazione ed estremamente dispendiosa. – *The repetition of these verifications, during frequent updates required by components from the IT world, is difficult to implement and extremely expensive.* – La componentistica proveniente dal settore dell'automazione industriale presenta generalmente cicli di vita più lunghi (di norma superiori a 10 anni). – *Components from the industrial automation sector generally have longer life-cycles (usually over 10 years).* – L'interdipendenza hardware e software è ancora molto presente nei sistemi OT, in particolar modo all'interno delle sue componenti periferiche. – *Hardware and software interdependence is still very present in OT systems, particularly within peripheral components.*

struttura hardware e software di elaborazione, di archiviazione e di rete fa si che la stessa infrastruttura risulti di norma completamente trasparente alle applicazioni e ai servizi IT da questa erogati, fino a raggiungere la consistenza eterea delle architetture di cloud computing[3] che contraddistinguono la tendenza del settore in questi ultimi anni.

La tabella 1 riporta in sintesi i punti di attenzione precedentemente analizzati.

street, parking lots, bike sharing and road pricing ("Area C"), with related payment systems.

It also carries out planning and maintenance activities of the Traffic Control System and Territory on behalf of the municipality, on which the telecommunications networks depend (dedicated mobile radio and broadband optical fibre networks) and systems used by Local police and the municipal offices in charge of controlling the territory, security and video surveillance, centralised traffic light control and mobility information.

This article is limited to the analysis of the systems and technologies used to run subway lines and more specifically to the centralised command and control systems of train circulation, but considerations may be also be extended to other operational areas of the company and more generally to the industrial utilities sector.

[3] Con il termine "cloud computing" si intende la possibilità di accedere a servizi informatici di elaborazione ed archiviazione dati utilizzando semplicemente la connettività alla rete Internet (mediante sottoscrizione di specifici abbonamenti), senza dover disporre nelle proprie sedi dell'infrastruttura informatica hardware e software che eroga detti servizi.

3. Il caso di ATM

L'Azienda Trasporti Milanesi S.p.A. (ATM) è la società che dal 1931 si occupa di Trasporto Pubblico Locale nell'area metropolitana di Milano. Negli anni ha esteso la propria attività dalle linee di superficie (autobus, filobus e tram) alle linee metropolitane, con l'inaugurazione della prima tratta della linea 1 avvenuta nel 1964, fino ad oggi, con la gestione delle 4 linee metropolitane dell'area milanese, inclusa la linea 5, completamente automatizzata, con treni senza conducente (driverless). In campo internazionale gestisce anche la metropolitana di Copenhagen.

Oltre al servizio di trasporto pubblico locale, ATM si occupa della gestione di altri servizi legati alla mobilità, tra cui sosta su strada, parcheggi, bike sharing e road pricing ("Area C"), con i relativi sistemi di pagamento. Svolge inoltre per conto dell'amministrazione comunale attività di progettazione e di manutenzione del Sistema di Controllo del Traffico e del Territorio, a cui fanno capo le reti di telecomunicazione (reti dedicate radio mobili ed in fibra ottica a banda larga) ed i sistemi usati dalla Polizia Locale e dagli Uffici comunali preposti al controllo del territorio, sicurezza e video sorveglianza, regolazione semaforica centralizzata e infomobilità.

In questo articolo si limita l'analisi ai sistemi e alle tecnologie utilizzate per l'esercizio delle linee metropolitane e più specificatamente ai sistemi di comando e controllo centralizzato della circolazione dei treni, ma le considerazioni svolte possono essere estese anche agli altri ambiti operativi dell'azienda e più in generale al settore industriale delle utilities.

3.1. Le tecnologie utilizzate da ATM per l'esercizio delle linee metropolitane

Sin dall'inizio (1964, prima tratta della Linea 1, da Sesto Marelli a Lotto, 11,8 km e 21 stazioni) la gestione della rete metropolitana è stata pensata in modalità centralizzata, attraverso una sala operativa equipaggiata con sistemi di telecomunicazione e di telecomando che hanno continuamente seguito il progressivo sviluppo delle tecnologie: originariamente erano utilizzate linee di telecomando con connessioni dirette in rame, di tipo "punto – punto" o "a direttrice" ("punto – multipunto"), trasmissioni dati a velocità "telegrafiche" e nei casi migliori a 300, 600 e 1.200 bit/s, centrali telefoniche elettromeccaniche, apparati centrali e di campo basati esclusivamente su logiche elettromeccaniche cablate, sistemi audio e video interamente analogici (fig. 1).

Oggi la metropolitana di Milano è composta da 4 linee (Linea 1, Linea 2, Linea 3 e Linea 5), per complessivi 101 km di rete e 113 stazioni. È inoltre in fase di costruzione la Linea 4 (15 km, 21 stazioni), con attuale previsione di completamento dei lavori nel 2022.

