T&D europe
The European Association of the Electricity Transmission and Distribution Equipment and Services Industry

Reinventing electricity
Reaching Energy Union Goals through Grid Interconnection and Digitisation
29 November 2016
Martin's EU Hotel, Boulevard Charlemagne 80, Brussels

Harmonized Cyber Security standards for the European Union Electric Grid
Position Paper

Brussels, 29 November 2016

Executive Summary

As the T&D industry becomes increasingly integrated to form an even more interconnected, smarter grid, our critical infrastructure faces new and known cyber threats and attacks that could impact the reliability, stability and security of the electric grid, ultimately leading to outages and the loss of this necessity for our daily lives.

T&D vendors are playing an important role in helping TSOs/DSOs and regulators to develop security frameworks with the latest security measures. This can only be accomplished through harmonization, standardization and certification that eliminates the patchwork of geographically based requirements and leaves a strong, continental approach to securing the grid that supports the European Commission's Digital Single Market strategy of a public private partnership (cPPP) on cyber security. T&D vendors are applying cyber security concepts, beyond only network security, that are specially adapted to the OT systems that manage Europe's critical infrastructure.

As a conclusion, this paper provides the position of T&D Europe on standardization, certification and harmonisation in the context of cyber security and takes the following positions:

1. Increase T&D Europe's engagement in cyber security related regulatory activities

2. Promote the use of international standards

3. Promote cyber security certification to be system oriented and focussed on processes

4. Promote the harmonization of cyber security requirements across European member states

Introduction

Electricity is an essential service that plays an important but often unseen role that is typically taken for granted. It powers not only the multitude of gadgets we rely on daily, but also provides the foundation for our businesses and our economy. More interconnected and smarter with active consumers and distributed generation, our critical infrastructure faces new and known cyber threats and attacks that could impact the reliability, stability and security of the electric grid, ultimately leading to outages and the loss of this necessity for our daily lives.

This paper discusses the important role that T&D vendors play in helping regulatory authorities by defining a minimum set of requirements in order to protect critical infrastructure with a focus on operational technology (OT) cyber security. Privacy is seen as a relevant topic as well for personal protection, but is not in the scope of this position paper and is already well covered by the European Commission's General Data Protection Regulation (GDPR). T&D Europe supports harmonization efforts and is promoting its participation in European regulation activities to ensure that requirements are harmonized with industry initiatives and standards. Further, this paper outlines the relevance of industry standards and presents T&D Europe's view on certification.

Today, as purveyors of the underlying operational technology systems that manage the electric grid, vendors are best positioned with the cyber security expertise to protect and maintain the resilience and integrity of the electric grid. Based on this expertise, T&D Europe is best positioned to play a key role in regulatory activities within the European Union.

Cyber Security in the Utility Context

Of all of the utilities, electricity has arguably become the most critical to our lives. Electricity is everywhere, and with more dependence on computer technology, the stable supply of electricity is even more essential. Below are some examples of the impact on society of a sustained, widespread blackout:

- Environment: No heating, cooling, running water or light.
- Finance: No stock or trading markets, no commerce.
- Industry: No business operations, lost revenue.
- Health: Limited emergency health care services.
- Transport: Loss of supply chain and food distribution, difficulty refuelling vehicles, no movement of people.
- Digital infrastructure: No communications services for telephones or computers. No television or radio. No Internet.
- Infrastructure: No water and wastewater, no defence services.

The high dependency on electricity in our modern lives means that power outages are either undesirable or unacceptable, and in most countries result in commercial penalties against the electricity network operators for customer minutes lost and frequency of interruptions. As a result there is currently a drive towards adding instrumentation to detect failures, and control and automation to reconfigure the network to minimize the extent of any outage.

Cyber security is on the top of the agenda across most industries, and for all levels of government. There have been several well documented incidents that cover almost every aspect of life, from hacking into automotive systems[1] and financial organizations, theft of personal data from companies[2] and government departments[3], to the wilful interruption of industrial processes[4] and public services[5].

For example, for electric utilities, the impact of disrupting any single grid node on the network is mostly restricted to the customers connected via that node. This could affect one customer or millions depending on where the node is located in the supply network. The more strategically important a substation, the more physical security and redundant supply paths are used to maintain operations. However, the potential impact of gaining access to the data network that connects substations to the control centres is vast.

In Europe, the number of potential points for monitoring and control, the substations and control points that are the nodes in the network, exceeds 4-million substations[6] in the electricity network alone. Each monitoring and control point is a potentially open door for a cyber attacker.

Substations vary in size and complexity from small installations on wooden poles in fields, to large compounds with high steel fences. The difference between the security of utility substations and a typical enterprise IT system is that many of these nodes are in isolated rural or suburban locations with little or no physical security.

