Cybersecurity challenges and regulation opportunities for OT systems in Energy sector

Introduction

The latest EU Cybersecurity Strategy, including the revision of important directives such as the Directive on Security of Network and Information Systems (NIS 2 Directive)[1] and the Critical Entities Resilience (CER) Directive[2], focusses on European infrastructure and industry resilience and emphasizes the importance of having robust processes for risk management and business continuity.

These European initiatives are complemented by sectorial regulations, such as the upcoming Cybersecurity Network Code[3] and with the increasing and planned portfolio of certification schemes being developed by ENISA in the context of the EU Cybersecurity Act. This activity shows great potential and positive contribution to improve the security of system and products and contributes to the objective of greater resilience across the energy sector.

T&D Europe recognizes the importance of such initiatives and, with its members, has been actively working and contributing on electrical infrastructure resilience and cybersecurity for many years. T&D Europe members, working alongside grid operators and regulators, are regular contributors in various European initiatives aimed at finding effective solutions to cyber security problems. In this regard, T&D Europe and its members have been continuously highlighting the importance of paying special attention to the **Operational Technology[4] (OT) systems security** of the **installed base** and associated digital equipment that are supporting today's electrical grid.

These digital components play important roles in grid protection and control and comprise equipment such as protection relays, controllers, communication equipment, RTUs, man machine interfaces, mobile apps and other accessories necessary for the system's specific mission. Currently these components are integrated in physically dispersed OT Systems located in utilities' service perimeter areas.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN
[3] Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows
[4] See: https://www.ncsc.gov.uk/guidance/operational-technologies

With regard to the system's mission, it is relevant to point out that these assets can be of critical importance for grid stability which, due to the strategic function of power transmission and its role in cross border energy exchange, means that vulnerabilities can have an amplified consequence at grid level.

Current industrial practices

High reliability and uptime are the key principles of OT systems. All security measures and maintenance practices are designed around those principles to ensure cyber security posture and maintain risk at acceptable levels.

Evolving attack techniques, new vulnerabilities, and an evolving threat landscape due to digitization are forcing grid participants to regularly update and adjust security measures on live production systems to keep them protected from known vulnerabilities and threats.

The challenge to grid participants is ensuring secure operation of the electrical assets during their entire operational lifetime where this is much longer than anticipated in enterprise IT systems lifetimes. The system supporting the electrical process needs to evolve regularly to match business needs and security operational requirements.

One practice of asset owners is to perform regular risk assessments of their system's security perimeter, these assessments can be triggered either by a time-based policy or by a vulnerability disclosure event. With such studies in hand, adequate cybersecurity measures can be taken to mitigate any identified vulnerability and risk in order to maintain the cyber security posture. Examples of such mitigations could be patching affected equipment or the inclusion of compensating security countermeasures at system level.

High availability systems in operation are always a challenge for secure operations. Grid operators must carefully plan their security maintenance activities and balance out the risk in their systems. **It's often the case that security patches in OT systems are not deployed due to process complexity or operational difficulties,** such as impact on system operation, predictability of response, quantity of impacted systems, the need for requalification of products or service downtime.

This life cycle challenge in OT systems demands a higher level of engagement between operators and product / system suppliers, not only for coordination and development of effective cyber measures but also for operational expenditure in systems cyber security maintenance. From an OT system perspective some of these challenges could be:

- System vulnerabilities identification and disclosure cooperation
- Temporary corrective measures, if necessary
- Product patches and deployment strategies
- Defense in depths strategy assessment
- Digital equipment end-of-life management

System suppliers are expected to collaborate with grid operators providing elements of those technical measures where products/systems are not end-of-life and are covered by warranty and maintenance agreements.

T&D Europe highlights the importance of having formal contractual relationships, particularly between system providers and grid operators and promoting a close collaboration on OT systems security. Such collaboration can provide grid operators with access to technology expertise, secure deployment experience and in depths OT process knowledge that supports OT systems and underlying products to be managed in regards of security.