Di particolare rilevanza è la densità di traffico gestito sulla rete metropolitana, sia in termini di passeggeri (ol-

3.1. Technologies used by ATM to run underground lines

From the beginning (1964, the first section of Line 1, from Sesto Marelli to Lotto, 11.8 km and 21 stations), the metro network management was designed in a centralised manner through an operational room equipped with communication and remote control systems that have continuously followed the gradual development of technologies: originally remote control lines were used with direct copper "point to point" or "route" type connections, telegraphic speed data transmissions and in the best cases at 300, 600 and 1.200 bits/s, electromechanical telephone exchanges, central and field stations exclusively based on wired electromechanical logic, entirely analogue audio and video systems (fig. 1).

Today the Milan metro consists of 4 lines (Line 1, Line 2, Line 3 and Line 5), for a total network of 101 km and 113 stations. Line 4 is also under construction (15 km, 21 stations), with current forecast for completion of works in 2022.

The traffic density handled on the subway network is particularly significant, both in terms of passengers (more than 1.000.000 passengers a day) and of trains running (more than 1.200 daily departures, with headways that even go down to 90 seconds during peak hours).

To support such management complexity, over time the underground system has adopted increasingly sophisticated technological systems: optical fibre networks and broadband telecommunication systems, distributed along the tunnels and underground stations, digital radio networks for secure wireless and emergency communications, audio and video communications over IP, magnetic electronic ticketing systems with input and output barriers able to read various types of tickets, from paper to proximity ones, until the fully digital ticket (NFC and QR CODE).

The constant evolution of these systems, which as said represent the so-called OT systems for ATM, led to the commissioning, in 2014, of the new control room of the metro

Fig. 1 - Quadri sinottici e banchi di comando della vecchia sala operativa della Linea 2.
Fig. 1 - Interlocking control panels and control desks of the old operations room of Line 2.

tre 1.000.000 di passeggeri al giorno) che di treni circolanti (oltre 1.200 corse al giorno, con cadenzamenti che scendono anche a 90 secondi negli orari di punta).

Per supportare una tale complessità di gestione, la rete metropolitana si è dotata nel tempo di sistemi tecnologici sempre più sofisticati: reti di fibre ottiche e sistemi di telecomunicazioni a banda larga, distribuiti lungo le gallerie e nelle stazioni metropolitane, reti radio digitali per comunicazioni wireless sicure e di emergenza, comunicazioni audio e video su IP, sistemi di bigliettazione magnetico elettronica con barriere di ingresso ed uscita in grado di leggere varie tipologie di biglietti, dal cartaceo a quello di prossimità, sino al biglietto interamente digitale (NFC e QR CODE).

La costante evoluzione di questi sistemi, che per quanto detto rappresentano per ATM i cosiddetti sistemi OT, ha portato alla messa in servizio, nel 2014, della nuova sala operativa della rete metropolitana, completamente informatizzata e basata su un middleware di integrazione che sfrutta le più recenti tecniche IT di virtualizzazione sistemistica ed applicativa (ridondanza sistemistica mediante utilizzo di architetture cluster, virtualizzazione dei server e dei sistemi operativi realizzata tramite prodotti commerciali standard, sistemi storage software defined, ecc.) (fig. 2).

Entrando nello specifico, osservando le architetture dei sistemi di telecomando e di segnalamento utilizzati nelle linee metropolitane 1, 2 e 3, si riconosce immediatamente il fenomeno della convergenza IT/OT descritto nelle pagine precedenti.

In fig. 3 viene riportata l'architettura dei sistemi utilizzati in Linea 2, prima che gli stessi venissero integrati all'interno della piattaforma IT della nuova sala operativa.

In tale contesto, i sistemi di telecomando erano costituiti da apparati di posto centrale e da apparati periferici, interamente realizzati in logica elettromeccanica, connessi in modalità punto - punto da linee dedicate in rame (per ogni località da telecomandare vi era un apparato periferico ed il suo corrispondente di posto centrale).

Tali apparati consentivano il governo della circolazione dei treni in modalità centralizzata, mediante acquisizione dei controlli ed attuazione dei comandi dal banco/quadro sinottico del Dirigente Centrale del Traffico (fig. 1) verso i sistemi di segnalamento periferici (ACEI e sistemi di blocco), a cui venivano demandate tutte le funzioni di sicurezza e protezione. In modo del tutto analogo erano realiz-

Fig. 2 - La nuova sala operativa delle Linee Metro 1, 2 e 3.
Fig. 2 - The new Control Room of Metro lines 1, 2 and 3.

network, fully computerised and based on an integration middleware that uses the most recent system and application virtualisation IT techniques (system redundancy through the use of cluster architectures, virtualisation of servers and operating systems built using standard commercial products, software defined storage systems, etc.) (fig. 2).

In particular, observing the architecture of the remote control and signalling systems used in subway lines 1, 2 and 3, the IT/OT convergence phenomenon described in the previous pages can be immediately recognised.

Fig. 3 shows the architecture of the systems used in Line 2, before they were integrated into the IT platform of the new control room.