In the case of utility industries, and particularly in the energy sector, there are key aspects that make cyber security even more important:

- The number of potential points of attack
- Geographically distributed nature of grid nodes
- The criticality of the grid node
- The scale of impact

As demonstrated by an incident in Ukraine[7], where a cyber attack left 225,000 utility customers of three distribution utilities without electricity for up to four hours, it is possible for attackers to infiltrate a system months or years before, gain knowledge of the system and then attack. Compromised systems lay undetected until triggered by a signal or external event. In this case, even power backup systems were compromised so that when power was cut to the control centre, the backup supply did not turn on.

In the USA, the Federal Bureau of Investigation has uncovered evidence of a foreign hacker known as UglyGorilla[8], who had infiltrated the systems of a utility in the northeastern United States responsible for managing liquid natural gas pipelines. During his repeated sorties into the company's systems he copied confidential information such as pipeline schematics and had access to systems that are used to regulate the flow of natural gas. More and more of these types of events are being detected, where hostile actors look to collect information that could be used to disrupt the delivery of essential services.

This makes compromise detection a top priority for utility network operators.

Operational Technology (OT) Cyber Security

The world of traditional Information Technology (IT) has morphed greatly over the years into non-traditional areas, such as supporting electricity management and control systems. As technology advances, so too must the capabilities, roles, and responsibilities of IT professionals. Companies' heavy dependency on IT and the evolution of skill sets required to support operational systems has outpaced the current skill capabilities and range of IT professionals. This evolution has given rise to the need of cyber security within Operational Technology (OT). The OT role focuses on the process controls required to manage the operations side of the business. The differences between OT and IT can be confusing for those on either side when it comes to the specific roles each competency plays, but both types of security are necessary to ensure the protection of our critical infrastructure.

The main principles behind a cyber-secure system can be defined using the CIA triad. CIA stands for confidentiality, integrity and availability.

Confidentiality: Protect data from unauthorized access or disclosure.

Integrity: Protect the consistency of information ensuring the actual data is correct.

Availability: Ensure that the data and systems are available and that downtime is avoided or minimized.

In the IT world, the priority for these concepts is typically CIA, while in the OT world the priority is normally inversed as AIC. For example, take the case of a financial company. In the event of a cyber incident, it may be a normal practice to place their system offline to protect the confidentiality of their customers' data, whereas an electric utility would almost never consider taking their protection and control system offline. Doing so could potentially cause unsafe conditions for their personnel or leave a section of the grid in an outage condition.

High reliability and uptime is one of the key principles of an OT system. All security measures and maintenance practices are designed around maintaining this. Secondly, performance and reaction time are also very important. In the electrical grid, the time required to react needs to be in the range of tens of milliseconds. Lastly, OT systems use control methodologies and specialized protocols such as IEC 61850, which require specific domain expertise to both configure and secure. Some other key differences between IT and OT are shown in this table:

	Information Technology (IT)	**Operational Technology (OT)**
Purpose	Transaction Systems; business systems, information systems, IT security standards,	Control Systems; control or monitor physical processes or equipment, OT security standards, OT

Architecture	Enterprise wide infrastructure and applications	Geographically distributed, event-driven, real-time,
Interfaces	Personal Computers, Mobile devices	SCADA, protection relays, RTUs, HMIs, switchgear
Ownership	CIO, finance and administration departments, IT managers	COO, electrical engineers, technicians, operators, and
Connectivity	Corporate network, Internet, IP-based	Control networks, hard-wired twisted pair, fibre optic, powerline communications, and IP
Responsibility	Keeps the enterprise running and protects company assets	Keeps the lights on, protects operational assets and ensures safety

With our years of experience in the OT domain, T&D vendors are highly positioned to help apply cyber security concepts from the IT world and specially adapt them to the OT systems that are managing Europe's critical infrastructure.

Harmonization

In today's energy grid, assets differ not only in their purpose and function, but also in the different component lifetimes seen in deployed infrastructures. In the electric grid, next to primary assets such as transformers and switchgear, is the automation level containing protection and control functions. Devices deployed in different periods of time do typically not support the same level of cyber security functionality. The requirements of cyber security functionality are evolving over time and best determined by the international standards relevant for the energy sector. Operators of critical infrastructure derive security requirements by a risk-based approach, where infrastructure has been assessed in order to derive an appropriate protection level. Several security controls are typically applied in a protection approach in order to mitigate risks. The key questions answered are related to confidentiality, integrity and availability (CIA) protection goals. While some controls can be translated directly into functional cyber security requirements, others are translated into people- and process-related security requirements. Protection goals and related security requirements are relevant for operators as well service providers, integrators, and vendors. The requirement for harmonization follows the cyber security need to protect critical infrastructure.