With this context in mind what is currently observed by T&D Europe members is:

- OT systems components are not being patched regularly, thereby degrading the established defense in depths strategy and overall system resilience.
- OT installed based is often outdated, relying mainly on perimeter security countermeasures
- An over reliance on product assurance schemes will not cover system security lifecycle issues and defense-in-depth completely
- A lack of incentives for grid operators to establish cyber security maintenance service agreements in new and existing solutions.

A way forward

T&D Europe members believe that a number of steps are needed to provide a robust way forward:

- T&D Europe members consider that the implementation of **an asset identification and classification system** for the OT systems, **as proposed by ACER cyber security network codes,** will help define the priority, engagement type and reaction time needed from the security operations team and associated partners.

- T&D Europe members highlight that it is a frequent request in commercial specifications that products or systems have regular cybersecurity patches provided for known vulnerabilities. However, this contractual request does not answer the system security challenges over its expected lifespan and a more comprehensive service level agreements should be encouraged to provide adequate services.

- A **security service level agreement** with system providers can help increase operational security and prevent defense in depths strategies being degraded e.g. by non-patched products inside the system or by degrading hardening.

  It's relevant to note that products are not used independently in systems, they actively participate in the overall security strategy and are fully integrated in distributed system level functions. Interventions are challenging and need assessment and relevant expertise in the OT domain prior to any modification that might have an impact on the security level.

  In this context a cybersecurity service agreement can help reduce intervention risk and cost while minimizing downtime and total intervention time. Examples of what could be expected are:

  - OT System specific risk exposure analysis and impact
  - OT system specific risk contingency and temporary mitigation plan
  - Patch qualification and interoperability verification within a specific system context
  - OT system specific Intervention plan
  - Scheduled maintenance plan over the affected perimeter

    - Patching procedure and sequencing
    - Re-validation and specific testing

- In those cases where some products are reaching the end of their operational market life, the support of the solution provider becomes even more important since additional guidance could be provided, such as:

    - Identification of vulnerabilities for deployed systems
    - Migration of a system, e.g., by deploying compatible in-production products
    - New product qualification, integration system testing and deployment

T&D Europe members contend that the current European cybersecurity measures do **not provide a balanced answer to OT systems lifecycle security** and should include mechanisms to support service level agreements in the cyber security service relation between system providers and asset owners that matches the importance and value of this service.

Conclusion and recommendations

The grid code for cybersecurity aspects of cross-border electricity flow guideline published by ACER in July 2021[5] contains important requirements that can help to address the issues highlighted here for new and installed OT systems.

It is imperative that the new cybersecurity grid code promotes ways to achieve a sustainable **lifecycle cybersecurity support for OT systems with regular patches and update services**, and these should not be limited only to critical assets for cross-border flows, but to the majority of important assets providing essential energy services to society.

5 https://documents.acer.europa.eu/Official_documents/Acts_of_the_Agency/Framework_Guidelines/Framework%20Guidelines/Framework%20Guideline%20on%20Sector-Specific%20Rules%20for%20Cybersecurity%20Aspects%20of%20Cross-Border%20Electricity%20Flows_210722.pdf

T&D Europe members recommend that during the writing process of the Grid codes ENTSO-E and EU DSO include in the guidelines such topics and consider the entity level risk assessment and supply chain security as important enablers for solving the challenges highlighted by this paper.

T&D Europe also reminds other stakeholders that an open dialogue with the T&D industry is especially important for assessing the technological choices for OT system risk mitigation and supply chain security success.

ABOUT T&D EUROPE

T&D Europe is the European Association of the Electricity Transmission & Distribution Equipment and Services Industry, which members are the European National Associations representing the interests of the electricity transmission and distribution equipment manufacturing and derived solutions. The companies represented by T&D Europe account for a production worth over € 25 billion EUR, and employ over 200,000 people in Europe. Further information on T&D Europe can be found here: http://www.tdeurope.org

CONTACTS

Diederik Peereboom
Secretary General, T&D Europe
Diederik.Peereboom@tdeurope.eu
+32 2 206 6888

Laure Dulière
Policy Adviser
Laure.Duliere@tdeurope.eu
+32 2 206 86863