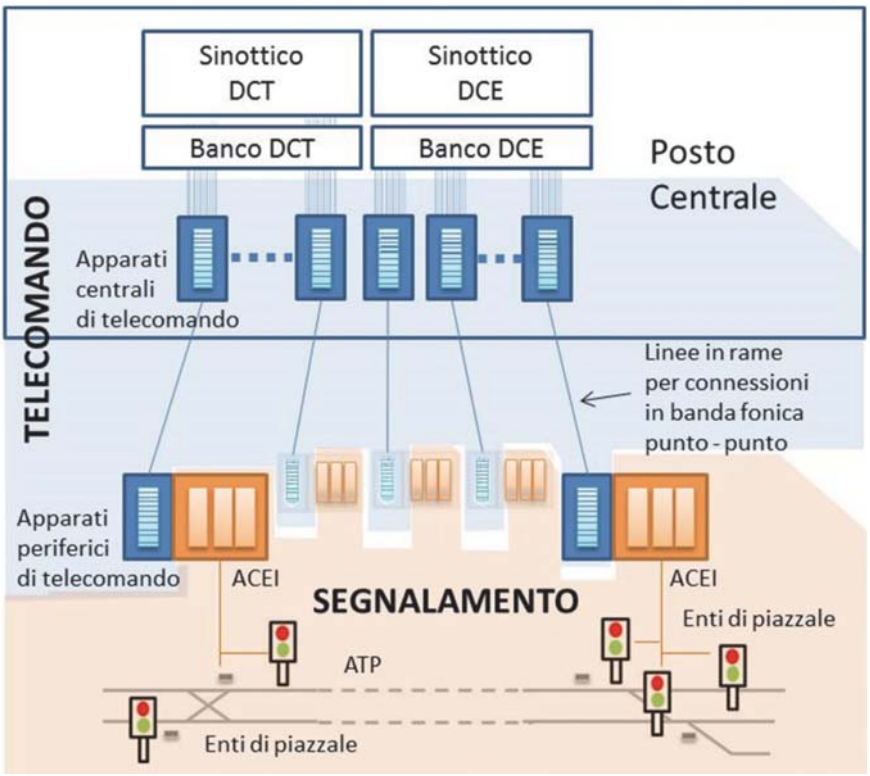

Fig. 3 - Schema di principio dei sistemi tradizionali di telecomando e di segnalamento.
Fig. 3 - Schematic diagram of traditional remote control and signalling systems.

zati gli impianti di telecomando per il Dirigente Centrale Elettrificazione (DCE), competente sugli impianti di alimentazione elettrica (Sottostazioni elettriche e linee di trazione) e sugli impianti tecnologici di stazione (insieme al DCV - Dirigente Centrale Viaggiatori, per gli impianti di illuminazione, scale mobili, ascensori, ecc.).

In una siffatta architettura "verticale, in cui anche l'infrastruttura di rete risulta dedicata alla specifica funzione, l'utilizzo di componenti informatiche è praticamente assente.

La realizzazione della nuova sala operativa, dotata di postazioni a calcolatore (workstation), ha reso necessario integrare i tradizionali apparati di telecomando, basati su interfacce a contatti (digital I/O), con i sistemi di supervisione ATS (Automatic Train Supervision) e SCADA, completamente informatizzati, che implementano nuove interfacce operatore sui monitor delle workstation, e non più sui tradizionali banchi/quadri a mosaico, rispettivamente per le funzioni di comando e controllo centralizzato della circolazione dei treni e di comando e controllo centralizzato degli impianti di alimentazione elettrica e tecnologici di stazione.

Il risultato è quello riportato in fig. 4 dove, relativamente alla Linea 2, si osserva come gli apparati di telecomando di Posto Centrale sono stati sostituiti da un modulo di comunicazione, denominato FEP (Front End Processor), realizzato con componentistica informatica commerciale, che converte i vecchi protocolli proprietari degli apparati di telecomando, transitanti sulle linee punto – punto, in pacchetti dati basati sul protocollo TCP/IP e pertanto trasmissibili sulle comuni reti LAN, con le opportune protezioni in termini di sicurezza informatica.

Le interfacce operatore dei quadri sinottici e dei banchi di comando elettromeccanici sono state sostituite da HMI (Human Machine Interface) dedicate alle postazioni dei singoli operatori di sala, ciascuna composta da 5 monitor da 19" ad alta risoluzione per le visualizzazioni di dettaglio e da 4 monitor da 55" ad alta risoluzione, per le visualizzazioni di insieme, configurate in modalità desktop esteso[4], con una completa integrazione delle funzioni ATS (targatura e localizzazione treni, comando e controllo centralizzato enti di campagna, formazione manuale e automatica degli itinerari/instradamenti, regolazione marcia treni ad orario o a distanziamento, servizi parziali per la gestione di condizioni di degrado/perturbazioni in linea), con quelle di SCADA, Telecomunicazioni, Informazioni al Pubblico e Sicurezza-TVCC.

Un percorso del tutto simile a quello della Linea 2 è stato seguito anche per il processo di integrazione degli

In this context, remote control systems were made up of central station equipment and peripheral devices, made entirely with electromechanical logic, connected in point to point mode by copper dedicated lines (there was a peripheral apparatus and its corresponding central unit for each location to be remote controlled).

This equipment allowed presiding over train circulation in a centralised mode, through the acquisition of controls and the implementation of controls from the desk/interlocking control panel of the Central Traffic Manager (fig. 1) to the peripheral signalling systems (ACEI and locking systems), that were entrusted with all safety and security functions. The remote control systems for the Electrification Central Manager (DCE) were made in a similar way, competent on power supply systems (Electrical substations and traction lines) and on station technological systems (together with the DCV - Travellers Central Manager, for lighting systems, escalators, elevators, etc.).

