Cybersecurity as a Process Risk

Identification Methods

S. Palumbo and A. Tomas
Tema S.A.

As the internet is exponentially permeating daily life and work, in parallel, different events of cyberattacks have been recorded. There is a huge challenge nowadays on how to deal with them in the industrial sectors, especially in those with an associated high risk on safety, environment or significant socio-economic impact (i.e. strategic energetic facilities, etc.). This paper has the primary objective to evaluate the methodologies available in the market to face new risks derived from the overlap of Information Technology (IT) and Operation Technology (OT). Secondary objective of the study is to offer a flawless alternative to the existing cybersecurity analytical methods.

KEYWORDS: Industry 4.0, Cyberattack, IoT, Information Technology, Operation Technology, Industrial Control System, Cybersecurity, C-HAZOP, PHA, Cyber Security Process Review

A medida que internet va permeando exponencialmente la vida cotidiana y laboral, paralelamente se han registrado diferentes eventos de ciberataques. Existe un gran desafío hoy en día sobre cómo abordarlos en los sectores industriales, especialmente en aquellos con un alto riesgo asociado en seguridad, medioambiente o impacto socioeconómico significativo (i.e. instalaciones energéticas estratégicas, etc.). Este trabajo tiene como objetivo principal evaluar las metodologías disponibles en el mercado para enfrentar los nuevos riesgos derivados de la superposición de Tecnologías de la Información (TI) y Tecnologías de Operación (OT). El objetivo secundario del estudio es ofrecer una alternativa impecable a los métodos analíticos de ciberseguridad existentes.

PALABRAS CLAVE: Industria 4.0, Ciberataque, IoT, Tecnologías de la Información, Tecnologías de Operación, Sistema de Control Industrial, Ciberseguridad, C-HAZOP, PHA, Revisión de Procesos de Ciberseguridad.

INDUSTRIAL EVOLUTION

In modern history, there are three significant industrial evolution steps that can be easily identified:

1. The passage from human workforce to machinery assembly line.
2. The production improvement obtained by the adoption of computer and automation.
3. The ongoing cybernetical systems integration in the industrial processes.

After the connection between humans and machineries by mean of robots, the attention focused on processes connections and integration to achieve optimized production (data driven analysis) and nowadays the keywords of an Industry 4.0 are Artificial intelligence (AI), cloud services and industrial internet.

CYBER-ATTACKS EXPOSURE

Shifting to a new industrial approach also entails new potential threats to be taken in account. It has been reported by major cyber security providers (i.e. W. Schwab and M. Poujol, "The State of Industrial Cybersecurity 2018", Kaspersky LAB - CXP Group, 2018 [1] and "Symantec Security Response", 2014) [2] that the awareness of possible cyberattacks is growing in the last few years but industries readiness level is alarmingly low.

It´s remarkable the example of the Remote Access Trojan (RAT) called Havex used to spy industrial control systems (ICS), developed by a team called Dragonfy (also known as "Energetic Bear" for their involvement in attacks to different energetic facilities) that was started to be spread in 2010, but it was discovered only in 2013, despite his massive presence on industrial computers. Similarly, the code of the Trojan Karagany, from the same team Dragonfly, leaked and become public in 2010, but it was still involved in the 5% of the attacks of the 2013, until industry business did not adopt proper protections against it.

INFORMATION TECHNOLOGY VS OPERATION TECHNOLOGY

The cyberattacks were considered as the area of intervention of the only Information Technology (IT), that makes use of computers to store, retrieve, transmit, and manipulate data or information. The end to end communication is monitored and protected by IT, to avoid network intrusion, data redirection or stealing of information. The cyberwar is fought by IT departments by means of updated cybersecurity software, resistant firewalls and controlled data transferring across networks and in particular across internet servers.

Operation Technology (OT), that is responsible for the control of the industrial process parameters, adopted a completely different approach to protect their data and it was achieved completely isolating them from external access. In OT, data transmission is realized by cabled modules between Programmable Logic Controllers (PLC), System Collection and Data Acquisition (SCADA) and/or Distributed Control Systems (DCS). The managing of the process data was indeed limited to the business enterprise, with no data exchange with other external networks, neither internet and all input systems respect a specific internal authorization policy.

