LA COMPLEMENTARIETÀ TRA SAFETY E SECURITY

Tra sicurezza e disponibilità di una unità produttiva esiste un certo trade-off dovuto al fatto che l'azione di portare l'impianto in uno stato sicuro corrisponde generalmente con lo spegnimento e quindi con un arresto della produzione. I sistemi di sicurezza ben progettati e configurati possono reagire in questo modo anche se ritengono di non poter fare affidamento sulle informazioni in loro possesso come può accadere se diventano oggetto di un attacco informatico

A cura di Massimiliano Veronesi (*)

Da qualche anno ormai non si parla più di "se" ma di "quando": diventa quindi necessario proteggere i sistemi di controllo, con specifica attenzione per quelli deputati alla sicurezza. È opportuno quindi fare un po' di ordine tra le due discipline rifacendosi agli Standard internazionali rispettivamente applicabili.
Un recente rapporto Clusit ha evidenziato come nel 2022 gli attacchi informatici verso bersagli italiani abbiano registrato una crescita

ben superiore a quella mondiale media, con particolare spicco di quelli ad impatto rilevante o addirittura critico. Le intrusioni esterne nelle reti aziendali sono ormai all'ordine del giorno nel contesto di crescenti tensioni internazionali in cui organizzazioni senza scrupoli usano ogni mezzo per trarre vantaggi per sé o causare problemi ad altri. Pur rimanendo i principali bersagli in ambito bancario, amministrativo e sanitario, anche il settore manifatturiero rientra nel mirino degli hackers; chi non riesce più a produrre innovazione tecnologica, a volte è disposto a rubarla. Le infrastrutture industriali hanno quindi da anni iniziato a difendersi per non pregiudicare la produttività e la sicurezza dell'impianto. Sull'altro fronte però la condivisione dei dati relativi all'esercizio è diventato un fattore chiave per la gestione della produzione la cui ottimizzazione è sempre più opportuna per assicurare la necessaria competitività internazionale. Risulta pertanto necessario trovare l'equilibrio più adatto in grado di bilanciare le esigenze di informazioni con quelle di sicurezza. In questo contesto gli IEC-Standard di riferimento per la Safety e la Security costituiscono una solida base sulla quale costruire la robustezza (tecnica e procedurale) necessaria per ridurre il rischio di incidenti, o difendere ciò che è stato fatto qualora si verificassero.

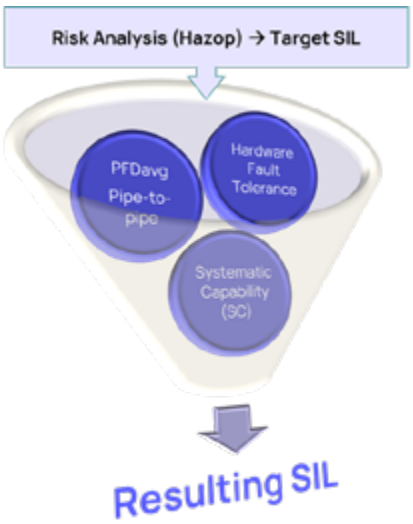
Functional Safety

I sistemi deputati alla messa in sicurezza di una unità produttiva, siano essi meccanici, elettro-meccanici, elettronici o a logica programmabile hanno come unico obiettivo quello di prevenire che una situazione fuori controllo possa determinare un incidente (oppure quello di mitigarne gli effetti, se già avvenuto); poco importa, in questo contesto, l'interruzione della produzione dato che vengono protetti l'ambiente la vita delle persone. Il sistema di sicurezza mette in atto le azioni che portano l'unità produttiva nel cosiddetto "stato sicuro" e lo possono fare anche se non si fidano più delle proprie rilevazioni o del proprio stato di salute: ciò significa che, se il sistema sospetta di essere stato attaccato, mette in atto le contromisure per evitare ogni incidente che si potrebbe verificare durante il suo disservizio, anche se un pericolo reale di processo effettivamente non c'è.
Viceversa, in caso di incidente, tutte le parti in causa, a partire da chi gestisce l'impianto, devono dimostrare di aver fatto tutto quello che era possibile fare per evitarlo. È in questo contesto allora che risultano importanti gli Standard in materia, che rappresentano le migliori pratiche ingegneristiche nei diversi campi. Nell'ambito della sicurezza funzionale, gli Standard attualmente applicabili sono le IEC61508/511. Entrambi sono basati sui seguenti capisaldi:

- Gestione del ciclo di vita della sicurezza
  - Le funzioni di sicurezza vanno gestite dalla fase di identificazione delle situazioni pericolose (analisi dei rischi tramite Hazop) fino al decommissioning dell'impianto, attraverso un ciclo di vita (lifecycle) che deve prevedere progettazione, implementazione, verifiche, gestione delle modifiche, test periodici, audit
- Allocazione e calcolo del fattore di riduzione del rischio
  - Per ogni situazione pericolosa occorre stabilire un fattore di riduzione del rischio che può essere di tipo preventivo (riduzione della probabilità che accada) o di tipo mitigante (riduzione dell'impatto dell'incidente); questa decisione deve esser presa attraverso un approccio metodologico formale come una Risk Matrix o un Risk Graph
  - questo fattore, espresso dal Safety Integrity Level (SIL) può essere raggiunto attraverso l'introduzione di vari livelli di protezione (Layers of Protection) tra i quali accorgimenti meccanici, elettro-meccanici, elettronici o a logica programmabile.
  - La Probabilità media di fallimento on demand (PFDavg) è un parametro di ogni funzione di sicurezza (SIF) e va pertanto calcolata per ogni funzione di sicurezza. Sono stabilite 4 fasce di PFDavg e il SIL è associato alla più elevata PFDavg di ciascuna intervallo
  - Il calcolo deve essere pipe-to-pipe ovvero inclusivo di tutti i dispositivi il cui fallimento può pregiudicare la funzione di sicurezza; tipicamente si va dunque dal sensore di misura (iniziatore) alle interfacce verso il campo, al controllore, ai relè di interfaccia all'organo finale di comando (elemento finale)
- Hardware Fault Tolerance (HFT)
  - La qualità dei dispositivi utilizzati determina quanti ne devono essere impiegati per una medesima funzione di sicurezza; anche il calcolo della PFDavg è diverso in base al voting tra dispositivi (1oo1, 1oo2, 2oo3 tanto per citare i più impiegati).
- Systematic Capability (SC)

• La capacità di una organizzazione di ridurre gli errori sistematici nel corso dei lavori deve essere in qualche modo proporzionale al SIL richiesto, che altrimenti è da ritenersi invalido; questa capacità si esprime attraverso il Functional Safety Management System (FSMS), ovvero l'insieme di procedure, istruzioni di lavoro, checksheets, e tools che l'organizzazione stabilisce vengano impiegati per la realizzazione di un sistema di sicurezza.
• Una SIF di grado SIL-x non può essere realizzata se non da una organizzazione con SC-x. Le più accorte organizzazioni si fanno certificare il proprio FSMS da enti accreditati (es. TUV)

A seguito degli attacchi informatici anche le situazioni di rischio legate a una penetrazione indesiderata devono essere considerate e le vulnerabilità del sistema devono essere per quanto possibile ridotte. Per questo motivo è utile includere nel Hazop-Team anche un esperto di reti e sicurezza informatica.



Functional Safety

Cyber-Security

Quello della sicurezza informatica è un contesto davvero ampio e in continuo divenire. È chiaro come possa essere elevato il costo di perseguire (invano) la completa invulnerabilità come pure quello di non fare nulla esponendosi a lunghe e ripetute indisponibilità dell'unità produttiva; occorre dunque trovare il giusto compromesso tra questi due dispendiosi estremi. Ancora una volta si deve partire da una analisi dei rischi che combini la probabilità di evenienza con la severità dell'impatto in modo da stabilire la criticità di ogni possibile situazione. Ancora una volta poi ci si può lasciare guidare dagli standard internazionali in materia che in questo caso sono ben rappresentati dalla IEC62443. Questo standard prevede:

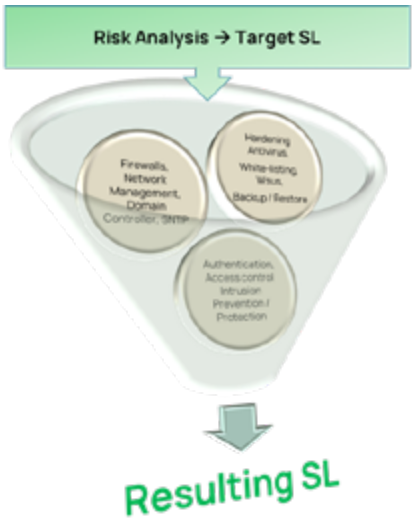
- Una architettura di rete suddivisa in livelli 1, 2, 3, 3.5, 4 (Intelligent Devices, Control Systems, Manufacturing Operations Systems, Demilitarized Zone, Enterprise)
- Un livello di sicurezza (Security Level) che può avere valore SL1, 2 ,3, 4
- 7 Foundational Requirements di natura tecnologica
  - Identificazione e autenticazione
  - Controllo delle funzioni (azioni vs. previlegi)
  - Integrità di sistema (robustezza vs. modifiche non autorizzate)
  - Confidenzialità dei dati (robustezza vs. distribuzione non autorizzata)
  - Restrizioni ai flussi di dati (segregazione in zone e condotti)
  - Tempestività della risposta agli eventi indesiderati
  - Disponibilità delle risorse (a fronte di servizi negati o similare)
- 4 Livelli di Maturità dell'organizzazione, relativi alla robustezza del suo apparato procedurale riguardo alla sicurezza informatica (analoga alla Systematic Capability per la Safety)

Per ciascuno dei Requisiti Fondamentali la completezza e la complessità delle contromisure da implementare dipendono dal grado di sicurezza (SL) desiderato, con particolare frattura tra i primi due livelli SL-1,2 e due più elevati. Ad esempio, solo per i livelli più alti sono indicati accorgimenti come identificazione tramite credenziali hardware (chiavi, riconoscimento impronte oppure oculare, ...), grammatica e scadenza delle password, audit-trail centralizzato, crittografia, backup automatici, segregazione fisica delle reti mediante data-diode.
Proteggere i sistemi di controllo significa proteggere la fonte dei dati di processo e produzione ed è particolarmente sentito da quando si è largamente diffusa l'esigenza di condividerli con le piattaforme gestionali integrandoli attraverso reti aziendali che ormai sono sempre più spesso globali.
La coperta è corta: apertura e comunicazione rendono più vulnerabile il sistema e la sovrapposizione tra IT (dove domina la confidenzialità del dato) e OT (dove conta la disponibilità) va a determinare un'area grigia di

rischio che i sistemi di protezione devono ridurre. Accorgimenti particolari sono opportuni per proteggere i sistemi di sicurezza onde evitare che un attacco possa tradursi in una azione di prevenzione che comporta lo spegnimento (e quindi l'indisponibilità) di una unità produttiva. Tra questi, alcuni possono essere resi disponibili dal fornitore stesso del SIS; ad esempio:

- Hardening severo della stazione di ingegneria
- Download sui controllori di sicurezza abilitato tramite digital input collegato con selettore a chiave
- Accesso tramite password alle impostazioni dei controllori
- Accesso tramite password ai codici sorgente
- Implementazione di un protocollo di comunicazione "sicuro" tra controllori di sicurezza, in modo che la trasmissione di un dato corrotto possa essere individuata e tradursi in una azione di prevenzione (stato sicuro)
- Certificazioni di conformità alla IEC62443-3.3 e IEC62443-4.2, le due sezioni più relative al prodotto inteso come dispositivo, come ad esempio le certificazioni ISA-Secure

Può essere infine di conforto una ulteriore certificazione di conformità (sempre disponibile tra quelle ISA-Secure) alla sezione IEC62443-4.1, la sezione dello Standard che riguarda il processo di progettazione e sviluppo dei prodotti.



Cyber-Security

Conclusioni

La protezione dagli attacchi informatici è diventata un requisito indispensabile nei progetti di sistemi di controllo; tra questi, particolarmente critici risultano i sistemi deputati alle funzioni di sicurezza che, se ben configurati, possono mettere in atto la funzione che porta l'impianto nello stato sicuro, determinandone tipicamente uno spegnimento (shut-down) parziale o completo. Diminuire quindi la vulnerabilità dei sistemi a logica programmabile non serve solo a salvaguardare i dati di produzione ma anche a mantenere alta la disponibilità stessa dell'unità di processo e con essa la continuità produttiva. In questo senso Functional Safety e Cyber-Security si abbracciano in una complementarietà ("available safety") che risulta vitale come un vero e proprio sistema immunitario per l'impianto industriale.