In such "vertical architecture", in which the network infrastructure is also dedicated to the specific function, the use of IT components is virtually absent.

The implementation of the new control room, equipped with computer workstations, has made it necessary to integrate the traditional remote control devices, based on CI (digital I/O), with fully computerised ATS Supervision (Automatic Train Supervision) and SCADA systems, which implement new operator interfaces on the workstation monitors, rather than on traditional desks/interlocking control panels, respectively, for the control functions and centralised control of train circulation and centralised command and control of electrical power and technological systems.

The result is shown in fig. 4 where, relatively to Line 2, it can be observed how the remote control devices of the central station have been replaced by a communication module, referred to as FEP (Front End Processor), made with commercial computer components, that converts the old proprietary protocols of the remote control devices, transiting on point to point lines, in data packets based on the TCP/IP protocol and therefore communicable on common LAN networks, with the appropriate protection in terms of computer security.

The operator interfaces of the interlocking control panels and electromechanical control desks have been replaced by the HMI (Human Machine Interface) dedicated to the workstations of individual room operators, each consisting of five 19" high resolution monitors for detailed visualisations and four 55" high-resolution monitors, for visualisations of the whole, configured in extended desktop mode[4], with full integration of ATS functions (train labelling and localisa-

[4] Con il termine "desktop esteso", tipicamente utilizzato in ambiente windows, si intende la possibilità di collegare più monitor alla scheda video di un computer per aumentare l'area (desktop) su cui sono visualizzate le icone e le finestre delle varie applicazioni. Il passaggio da un monitor ad un altro avviene in modo del tutto trasparente all'operatore, senza soluzione di continuità.

[4] The term "extended desktop", typically used in the Windows environment, is the ability to connect multiple monitors to the video card of a computer to increase the area (desktop) on which the icons and windows of various applications are displayed. Passing from one monitor to other occurs in a purely transparent way for the operator, without interruption.

impianti di telecomando e di segnalamento della Linea 3 con la piattaforma IT della nuova sala operativa.

Per entrambe le linee, i livelli periferici degli impianti di telecomando, così come gli impianti di segnalamento che implementano le funzioni di Interlocking (ACEI), ATP (Automatic Train Protection) e ATO (Automatic Train Operation), sono stati conservati.

Per quanto riguarda invece la Linea 1, il nuovo sistema di segnalamento CBTC (Communication Based Train Control con sistema di distanziamento a blocco mobile) ha ulteriormente esteso l'uso di componentistica IT su tutte le componenti di automazione e di sicurezza, fino agli impianti periferici.

Dalla fig. 4 si osserva come, in questo caso, il sottosistema ATS e tutti gli impianti di telecomando risultano completamente assorbiti nell'architettura del nuovo sistema di segnalamento, che presenta elementi realizzati in logica fail safe (SIL 4) anche al Posto Centrale, presso il quale è stato reso disponibile uno specifico modulo (VMMI – Vital Man Machine Interface) per l'invio e l'acquisizione di comandi e controlli sicuri.

tion, centralised command and control of rural institutions, both manual and automatic formation of itineraries/routing, adjustable train travel-time or distancing, partial services for the management of degraded conditions/perturbations on the line), with those of SCADA, Telecommunications, Public Information and Security-CCTV.

A path similar to that of Line 2 was also followed for the integration process of remote control installations and signalling of Line 3 with the IT platform of the new control room.

For both lines, peripheral levels of remote control systems, as well as of signalling systems that implement Interlocking functions (ACEI), ATP (Automatic Train Protection) and ATO (Automatic Train Operation), have been preserved.

As for Line 1, the new Communication Based Train Control signalling system (CBTC signalling system with a movable block spacing system) has further extended the use of IT components of all the automation and security components, up to the peripheral installations.

4. Il crescente fabbisogno di competenze informatiche nei settori OT

Osservando i cambiamenti che sono avvenuti nel corso degli ultimi decenni all'interno dei sistemi di gestione centralizzata della circolazione dei treni delle linee metropolitane di Milano, si rileva facilmente la continua e crescente diffusione nel settore dell'automazione industriale delle tecnologie tradizionalmente appartenenti al mondo dell'Information Technology (PC, LAN switch e router, server, storage, sistemi operativi, Data Base), a conferma del fenomeno di convergenza IT/OT precedentemente descritto.

La trasformazione in atto del settore OT, riscontrabile anche nell'offerta attuale del mercato dei componenti e dei sistemi di automazione, controllo e supervisione, comporta di conseguenza una corrispondente trasformazione delle competenze tecniche del personale preposto alla gestione e manutenzione di tali sistemi. È infatti assolutamente indispensabile acquisire presso i reparti OT le conoscenze informatiche necessarie per gestire e manutenere correttamente i nuovi sistemi.