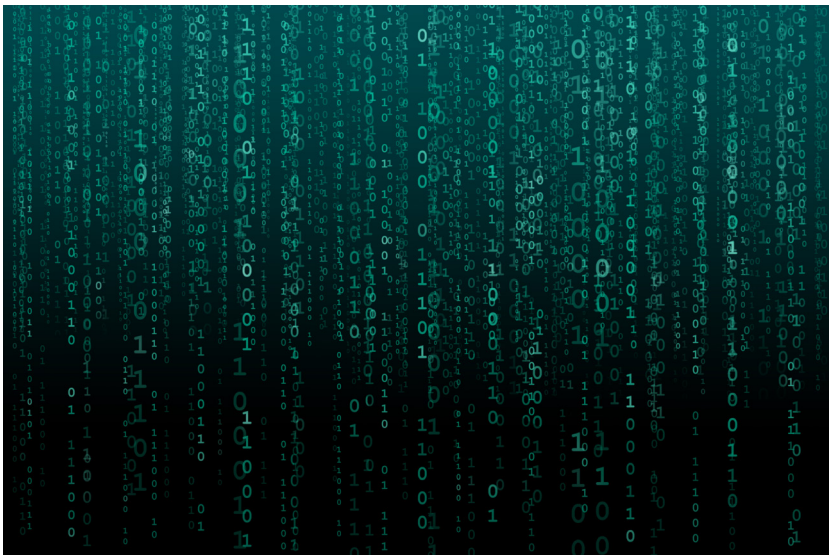
For Information Technology (IT) companies, a cybernetic attack may have an economic impact due to potential data loss or virtual system disabled. On the other hand, Industry 4.0 is realizing that if the Operation Technology (OT) of a production plant is victim of a hackers, direct consequence on the personnel safety and on the environment integrity may occur. Differences between those two approaches can be identified also in the solution they propose (Table 1):

1) For IT the solution is to prevent cyberattacks with means of continuous software updates, patching discovered vulnerabilities, use of multilayers firewalls and upgrades to robust system configuration.

2) For OT the update to a new system implies a potential risk for the continuity of the operation, as well as the integrity of the process, since safety functions would be temporarily disabled. This implies that a software upgrades cannot be done as soon as a vulnerability is discovered, but requires a dedicated planning and risk assessment.

C-HAZOP

Until IT was completely separated by OT, this approach guaranteed a limited impact of cybernetic attacks to a process plant, but now that this limit is blurred and the communication



between smart sensors (i.e. Internet of Things – IoT) and final users are passing through internet, the risk of being victim of a cyberattack to Instrumented Control System (ICS), PLC, SCADA or a DCS, is real.

A large variety of smart sensors, real-time data monitoring solutions, and cloud service data management are offered on the market, but the lack of common standards is creating difficulties to comply with the system safety updates, when a new vulnerability is discovered. In order to mitigate this situation, the norm IEC 62443 was developed, with a dedicated section directed to manufacturers, vendors and cybernetic systems providers, trying to standardize methods, procedures and components.

Additionally, a risk analysis was proposed to evaluate the effects of a potential cybernetic attack on the vulnerabilities created by the interaction between IT and OT, and it is called Control Hazard and Operability Study (C-HAZOP). The approach of C-HAZOP is to identify failure modes of industrial and communication data components and to give a better understanding of the cyberattack vectors, in order to propose recommendation to avoid them.

First step in a C-HAZOPs is to divide in sub-units the overall systems, identifying as per IEC 62443:

- Zones: "a group of logical or physical assets that share common security requirements".
- Conduits: "A logical group of communication assets that protects the security of the channels it contains".

The firsts are the areas responsible of the control, storing and integrity of the data, while the second are responsible for transferring the information between zones. Each of this area is analysed considering possible system vulnerabilities, assigning to them a likelihood of cyberattack, and ranking the highest risks, based on the consequences identified. Next step of this analysis is to take in account existing IT countermeasures, and to assign, for each resulting risk, a Security Level (SL) target, that is defined as "a set of policies, procedures and practices that must be implemented to secure a ICS zone" (IEC 62443) (Figure 1).

