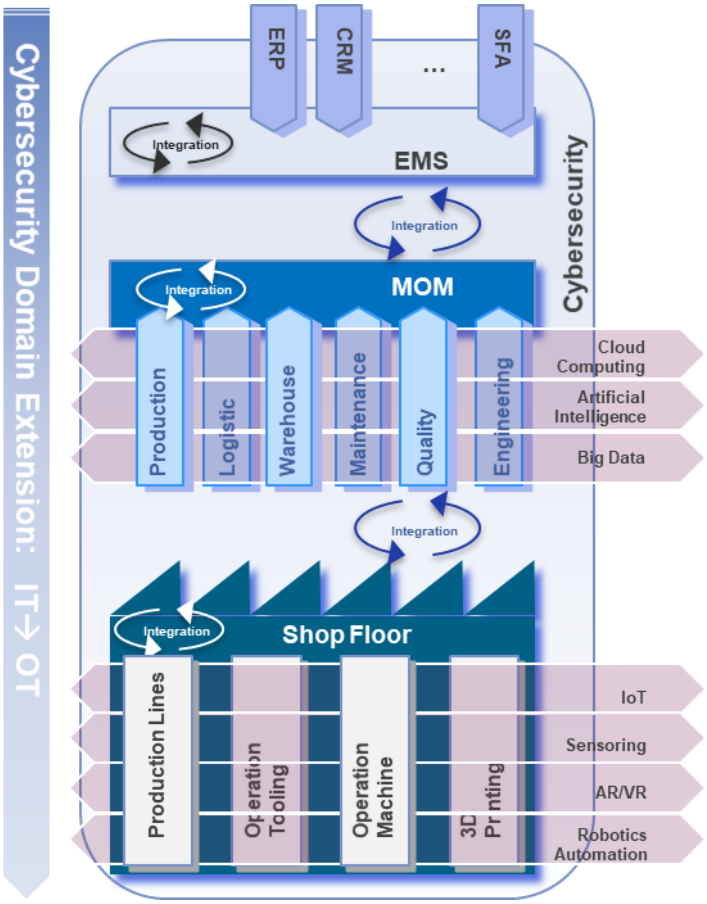
Addressing the Emerging Challenges of OT Security in the Era of Industry 4.0

The evolution of manufacturing according to the so-called 'Industry 4.0' model has led to a profound transformation in the management of industrial processes, thanks to the convergence between Information Technology (IT) and Operational Technology (OT) and the adoption of new technologies such as Cloud Computing, IoT, 5G, Artificial Intelligence, Digital Twin, etc.
The 'fourth industrial revolution' represents a great opportunity for development and growth for companies in the sector, and it is an ongoing process as new technologies are constantly being developed and implemented, promoting further integration and synergy at multiple levels between Enterprise Management Systems (EMS), Manufacturing Operations Management (MOM), and the Shop Floor.



On the other hand, this change requires a 'dynamism' that is not so common in the OT context, and has highlighted the need to implement cybersecurity also in this domain, which has traditionally been considered less exposed to cyber risks.

The challenge of IT/OT convergence

The abandonment of the complete segregation ("air-gap") model between IT and OT has introduced new challenges in terms of cybersecurity. While the IT domain is traditionally well-secured, the OT domain has specificities that require particular attention. The lack of effective governance, the weakness in the partitioning of responsibilities, and the

insufficient training of production personnel on cybersecurity issues are just some of the challenges faced in OT.

In the context of Industry 4.0, the convergence between IT and OT has become an unavoidable reality. This convergence has brought significant advantages in terms of operational efficiency and process optimization, but it has also exposed OT systems to new and more sophisticated cyber threats. The lack of a clear separation between the two domains increases the risk of unauthorized access and targeted attacks, but it can also allow the simple propagation of malware from one environment to another (consider, for example, the 2021 cyber crisis at Colonial Pipeline, where the accidental spread of ransomware from the IT area to the OT area led to the partial shutdown of one of the largest pipelines in North America, with significant consequences not only on the company's business but even on the global cost of crude oil).

The challenge is further exacerbated by recent geopolitical situations that have highlighted the crucial importance of cybersecurity in strategic sectors such as energy and industrial production and those related to primary services (water distribution, logistics, transportation, etc.): all these sectors increasingly use cyber-physical systems that fall within the OT or x-IoT domain (with the "x" potentially taking on various meanings).