Tutto questo può essere fatto attraverso l'adozione di diversi schemi or-

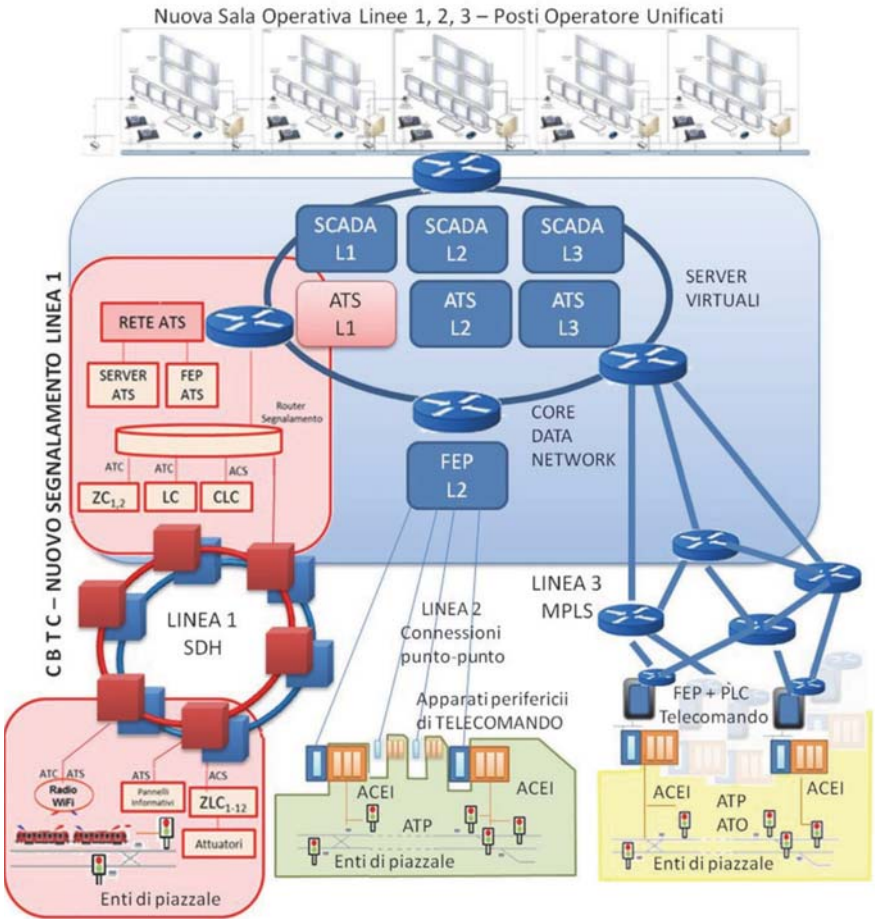

Fig. 4 - Schema generale di integrazione dei sistemi di telecomando e segnalamento.

Fig. 4 - General diagram of integration of remote control and signalling systems.

ganizzativi e di rinnovo degli skill tecnici del personale: si può procedere con l'iniezione di personale informatico nei reparti tradizionalmente preposti alla manutenzione dei sistemi OT, rischiando di creare ridondanze di posizioni organizzative e di competenze tecniche e professionali, oppure, in alternativa, favorire l'interazione dei reparti IT e OT già presenti all'interno dell'azienda, ponendo in tal caso particolare cura nel definire le relazioni funzionali ed i livelli di servizio a ciascuno richiesti.

La convergenza IT/OT non è quindi esclusivamente rappresentabile come un puro processo di trasformazione tecnologica, ma richiede anche una precisa azione di "change management", finalizzata a gestire nel modo corretto l'integrazione di due settori, IT e OT, che storicamente sono sempre stati considerati funzionalmente distinti e che conseguentemente hanno con il tempo acquisito differenti culture aziendali [7].

Questo processo di integrazione non potrà che avvenire gradualmente seguendo il progressivo consolidamento delle infrastrutture IT all'interno dei sistemi OT.

5. La necessità di ridefinire i modelli organizzativi di gestione e di manutenzione

Osservando le modalità di implementazione delle funzioni rese disponibili presso la nuova Sala Operativa della rete metropolitana (SCADA, ATS, Telecomunicazioni, Informazioni al Pubblico e Sicurezza) è interessante notare come la convergenza IT/OT sopra descritta si traduca di fatto in una trasformazione delle modalità di erogazione delle suddette funzioni, di seguito per brevità identificate con il termine "funzioni OT", che vengono a perdere la stretta associazione con gli impianti "verticali" storicamente preposti alla loro erogazione (fig. 3), composti da apparati periferici, trasmissivi e centrali, la cui ownership era indiscutibilmente associata ai reparti che ne curavano interamente la manutenzione, per assumere una connotazione sempre più orientata al servizio, realizzata attraverso una pila di infrastrutture "orizzontali", con una crescente diffusione e complessità di quelle di estrazione tipicamente IT.

Lo schema riportato in fig. 5 illustra in sintesi la tendenza in atto.

Chiaramente il modello indicato rappresenta gli estremi limite in quanto anche nella configurazione impiantistica cosiddetta «tradizionale» (di sinistra) esistevano delle trasversalità, come ad esempio la rete dei cavi di telecomunicazione, che forniva i collegamenti fisici ai vari impianti o, ancora, i sistemi di alimentazione elettrica (cabine di trasformazione, linee e quadri di distribuzione): esse però, da un lato, costituivano un'eccezione e non un caratteristica distintiva, dall'altro dette trasversalità riguardavano tecnologie estremamente consolidate.

