cigre | PARIS 2022

SIEMENS
TI Safe
Chesf

Study Committee D2

Information Systems and Telecommunication

Paper 10185_2022

A PRACTICAL APPROACH IN CYBERSECURITY MEASURES FOR BRAZILIAN UTILITIES

Paulo ANTUNES*, Armando TEMPORAL, Marcelo BRANQUINHO

Siemens, CHESF, TI Safe

Motivation

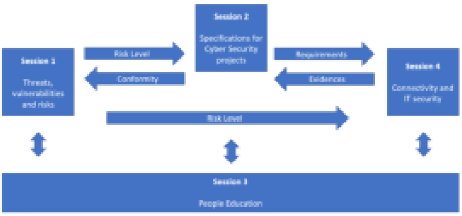
- Cyber security gained a lot of relevancies worldwide, primarily due to the spread of remote working and services because of Covid-19 social distancing. Specifically, in Brazil, according to TI Safe ICS-SOC, **Cyber incidents with Electrical Utilities has grown 860% in 2020**
- Knowing the reality of Brazilian electrical grid and the profile of professionals acting on the engineering maintenance, and operation, **Cigre WG presents what would be the most appropriated** path to be followed by these companies for a more secure digital operation

Method/Approach

- **Cigré Brasil maintained a Working Group on Cyber Security**, which was already in operation before the pandemic started spreading in our country. While everything was happening and seeing this new scenario of high increase in cyber incidents, the group was forced to collaborate with the electricity sector and built, over the last 2 years, 4 technical brochures on the topic: Cyber Security, a practical approach for the Brazilian electricity sector.

Objects of investigation

- The sessions are divided as subjects per below:


Session 1
Threats, vulnerabilities and risks
Risk Level
Conformity
Session 2
Specifications for Cyber Security projects
Requirements
Evidences
Session 4
Connectivity and IT security
Risk Level
Session 3
People Education

Experimental setup & test results

- With the participation of **professionals from the most diverse areas of activity, such energy utilities, consultants, suppliers and universities, documents were prepared with the purpose of supporting companies in the electricity sector** in their transformation towards an operation with proper management of cyber risks, bringing a holistic view that addressed technology, processes, and people. This represents the fundamental triad of any cybersecurity solution.

Discussion

- The importance of Risk Analyses previously to a Cyber Security project
- How to specify a Cyber Security RFP?
- Strategies for People Education
- Trade-off between Connectivity and OT Security

Conclusion

- This paper brings together 4 essentials pillars to build safer OT environments in the utilities market in Brazil. It highlights the importance of having cybersecurity in the agenda of the managing board, controlling cyber security risks as the companies does to all other risks that could affect the business continuity. The board must support resources and sponsor for cyber securities initiatives, including people, processes and technology needed to address the subject.
- Besides this engagement of managing board, there is a need to conduct Cyber Security Risks Analysis previously to any project deployment. It is basically impossible to protect an OT environment without having a clear view on the assets and risks associated.
- Furthermore, it is demonstrated the importance of having the right strategy for training and personal education, across the complete company hierarchy, and known roles and responsibilities related to the cyber security subject. Finally, there are example of solutions that could be implemented by Brazilian utilities.

Study Committee D2

Information Systems and Telecommunication

Paper 10185_2022

A PRACTICAL APPROACH IN CYBERSECURITY MEASURES FOR BRAZILIAN UTILITIES

continued

Subject 1: Threats, Vulnerabilities and Risks

- Risk analysis in OT (Operation Technology) environments is the sum of the results of static and dynamic analyses. The main cybersecurity frameworks used in analysis of this profile are: NIST, NERC-CIP, ISA/IEC 62443 and ISO 27001. Despite the evolution of the systems, Automation Technology (AT) has not incorporated known security controls from Information Technology (IT). In this context, risk management and, particularly, risk assessment, becomes increasingly necessary to reduce possible damage and losses, while contributing to plant efficiency indicators

Table 1 - Common vulnerabilities of industrial control systems for energy

SYSTEM	POTENTIAL VULNERABILITIES
Communication networks	– Inadequate physical security / Errors and failure of settings management / Inadequate door security /Use of vulnerable ICS protocols / Unnecessary firewall rules / Lack of intrusion detection capability
Configuration	– Inadequate account management / Bad password policies / Lack of update management / non-effective application of antivirus and *Whitelisting*
Platforms	– Lack of *hardening* in the system / Unsafe embedded applications / Application of untested third-party solutions / Lack of update management / *Zero-Day Vulnerabilities*
ICS Applications	– Poor code quality / Lack of authentication procedures / Use of vulnerable ICS protocols / Uncontrolled file sharing / *Zero-Day Vulnerabilities* / Integration of untested applications / Unnecessary replication of *Active Directory*
Embedded devices	– Errors inadequate management of settings / Lack of *hardening* in the system / Lack of update management / *Zero-Day Vulnerabilities* / Insufficient access control
Policies	– Inadequate data security awareness / Susceptibility to social engineering / Inadequate physical security / Insufficient access control