Despite the structured approach of the C-HAZOP, this method presents anyway some limitations, hereafter listed:

- The scenarios identified are based on evaluator´s personal experience.

TABLE 1.

COMPARISON BETWEEN IT AND OT

	INFORMATION TECHNOLOGY (IT)	OPERATION TECHNOLOGY (OT)
Objective	Store, retrieve, transmit, and manipulate data or information	Production and process safety
Focus	Computers, networks, data storage systems	Industrial control systems (ICS) to adjust process variables
Performed by	IT, Telecommunication and Networks engineers	Automation & Control engineers, Process and Maintenance engineers.
Priority 1	Confidentiality of the communication network by means of firewalls, user login, access permissions, etc	Availability of the process for continuous production and to ensure safety
Priority 2	Integrity of data stored adopting systems backups or other solutions	Integrity of the plant equipment to achieve the asset value revenue
Priority 3	Availability of data access, using redundant systems, or dynamic network configuration	Confidentiality due to different vendors involved in the plant construction, commissioning and operation
Hardware	Direct updates, easy modules installation, short-term life, remote support service by multiple vendors	Planned updates, full commissioning of upgrades, long-term life, support restricted to trusted vendors
Network and Communication	Internals with externals, over internet	Internals only, cabled network
Cyberattack consequences	Data loss, information stolen, inaccessible networks	Personnel safety, environment integrity, production disruption

- The analysis focus on the failure modes of components (like FMEA) for data management but they are not directly linked to the process plant parameters deviations as in the traditional HAZOP (High/Low Temperature, Over Pressure, High/Low Flow).
- A detailed component-based analysis is time consuming, requires more resources (components data provided by a variety of suppliers) and multi-area specialists.
- Evaluate the frequency of occurrence and the intention of cyber-attacks is aleatory, thus modifying significantly the C-HAZOP risk ranking.
- Once the attack is occurred, the possible safeguards (Alarms, Safety functions, etc, …) can be deactivated and this is not taken in account into a C-HAZOP risk ranking.
- As new vulnerabilities of cybernetic components are periodically discovered, a continuous update of a C-HAZOP is required.

CYBER SECURITY PHA REVIEW

In order to obtain a cybersecurity study focused on the industrial process, Tema S.A. is performing a Cyber Security PHA Review (CSPR), which goes beyond the limit of the high components details and

FIGURE 1. Source: TEMA S.A. , Barcelona, Spain.