All this makes an integrated approach to cybersecurity indispensable.

Implications of cybersecurity under the new EU machinery regulation

The new EU Machinery Regulation (2023/1230) - published on June 29, 2023, in the Official Journal of the European Union and coming into force on January 20, 2027 - requires manufacturers to also consider risks posed by cyberattacks: this is a new requirement and a significant advancement compared to the current EU Machinery Directive 2006/42/EC.

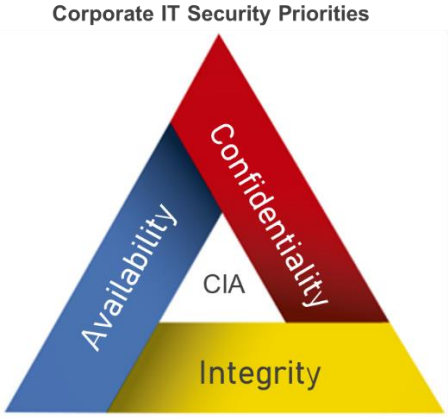
Specifically, paragraphs 1.1.9 and 1.2.1 set forth safety requirements aimed at ensuring that device interconnections do not cause hazards, that hardware components and critical software are adequately protected from unauthorized alterations, and that they are capable of collecting evidence of interventions. It is also required to identify and make easily accessible information on software essential for safe operation and monitor any changes to configurations. Furthermore, control systems must be designed to protect themselves from attacks, and it is necessary to track versions of safety software to demonstrate compliance to competent authorities for at least five years.

The Legislator's focus on this issue indicates a growing awareness, at all levels, of the potential cyber risk in this sector.

OT specific challenges

Cybersecurity in the OT domain has different requirements and constraints compared to the IT domain: this translates into an approach and solutions (both in technical/architectural terms and in terms of processes and governance) that have specific characteristics.

In the IT domain, the priority is given to the C-I-A triad (Confidentiality, Integrity, Availability), whereas for the OT domain, the focus is more on the S-R-P triad (Safety, Reliability, Productivity).



The lifecycle of OT systems is significantly longer than that of IT systems, and in the industrial sector, software obsolescence can be less effectively countered: it happens often to face operating systems that are well past their end of support, making security patches unavailable (which, by the way, the OT professionals are already reluctant to apply when a simple reboot - which translates into production downtime – is needed…).

To further complicate the situation, the OT context must consider the numerous special-purpose systems and proprietary protocols designed to maximize efficiency (or meet real-time constraints), often sacrificing some security aspects that would normally be considered fundamental in the IT domain.

Traditionally, the issue of cybersecurity in the design of production plants has always been inherently subordinated to aspects of safety and operational continuity, relegating it to marginal attention (and budget): often the best practice of “Security-by-Design” has been disregarded, which recommends providing adequate security measures from the initial stages of design (and you know very well that remedying later with ad hoc countermeasures will be less effective and more expensive…).