Subject 2: Specification for Cyber Security Projects

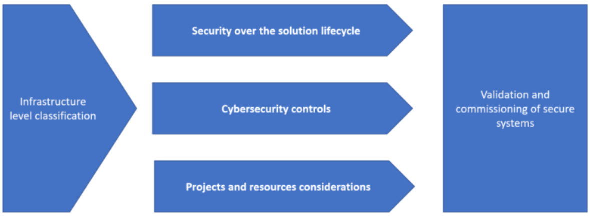
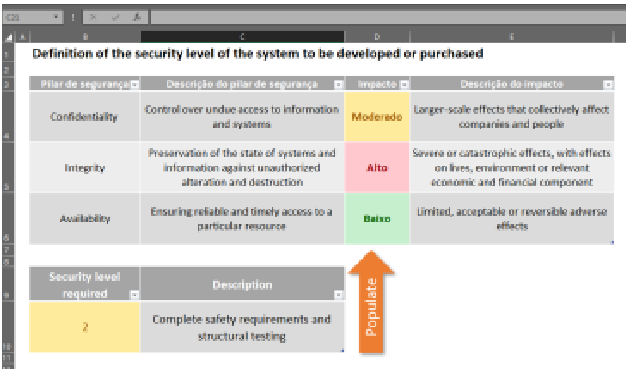

Infrastructure level classification
Security over the solution lifecycle
Cybersecurity controls
Projects and resources considerations
Validation and commissioning of secure systems

Figure 2 – Overall steps for Specification of Cyber Security Projects



Definition of the security level of the system to be developed or purchased

Pilar de segurança	Descrição do pilar de segurança	Impacto	Descrição do impacto
Confidentiality	Control over undue access to information and systems	Moderado	Larger-scale effects that collectively affect companies and people
Integrity	Preservation of the state of systems and information against unauthorized alteration and destruction	Alto	Severe or catastrophic effects, with effects on lives, environment or relevant economic and financial component
Availability	Ensuring reliable and timely access to a particular resource	Baixo	Limited, acceptable or reversible adverse effects

Security level required	Description
2	Complete safety requirements and structural testing

Study Committee D2

Information Systems and Telecommunication

Paper 10185_2022

A PRACTICAL APPROACH IN CYBERSECURITY MEASURES FOR BRAZILIAN UTILITIES continued

Subject 3: People Education

- Awareness and training of employees and cybersecurity staff in companies is a powerful tool to mitigate the risks of cyber incidents. It is important for stakeholder engagement and to stablish a security culture for the organization. According to NIST SP 800-16 [9], it is said: "Awareness is not training.
- Education is an ongoing process. Because cyber threats are constantly evolving, awareness and training mechanisms need to be frequent and constantly improved so that employees are always up to date.

Subject 4: Connectivity and IT Security

- Cigre working group investigated several possibilities before presenting what we understand as feasible for Brazilian situation. The list is a suggestion to be followed by utilities, rather them a definitive guidance.
- Given that, the process of improving cybersecurity in OT environments in energy companies must be continuous to mitigate equipment controls from external access and prevent the spread of disturbance within the industrial environment.
- Protection and control products must be equipped and implemented with security features and best practices associated with the use of each feature.
- Once all elements are configured to act in a safe way, it is necessary to have an environment that is possible to execute the test process. The process associated with a Security Testing, Assessment and Approval Laboratory is due to the continual emergence of new threats and vulnerabilities.
- The adoption of a SOC is a strong trend for industrial companies, especially the electricity sector, due to the various benefits it brings. It is important to say that the SOC is not created alone, it depends on a series of information so that a service that meets the needs of each company can be created or outsourced. Several aspects must be considered in its creation, from the retention of qualified professionals in the company, to the plan and performance metrics for SOC.

Conclusion

- This paper brings together 4 essentials pillars to build safer OT environments in the utilities market in Brazil. It highlights the importance of having cybersecurity in the agenda of the managing board, controlling cyber security risks as the companies does to all other risks that could affect the business continuity. The board must support resources and sponsor for cyber securities initiatives, including people, processes and technology needed to address the subject.
- Besides this engagement of managing board, there is a need to conduct Cyber Security Risks Analysis previously to any project deployment. It is basically impossible to protect an OT environment without having a clear view on the assets and risks associated.
- Furthermore, it is demonstrated the importance of having the right strategy for training and personal education, across the complete company hierarchy, and known roles and responsibilities related to the cyber security subject. Finally, there are example of solutions that could be implemented by Brazilian utilities.