Electric grids are interconnected within Europe and are considered as critical infrastructure with high potential impact on society. An electricity blackout has a direct impact on other critical infrastructure such as transport, telecommunication, health, and finance. Additionally, a blackout might cascade across borders. Therefore, the protection of the energy supply is one of the key topics for regulatory and legal authorities of the EU and its member states. The major steps toward regulation of cyber security across Europe are initiated by the European Commission with the General Data Protection Regulation (GDPR)[9] and Network

Information Security (NIS) Directive[10]. This is a harmonized approach across Europe. While the GDPR addresses privacy protection in particular, the NIS directive addresses the need for reporting and sharing of information related to incidents.

For operators of critical infrastructure, harmonization can be described as the need to provide a consistent level of cyber security functionality in order to meet protection goals. One key target is the support of interoperability in a multi-vendor environment without jeopardizing protection goals. Suppliers, integrators, and service providers of components of critical infrastructure are at the heart of the effort to support harmonization and implementation of cyber security by making contributions toward international standardization and by providing components for critical infrastructures that follow such standards. International standards are hereby forming the common language of cyber security used by all actors in the energy value chain.

Furthermore, regulatory authorities within the European Union are discussing the possibility to define a minimum set of security requirements in order to guarantee a minimum level of protection for critical infrastructure. In this context, T&D Europe supports harmonization efforts and is promoting its participation in European regulation activities to ensure that requirements are harmonized with industry initiatives and standards.

The harmonization of security requirements would directly benefit the economy by lowering implementation costs while supporting the European Commission's Digital Single Market strategy with products and systems deployable in all member states. Additionally, a minimum level of protection could be defined equally for all critical infrastructures within the European Union. Furthermore, building on international standards as a common language in cyber security with harmonized security requirements is improving interoperability and mitigating the risk of 'home-made' security requirements seen in the market.

Standards and Certification

T&D vendors have historically been involved in defining standards and industrial communications protocols at European and international levels, as well as industrial processes (for example, the protection functions inside a substation). They have a deep understanding of the underlying choices and historical evolution of these protocols and processes.

They also know the details of substation operations and the utility-specific needs of safety, availability, and performance.

This explains why T&D vendors are involved (together with utilities) in defining the cyber security standards for the electrical grid. The OT cyber security standard landscape is shown in the figure below:

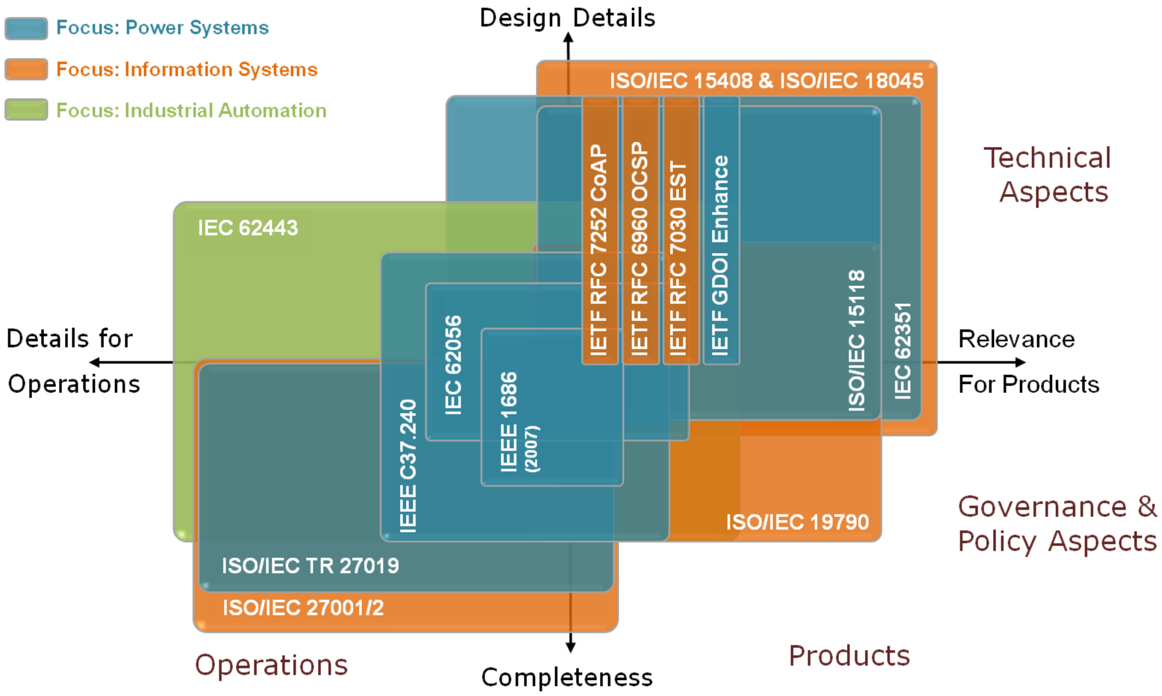

Figure: Cyber Security Landscape
(Source: SG-CG/M490/H_ Smart Grid Information Security; Smart Grid Coordination Group Document for the M/490 Mandate Smart Grid Information Security, Dec. 2015)

The key basic standards shown in this figure are ISO/IEC 270xx, IEC 62443, and IEC 62351. These cover security management, systems security and communication security aspects for the T&D industry.