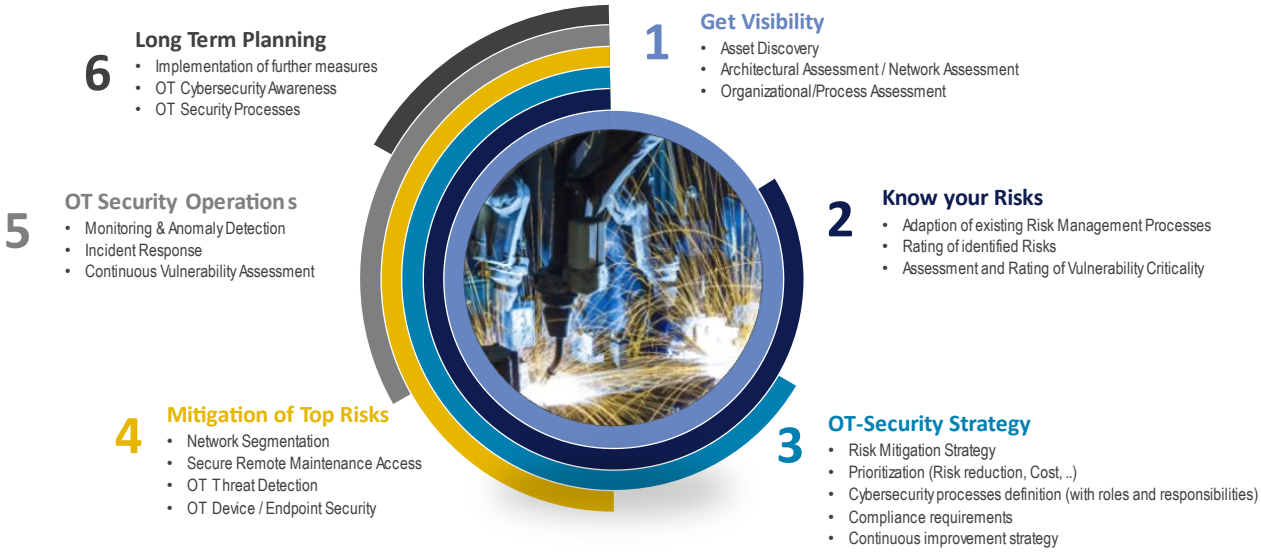
The combination of a network architecture not designed according to security best practices with the presence of legacy systems and insecure protocols represents a typical vulnerability in the OT environment.

The lack of robust governance and defined processes in the OT field can lead to inadequate or ambiguous partitioning of responsibilities between IT and OT departments, making it difficult to manage integrated cybersecurity.

The poor preparation of production personnel on cybersecurity issues can ultimately increase the risk associated with cyber threats, given the growing interconnection between OT devices and corporate networks.

A structured approach and progressive path to improve OT security

To address these challenges, companies in the sector should follow a gradual and structured path that allows them to improve their security posture without compromising productivity.
Aware of the specificities of companies in the various industrial sectors and of the fact that an OT Cybersecurity program must necessarily be tailored to the needs, priorities and spending capacity of each reality, at NTT DATA we have designed an incremental model to support our customers who intend to extend Cybersecurity control to their OT area and improve their overall security posture.



This path includes several phases, described below.

1. **Gaining Awareness of Corporate OT Assets and Internal Security Processes.** It is essential for companies to have full visibility of what their OT assets are and how they are interconnected with each other and with the rest of the IT infrastructure; this can be achieved through asset discovery activities (typically passive, and therefore non-invasive) for the creation and dynamic updating of a detailed asset inventory (possibly coordinated with the company CMDB).
   From a technical point of view, it is also important to carry out an assessment on architectural and network aspects.
   An organizational assessment is also useful to verify the correct attribution of roles and responsibilities in the cybersecurity field (RACI matrix), as well as the presence of adequate security processes and procedures.
2. **Cyber Risk Assessment.** An in-depth assessment of cyber risk (performed in an objective and context-aware manner) is essential to identify potential threats

that could compromise the security of OT systems. This process should include analyzing vulnerabilities, evaluating the potential impact of attacks, and determining appropriate mitigation measures.