Complementarietà tra safety e security

(*) Massimiliano Veronesi
Product Marketing Manager Process Control and Safety Systems, Yokogawa

Keywords: Safety, Security, Hazop, Risk Matrix, Risk Graph, SIL, PFDavg, SIF, PFDavg, FSMS, TUV, SC, HFT, IEC 62443, ISA Secure. SL

THE COMPLEMENTARITY BETWEEN SAFETY AND SECURITY

A certain trade-off exists between safety and availability of a production unit due to the fact that the action of bringing the plant to a safe state generally corresponds with a shutdown and thus a halt in production. Well-designed and configured security systems can react in this way even if they feel they cannot rely on the information they hold as can happen if they become the target of a cyber attack.

By Massimiliano Veronesi

For a few years now we have not been talking about "if" but about "when": it therefore becomes necessary to protect control systems, with specific attention to those deputed to security. It is therefore appropriate to bring some order between the two disciplines by referring to the respectively applicable International Standards. A recent Clusit report showed that in 2022 cyber attacks against Italian targets grew well above the average global growth rate, with those with significant or even critical impact particularly prominent. External intrusions into corporate networks are now commonplace in the context of growing international tensions in which unscrupulous organizations use any means to benefit themselves or cause problems for others. While banking, administration, and health care remain the main targets, the manufacturing sector also falls into the crosshairs of hackers; those who can no longer produce technological innovation are sometimes willing to steal it. Thus, industrial infrastructures have been defending themselves for years so as not to jeopardize plant productivity and security. On the other front, however, the sharing of operation data has become a key factor in production management, the optimization of which is increasingly appropriate to ensure the necessary international competitiveness. It is therefore necessary to find the most suitable balance that can balance information needs with safety needs. In this context, the IEC-Standards of reference for Safety and Security provide a solid foundation on which to build the robustness (technical and procedural) needed to reduce the risk of accidents, or defend what has been done should they occur.

Functional Safety

The systems deputed to secure a production unit, whether mechanical, electro-mechanical, electronic or programmable logic, have as their sole objective to prevent an out-of-control situation from leading to an accident (or to mitigate its effects, if one has already occurred); it matters little, in this context, the interruption of production since the environment the lives of people are protected. The security system enacts the actions that bring the production unit into the so-called "safe state," and they can do so even if they no longer trust their own detections or health status: this means that, if the system suspects that it has been attacked, it enacts countermeasures to avoid any incident that might occur during its disruption, even if a real process hazard actually does not exist.
Conversely, in the event of an incident, all parties involved, starting with those operating the plant, must show that they did everything possible to avoid it. It is in this context then that Standards in the field, which represent the best engineering practices in different fields, are important. In the area of functional safety, the currently applicable Standards are IEC61508/511. Both are based on the following cornerstones:

- Safety lifecycle management.
  - Safety functions need to be managed from the phase of identification of hazardous situations (risk analysis through Hazop) to the decommissioning of the facility, through a lifecycle that must include design, implementation, verification, change management, periodic testing, audits
- Allocation and calculation of the risk reduction factor.
  - A risk reduction factor must be established for each hazardous situation, which can be preventive (reducing the probability of occurrence) or mitigating (reducing the impact of the incident); this decision must be made through a formal methodological approach such as a Risk Matrix or Risk Graph
  - This factor, expressed by the Safety Integrity Level (SIL) can be achieved through the introduction of various layers of protection (Layers of Protection) including mechanical, electro-mechanical, electronic or programmable logic arrangements.
  - Average Probability of Failure on Demand (PFDavg) is a parameter of each safety

function (SIF) and should therefore be calculated for each safety function. Four ranges of PFDavg are established, and SIL is associated with the highest PFDavg of each range
    - The calculation must be pipe-to-pipe i.e., inclusive of all devices whose failure may impair the safety function; thus typically ranging from the measurement sensor (initiator) to the interfaces to the field, to the controller, to the interface relays to the final control element (end element)
- Hardware Fault Tolerance (HFT).
    - The quality of the devices used determines how many must be used for the same safety function; the calculation of PFDavg also differs depending on the voting between devices (1oo1, 1oo2, 2oo3 just to name the most used).
- Systematic Capability (SC)
    - The ability of an organization to reduce systematic errors in the course of work must be somewhat proportional to the required SIL, which is otherwise to be considered invalid; this capability is expressed through the Functional Safety Management System (FSMS), which is the set of procedures, work instructions, checksheets, and tools that the organization determines are used to implement a safety system.
    - A SIL-x grade FSMS cannot be implemented except by an organization with SC-x. The shrewdest organizations get their SIFS certified by accredited bodies (e.g., TUV).