Allo stesso modo anche la configurazione a cui si tende (quella di destra) è ancora lontana dalla configurazione attuale.

We can observe from fig. 4 how, in this case, the ATS subsystem and all of the remote control systems are completely absorbed in the architecture of the new signalling system, which presents elements made with failsafe logic (SIL 4) also at the Central Station, at which a specific module was made available (VMMI - Vital Man Machine Interface) for sending and acquiring secure commands and controls.

4. Growing demand for IT skills in OT sectors

Observing the changes that have occurred over the past few decades within the centralised management systems of train movement of metro lines in Milan, continuous and increasing diffusion of technologies traditionally belonging to the world of Information Technology (PC, LAN switches and routers, servers, storage, operating systems, Data Bases) in industrial automation can be observed, confirming the phenomenon of IT/OT convergence described above.

The ongoing transformation of the OT sector, that can also be seen in the current offer of the market for components and automation, control and supervision systems, involves therefore a corresponding transformation of technical skills of the staff responsible for the operation and maintenance of such systems. In fact it is absolutely essential to acquire computer skills at the OT departments necessary to manage and maintain the new systems properly.

All this can be done through the adoption of various organisational schemes and renewal of personnel technical skills: one can proceed with the introduction of IT staff in departments traditionally responsible for the maintenance of OT systems, risking to create redundancies of organisational positions and of technical and professional skills, or, alternatively, favouring the interaction of IT and OT departments already existing within the company by putting in that case special care in defining functional relationships and service levels required by each.

IT/OT convergence is not only representable as a pure technological transformation process, but also requires precise "change management" action that aims to manage properly the integration of two industries, IT and OT, that have historically always been considered functionally distinct and which consequently have acquired different corporate cultures over time [7].

This integration process can only take place gradually by following the progressive consolidation of IT infrastructures within OT systems.

5. Need to redefine management and maintenance organisational models

By observing the implementation methods of functions made available at the new Control Room of the underground network (SCADA, ATS, Telecommunications, Public Information and Security) interestingly, the IT/OT con-

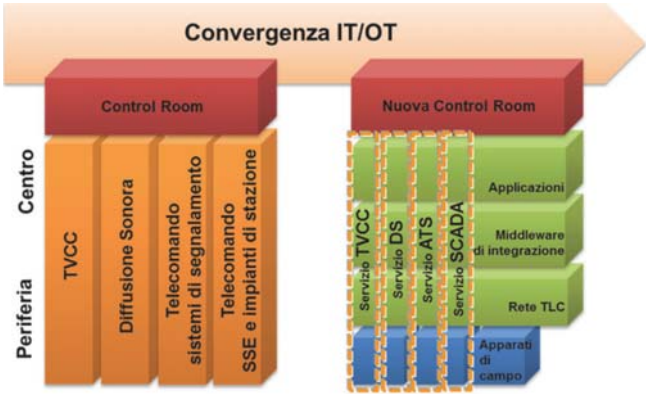

Fig. 5 - Convergenza IT/OT: dagli impianti "verticali" alla pila di infrastrutture "orizzontali".
Fig. 5 - IT/OT convergence: from "vertical" systems to "horizontal" infrastructure stacks.

Oggi, lo stato dell'arte è rappresentato da una situazione intermedia in cui coesistono architetture tradizionali con nuovi sistemi service oriented (fig. 4).

La situazione di transizione sopra descritta genera impatti importanti sulle modalità di gestione delle varie infrastrutture nonché sull'organizzazione e sulle competenze dei corrispondenti reparti di manutenzione, storicamente strutturati, come gli impianti che manutenevano, in modo verticale e che ora, a causa del progressivo consolidamento delle nuove infrastrutture orizzontali, devono adeguarsi ad una maggiore interdipendenza funzionale ed organizzativa, secondo un modello "a matrice".

Si modifica in particolare il rapporto cliente – fornitore che prima vedeva, per il caso specifico dei sistemi OT, una relazione di tipo "uno a molti" fra il Cliente, rappresentato tipicamente dagli Operatori delle Sale Operative, ed i Fornitori, rappresentati dai vari reparti di manutenzione che gestivano, in modo pressoché verticale (dal posto centrale al campo), le varie funzioni necessarie per la gestione operativa dell'esercizio.

Ora questa relazione uno a molti sembra trasformarsi in una relazione di tipo "molti a molti", dove una determinata funzione, ad esempio la visualizzazione in sala operativa delle immagini provenienti dai sistemi TVCC distribuiti lungo le linee metropolitane, può essere implementata solamente attraverso la cooperazione delle molteplici infrastrutture tecnologiche utilizzate (telecamere, data network, server farm, applicazione software specifica e relativa interfaccia operatore) e conseguentemente attraverso le dipendenze fra i reparti tecnici posti a capo di tali infrastrutture.