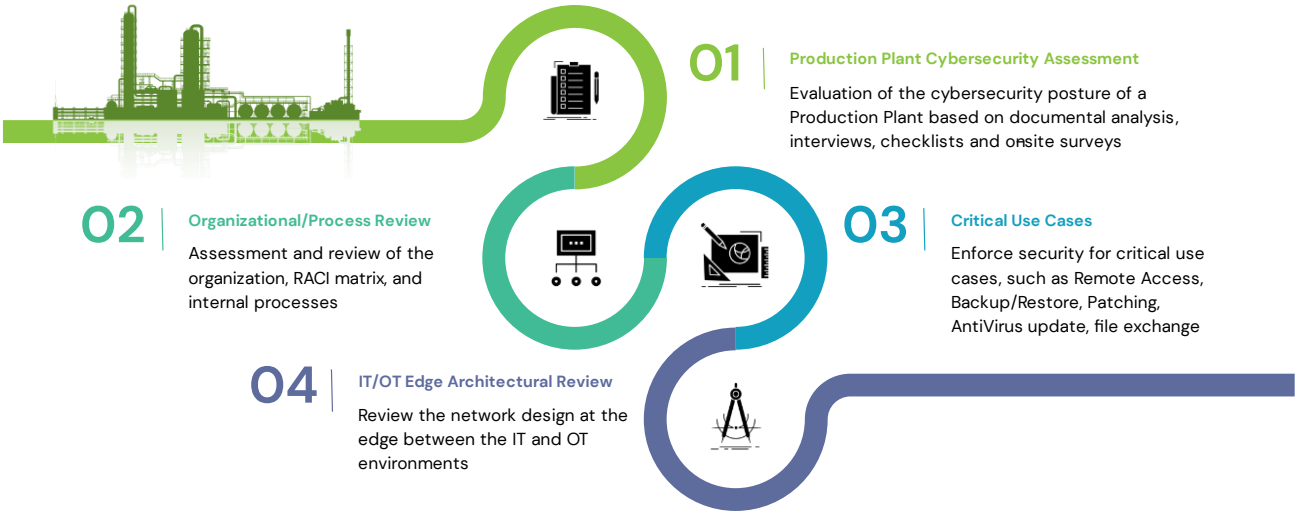
3. **Definition of an OT Security Strategic Plan.** Based on the results of the risk assessment, companies should develop a comprehensive strategic plan to improve the security of their OT systems. Interventions should be prioritized with a risk-based approach, but which also takes into account compliance with regulations (NIS/NIS2 Directive, National Cyber Security Perimeter, New Machinery Regulation...) and industry standards (ISA/IEC 62443, NIST SP 800-82,…) and of course also considering the associated costs. This plan should include clear objectives, specific actions and guidelines for managing risks and protecting systems.
4. **Mitigation of Major Risks.** Once the strategic plan is defined, companies should focus on implementing measures to mitigate the identified risks.
   A solid starting point is to use the Purdue Model as a reference, which is always useful for clearly defining security levels and outlining risk mitigation strategies for the different levels of control and management of information and processes. Technical countermeasures might include the implementation of network segmentation (with the creation, first and foremost, of an industrial DMZ at the border between IT and OT networks), the application of improved access controls (for example using Multi-Factor Authentication for remote access), updating security policies and implementing advanced incident detection and response technologies.
5. **OT Security Operations.** It is important that companies implement processes and procedures for continuous monitoring of the security of OT systems, as well as for the effective management of security incidents. This could include the implementation of passive network traffic monitoring systems (Intrusion Detection Systems), the analysis of anomalous behavior and the implementation of incident response workflows, under the aegis of a Security Operations Center (SOC) with qualified staff with OT Security know-how.
6. **Long-term planning for "*continuous improvement*".** Finally, companies should develop a long-term strategy for continuously improving the security of their OT systems. This may include periodically reviewing security policies and procedures, participating in cybersecurity training and awareness programs, and implementing innovative technologies and solutions to address emerging threats.

Steps to improving safety in a production (quick-wins)

For companies that do not have the possibility to immediately start a structured OT Cybersecurity program, but feel the need to gain a certain awareness of this path and of the gap to be filled, at least on a specific production plant, at NTT DATA we have defined a simplified path, which consists of:

- a technical/organizational assessment to be carried out at least "on paper" (conducted through document analysis, interviews with stakeholders, questionnaires and checklists),

- the analysis of some typical and particularly critical use cases (user management, remote maintenance, backup/restore, file transfer between IT and OT…),
- the architectural analysis of the border between the IT and OT networks.



Conclusions

OT Security has become an extremely important area in the Industry 4.0 era. Effectively addressing emerging challenges requires significant commitment from companies in the sector, but investing in the security of industrial plants is essential to ensure operational continuity and protect assets and people from increasingly sophisticated cyber threats.

Filippo Capocasale

Graduated with honours in Computer Engineering at UniCal, Filippo Capocasale has spent his whole career, spanning over more than 20 years, in the Cybersecurity sector.

He managed projects of Architectural Design, Implementation and System Integration for major Clients in Italy and other Countries. He spent over a year in Tokyo, working in Automotive Cybersecurity R&D. Currently he leads the «Cyber-Physical Security & Innovation» Practice in the Security BSL in NTT DATA Italia: his responsibility encompasses OT/IoT/IIoT Security, Automotive Cybersecurity and Innovation in the Cybersecurity domain.