As a result of cyber attacks, risk situations related to unwanted penetration must also be considered and system vulnerabilities reduced as far as possible. For this reason, it is useful to include a network and cybersecurity expert on the Hazop-Team.

Cyber-Security

That of cyber security is a truly broad and ever-changing context. It is clear how high the cost of pursuing (in vain) complete invulnerability can be as well as the cost of doing nothing by exposing oneself to long and repeated unavailability of the production unit; therefore, the right trade-off between these two costly extremes must be found. Once again one must start with a risk analysis that combines the probability of occurrence with the severity of impact so as to establish the criticality of each possible situation. Once again then one can be guided by the relevant international standards, which in this case are well represented by IEC62443. This standard provides for:

- A network architecture divided into layers 1, 2, 3, 3.5, 4 (Intelligent Devices, Control Systems, Manufacturing Operations Systems, Demilitarized Zone, Enterprise)
- A security layer (Security Level) that can have value SL1, 2 ,3, 4.
- 7 Foundational Requirements of a technological nature.
    - Identification and authentication
    - Control of functions (actions vs. privileges)
    - System integrity (robustness vs. unauthorized changes)
    - Data confidentiality (robustness vs. unauthorized distribution)
    - Restrictions on data flows (segregation into zones and conduits)
    - Timeliness of response to unwanted events
    - Availability of resources (in the face of denied services or similar).
- 4 Levels of Maturity of the organization, relating to the robustness of its procedural apparatus with respect to cybersecurity (analogous to Systematic Capability for Safety)

For each of the Fundamental Requirements, the comprehensiveness and complexity of the countermeasures to be implemented depend on the degree of security (SL) desired, with particular fracture between the first two levels SL-1,2 and two higher ones. For example, only for the highest levels are measures such as identification by hardware credentials (keys, fingerprint or eye recognition, ...), grammar and expiration of passwords, centralized audit-trail, encryption, automatic backups, physical segregation of networks by data-diode are indicated.

Protecting control systems means protecting the source of process and production data and is particularly keenly felt since the need to share them with management platforms by integrating them through enterprise networks that are now increasingly global.

The deck is short: openness and communication make the system more vulnerable, and the overlap between IT (where data confidentiality dominates) and OT (where availability counts) goes to determine a gray area of risk that protection systems must reduce.

Special precautions are appropriate to protect security systems to prevent an attack from

resulting in a shutdown (and thus unavailability) of a production unit. Among these, some may be made available by the SIS vendor itself; for example:

- Severe hardening of the engineering station.
- Downloading to safety-enabled controllers via digital input connected with key switch.
- Password access to controller settings.
- Password access to source codes
- Implementation of a "secure" communication protocol between safety controllers, so that the transmission of a corrupted data can be detected and result in a preventive action (safe state)
- Certifications of compliance with IEC62443-3.3 and IEC62443-4.2, the two sections most related to the product intended as a device, such as ISA-Secure certifications

Finally, an additional certification of compliance (always available from the ISA-Secure certifications) to IEC62443-4.1, the section of the Standard that addresses the product design and development process, may be of comfort.

Conclusions

Protection from cyber attacks has become an indispensable requirement in control system designs; among these, systems deputed to safety functions are particularly critical, which, if well configured, can enact the function that brings the plant into the safe state, typically resulting in its partial or complete shutdown (shut-down). Thus, decreasing the vulnerability of programmable logic systems serves not only to safeguard production data but also to maintain high availability of the process unit itself and with it production continuity. In this sense Functional Safety and Cyber-Security embrace each other in a complementarity ("available safety") that is vital as a true immune system for the industrial plant.

Keywords: Safety, Security, Hazop, Risk Matrix, Risk Graph, SIL, PFDavg, SIF, PFDavg, FSMS, TUV, SC, HFT, IEC 62443, ISA Secure. SL