Taken into consideration the maturity and depth of expertise invested in these standards, it is recommended that these standards are referred to in European cyber security policy and mandates.

Technical Certification

In an attempt to control product security implementation, one could be tempted to ask for an independent product certification.

However, in a very dynamic threat landscape, product (i.e., protection relays) certification certainly has its challenges, will not achieve much, and may foster a false sense of security.

The systems used for operational technology are by definition systems, integrating components, but a collection of secure components does not make a secure system. Components must be properly configured within the system, security features must be interoperable between vendors, and security measures must be implemented in the context of the entire system.

Component technical certification usually involves:

- Defining a set of requirements (usually as an international standard, as interoperability is required)
- Defining a set of evaluation criteria
- Defining the certification process
- Upgrading the component to meet evaluation criteria
- Passing certification

The whole process could take years and, as the cyber security landscape changes much more rapidly, would only result in an obsolete component by the time the certification has been achieved.

Supposing that the component technical certification is relevant at release time, then the product lifetime must also be considered. Contrary to traditional IT, where hardware is amortized quickly (3 to 5 years) and replaced often, substation hardware is installed for a minimum of 15 to 25 years. It is not possible to ensure that a certification will still be relevant over such a long period of time.

Another challenge to certification is the potential variety of requirements to fulfil in the absence of a common certification program across member states. Some member states are engaged in the definition of protection profiles and security targets in order to certify OT devices. Such certification, different for every country, would represent a significant burden for the market as an obstacle to penetrate new markets, as investment in compliance would first be directed toward historical markets.
Given the constraints above, a certification framework should:

- Be system oriented (design and lifecycle of the system)
- Be common to all member states
- Rely on functional requirements rather than short-lived technical requirements. For example, encryption shall be a functional requirement but the technical implementation of this will evolve over time and should not be a part of a regulation or standard.
- Support flexible use cases based on context
- Be based on international standards
- Consider the expected long lifetime of components
- Avoid certification barriers while preserving a transparent and fair certification scheme for processes
- Allow self-declaration of security for systems and components designed under a certified process

European authorities should promote the cooperation and harmonization of national regulatory activities to promote a common cyber security certification framework.

Certification should be focused on processes and not components, such as ISO/IEC 27001 which focuses on the management of security, while IEC 62443-2-4 focuses on the process of a system integrator.

Conclusion

The electricity grid is one of the most critical infrastructures for Europe and is increasingly a target for cyber-attacks. T&D Europe has the expertise in the T&D and cyber security domains and is diligently working to protect this infrastructure. As such, the position of T&D Europe is to:

1. Increase T&D Europe's engagement in cyber security related regulatory activities

2. Promote the use of international standards

3. Promote cyber security certification to be system oriented and focussed on processes

4. Promote the harmonization of cyber security requirements across European member states

T&D Europe is ready to act as a cooperative and constructive partner to the European commission and its stakeholders in discussing and promoting a cyber-secured electric grid.

References

[1] Andy Greenberg. (2016, March) Wired Magazine. [Online]. https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/

[2] Suzanne Philion. (2016, Septmeber) Business Wire. [Online]. http://www.businesswire.com/news/home/20160922006198/en/

[3] Ellen Nakashima. (2015, July) Washington Post. [Online]. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

[4] ENISA. (2010, October) [Online]. https://www.enisa.europa.eu/news/enisa-news/stuxnet-analysis

[5] Alan Martin. (2015, February) We Live Security. [Online]. http://www.welivesecurity.com/2015/02/24/british-hacker-due-sentencing-public-service-ddos-attacks/

[6] Pavla Mandatova. (2013) Eurelectric. [Online]. http://www.eurelectric.org/media/113155/dso_report-web_final-2013-030-0764-01-e.pdf

[7] Robert Lee. (2016, March) SANS. [Online]. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[8] Michael Riley. (2014, June) Bloomberg. [Online]. http://www.bloomberg.com/news/articles/2014-06-13/uglygorilla-hack-of-u-s-utility-exposes-cyberwar-threat

[9] European Parliament. (2016, April) Official Journal of the European Union. [Online]. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[10] European Parliment. (2016, July) Official Journal of the European Union. [Online]. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

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