È chiaro che in un contesto di simile complessità relazionale si dovrà procedere con una precisa definizione delle interdipendenze e dei tempi di intervento richiesti a ciascun reparto coinvolto, sia esso appartenente al settore OT che a quello IT prevedendo, ove necessario, servizi di reperibilità e di pronto intervento h24 anche per reparti storicamente legati ai normali orari ufficio e verifican-

vergence described above will result in a transformation of the delivery mode of the above functions, hereinafter for brevity identified as "OT" functions, that lose the close association with "vertical" systems historically responsible for their delivery (fig. 3), composed of peripheral, transmission and central apparatuses, whose ownership was indisputably associated to departments that were fully responsible for maintenance, to assume a characteristic more and more oriented to service, performed through a stack of "horizontal" infrastructures, with growing diffusion and complexity of those typically of IT extraction.

The diagram shown in fig. 5 summarises the trend.

Clearly the model represents the limit extremes as transversalities were also in the so called "traditional" plant engineering configuration (on the left), such as the telecommunications cables network, which provided physical connections to the various installations or, still, the power supply systems (transformer substations, lines and distribution panels): however, on the one hand, they constituted an exception and not a distinctive feature, on the other hand said transversalities concerned extremely consolidated technologies.

Similarly the configuration also pointed to (the right one) is still far from the current configuration.

Today, the state of art is represented by an intermediate situation in which traditional architectures coexist with new service-oriented systems (fig. 4).

The transition situation described above creates major impacts on the various infrastructure management modes as well as on the organisation and competencies of the corresponding historically structured maintenance departments, such as plants that performed vertical maintenance, and that now, due to the progressive consolidation of new horizontal infrastructures, must adjust to greater functional and organisational interdependence, according to a "matrix" model.

In particular the customer-supplier relationship is modified that first saw, for the specific case of OT systems, a "one to many" type relationship between the Customer, typically represented by the Operators of Control Rooms, and Suppliers, represented by the various maintenance departments that ran the different tasks necessary for the operational management of the business in an almost vertical way (from the central station to the field).

Now this one to many relationship seems to turn into a kind of "many to many" relationship, where a particular function, such as visualisation in the control room of images from the CCTV systems distributed along the metro lines, can be implemented only through the cooperation of multiple technological infrastructures used (cameras, data networks, server farms, specific application software and its operator interface) and consequently by the dependency between the technical departments placed at the head of such infrastructures.

do, attraverso specifici sistemi di gestione, tracciatura e monitoraggio, che l'intero processo manutentivo garantisca, con adeguata continuità, i livelli di servizio originariamente richiesti.

Nel caso di ATM, oltre ad un percorso di riqualificazione del personale dei reparti OT, tutt'ora in corso, finalizzato a fornire gli elementi di base per consentire la corretta operatività sui nuovi impianti, si sta provvedendo a formare una cultura comune fra il settore IT e quello OT: scambio strutturato di esperienze lavorative, condivisione di nuovi progetti, attivazione di gruppi di lavoro interdisciplinari, incontri periodici indirizzati ad analizzare le attività svolte e a consolidare un linguaggio comune.

Si sta inoltre intervenendo a livello organizzativo attraverso la ridefinizione dei livelli di servizio, da garantire non solo fra gli utilizzatori finali (nel caso considerato, la Sala Operativa di Esercizio) ed i reparti tecnici di manutenzione, ma anche all'interno degli stessi reparti tecnici, incluso il settore IT, che progressivamente perderà la connotazione tradizionale di organo di staff per assumere un ruolo preciso all'interno delle linee di produzione aziendale, almeno per gli aspetti strettamente legati alla gestione delle reti di telecomunicazioni e dei sistemi hardware e software mission critical.

Ad esempio, le infrastrutture critiche IT asservite ai sistemi di esercizio già oggi sono monitorate e gestite attraverso la rilevazione periodica dei parametri RAM[5], normalmente utilizzati nell'impiantistica industriale, e sono supportate da un'area dedicata di Ingegneria di Manutenzione, al pari degli altri impianti asserviti alla produzione industriale di ATM (segnalamento, elettrificazione, armamento, materiale rotabile, ecc.).

6. Conclusioni

L'analisi svolta evidenzia il cambiamento tecnologico in corso nell'ambito dei sistemi di automazione industriale, identificati con il termine Operational Technology (OT), per gran parte dovuto all'introduzione di architetture e componentistica proveniente dal settore dell'Information Technology (IT).

Questo fenomeno di "contaminazione informatica" prende il nome di "IT/OT convergence" ed investe come detto, l'intero settore dei sistemi industriale di automazione, supervisione e controllo.

Anche nel settore delle utilities, nel caso specifico il trasporto pubblico locale ed in particolare i sistemi metro-ferroviari di controllo delle linee metropolitane di Milano, risulta evidente questa trasformazione, che non è di

It is clear that in a context with similar relational complexity we will have to proceed with a precise definition of the interdependencies and response times required from each department involved, whether belonging to the OT sector and to the IT one, providing where necessary, on-call and 24 hour emergency services also for departments historically linked to normal business hours and verifying, through specific management systems, tracking and monitoring, that the entire maintenance process guarantees the originally required service levels, with proper continuity.