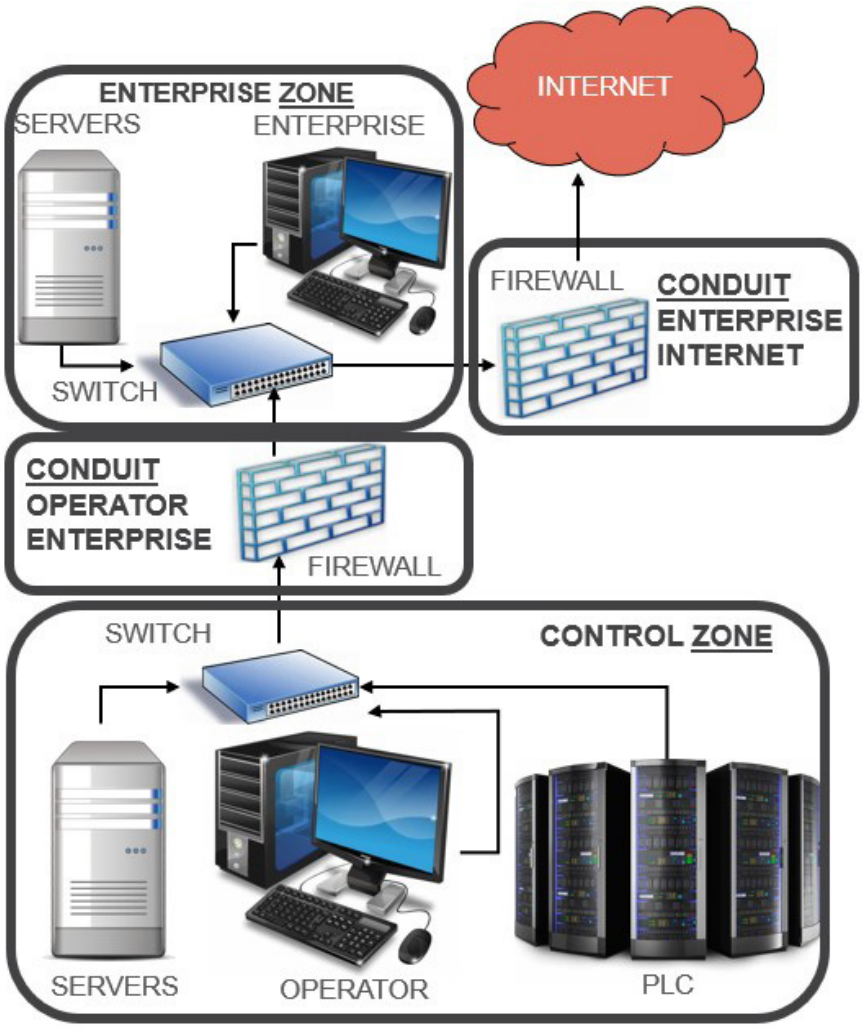


TABLE 2.

COMPARISON BETWEEN C-HAZOP AND CSPR

	C-HAZOP	CSPR
International standard reference	IEC 62443	IEC 62443
Objective	Store, retrieve, transmit, and manipulate data or information	Production and process safety
Focused on	Plant components (like FMEA)	Plant Process Parameters (like HAZOP)
Primay skill required	IT skills	Safety Review skills
Time managemnet	Significant time consuming	Time saving (HAZOP add-on)
Risk Evaluation	Affected by likelihood of being hacked	Consider the case if the attack already occurred
Reccommendations	Associated to full zone or conduit	Specific for plant element
Results updates	Periodically required, when new vulnerabilities are discovered	Independent from vulnerabilities discovered

lack of a unique standard, assuming the hypothesis that an attack has taken place, and evaluating how it affects the process parameters (Table 2).

Tema S.A. has a robust records of HAZOP studies performed worldwide to guarantee personal safety and environmental protection, especially for Chemical industries, Petrochemical plants, Oil and Gas companies, Energy and Mining businesses.

Starting from the results of the traditional HAZOP, the CSPR identifies which scenarios are vulnerable to a cyberattack, and the risk is evaluated through the analysis of the existing safeguards in place. The following step of this analysis is the risk ranking that allows to develop a prioritized actions list assigning the required Security Level (SL) to each scenario as per IEC 62443.

» Starting from the results of the traditional HAZOP, the CSPR identifies which scenarios are vulnerable to a cyberattack, and the risk is evaluated through the analysis of the existing safeguards in place

CONCLUSIONS

The advantages of the CSPR offered by Tema S.A. are:

- A structured evaluation of the cybernetic risks, identifying specific areas exposed to target attacks or to conventional malwares.
- Time and resources consumption are minimized, since there is no need to start from scratches, but the method can be implemented as an HAZOP add-on.
- Analysis results are independent from the cyberattack likelihood to occur or the hacker capability, so they don't need a periodical evaluation update.
- It provides detailed and specific recommendations for each vulnerable element of the plant analysed.
- Allows to realize proposals for intrinsically safe systems against cyberattacks.
- Comply with international standards IEC 62443.

Results obtained by CSPR performed by Tema S.A. are a valuable cost-efficiency input to manage the OT/IT cybersecurity threads and to define the cybernetic investment plan to shift companies into the Industry 4.0.

References

[1] W. Schwab and M. Poujol, "The State of Industrial Cybersecurity 2018", Kaspersky LAB - CXP Group, 2018. https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2018.

[2] Symantec Security Response, 2014. "Dragonfly: Cyberespionage Attacks Against Energy Suppliers", Symantec Corporation. Https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat-energetic-bear.