In the case of ATM, besides providing the basics to enable correct operation of new systems, it is taking steps to form a common culture between the IT and OT sector as well as a retraining course of OT department staff, still ongoing: structured exchange of work experiences, sharing of new projects, activation of interdisciplinary work groups, regular meetings aimed at analysing the activities performed and consolidating a common language.

Work is also being done at organisational level by redefining the service levels, to ensure not only among end users (in the case considered, the Control Room) and technical maintenance departments, but also within the same technical departments, including the IT sector, that will gradually lose the traditional connotation of staff member to take on a precise role within the company production lines, at least for matters strictly related to the management of telecommunications networks and mission-critical hardware and software systems.

For example, IT critical infrastructures subservient to the operating systems today are already monitored and managed through the periodic detection of RAM parameters[5], normally used in industrial plant engineering, and are supported by a dedicated Maintenance Engineering area, like other plants subserving ATM industrial production (signalling, electrification, permanent way, rolling stock, etc.).

6. Conclusions

The analysis highlights the technological change in progress in the field of industrial automation systems, identified with the term Operational Technology (OT), largely due to the introduction of architectures and components coming from the field of Information Technology (IT).

This "IT contamination" phenomenon is called "IT/OT convergence" and as said invests the whole field of industrial automation, supervision and control systems.

Also in the utilities sector, specifically in local public transport and in particular the control of metro-rail sub-

[5] RAM è l'acronimo di Reliability (Affidabilità), Availability (Disponibilità), Maintainability (Manutenibilità). Raggruppa una serie di indicatori statistici, basati sull'osservazione dei guasti e dei tempi di intervento, per fornire informazioni misurabili e confrontabili sulle performance degli impianti e delle attività di manutenzione.

[5] RAM stands for Reliability, Availability, Maintainability. It groups a series of statistic indexes, based upon the observation of failures and technical intervention times, in order to provide measurable and comparable information related to plants performance and maintenance activities.

natura esclusivamente tecnologica, in quanto impatta anche sui modelli organizzativi aziendali e sulle competenze professionali richieste al personale tecnico dei reparti di manutenzione.

In pratica la funzione IT, storicamente intesa negli organigrammi aziendali come una funzione di staff, entra decisamente all'interno degli organi di line.

Ne consegue un cambiamento radicale nella gestione del personale IT, che deve abbandonare il tradizionale ruolo di "consulente" aziendale, spesso auto referente, per diventare ingranaggio di un processo di produzione industriale che di norma costituisce il core business dell'azienda, con relazioni, vincoli, e obiettivi differenti rispetto a quelli tipici del mondo IT di Corporate.

Per contro, anche il personale tecnico dei reparti di manutenzione deve affrontare complessità informatiche sempre maggiori che spesso non trovano riscontro nella formazione e nella cultura aziendale dei reparti OT.

Occorre pertanto avviare, accanto al processo di trasformazione tecnologica, ineluttabile e guidato dal mercato, anche un processo interno di cambiamento organizzativo, che ridefinisca i rapporti fra i due settori IT e OT [8].

way systems in Milan, this transformation, which is not only technological in nature, is clear as it impacts on company organisational models and on the expertise required to the maintenance departments technical staff.

In practice, the IT function, historically understood in organisation charts as a staff function, definitely enters within the organs of line.

The result is a radical change in the management of IT staff, which must abandon the traditional role of corporate "consultant", often self referential, to become a mechanism of a manufacturing process that normally constitutes the core business, with relationships, constraints, and different goals than those typical of the Corporate IT world.

By contrast, maintenance departments technical personnel must deal with increasing computing complexities that often are not reflected in corporate training and culture of OT departments.

Therefore, even an organisational change internal process must be started, besides the technological, inescapable and market driven transformation process that redefines relations between the two IT and OT sectors [8].

BIBLIOGRAFIA - *REFERENCES*

[1] Paul Robertson, Colin Gordon, Simon Loo, *"Implementing Security for Critical Infrastructure Wide-Area Networks"*, 2013, Schweitzer Engineering Laboratories.

[2] Michael Horkan, *"Challenges for IDS/IPS Deployment in Industrial Control Systems"*, 2015, The SANS Institute.

[3] Centre for the Protecion of National Infrastructure, *"Good Practice Guide – Process Control and SCADA Security"*, https://www.cpni.gov.uk.

[4] Heather Mackenzie, *"SCADA Security Basics: Why Industrial Networks are Different than IT Networks"*, 2012, https://www.tofinosecurity.com/blog/scada-security-basics-why-industrial-networks-are-different-it-networks.

[5] U.S. Departement of Homeland Security, *"Recommended Practice for Patch Management of Control Systems"*, https://ics-cert.us-cert.gov.

[6] Keith Stouffer, Joe Falco, Karen Scarfone, *"Guide to Industrial Control Systems (ICS) Security - NIST Special Publication 800-82 Revision 2"*, 2015, Recommendations of the National Institute of Standards and Technology.

[7] Derek R. Harp, Bengt Gregory-Brown, *"IT/OT Convergence - Bridging the Divide"*, http://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf

[8] Andrew Woodward, Craig Valli, *"Which Organisational Model Meets Best Practice Criterion for Critical Infrastructure Providers: An Examination of The Australian Perspective Based on Case Studies"*, 2010, Edith Cowan University.