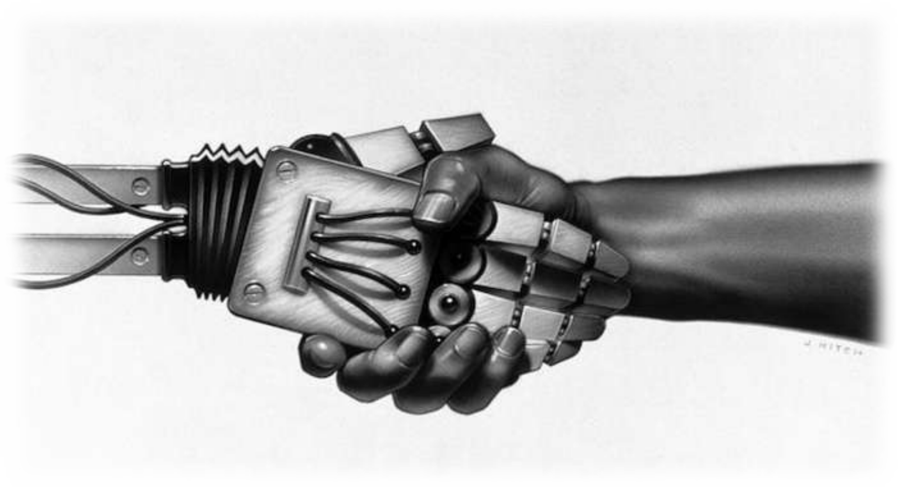
Smart Grid Cybersecurity 2020

edp distribuição

Substation Security
Developing an integrated cyber & physical security strategy



EDP Distribuição

Nuno Medeiros, Head of IT/OT Strategy and Cybersecurity

October 2020

EDP Distribuição is a company of the EDP Group, this being a global energy player with a strong presence in Europe, Brazil and considerable investments in the USA.

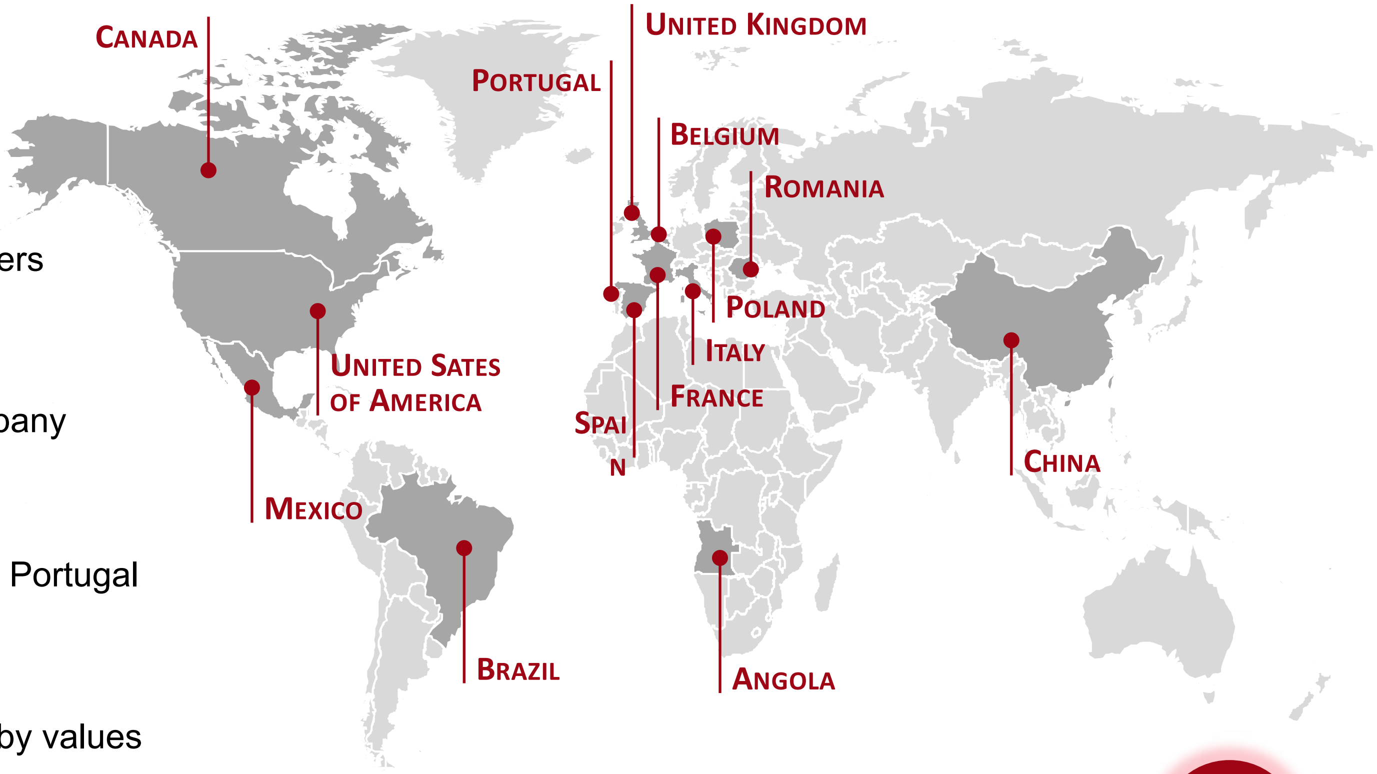
Present worldwide

11 Million electricity consumers

#4 World wind energy company

One of the largest employers in Portugal

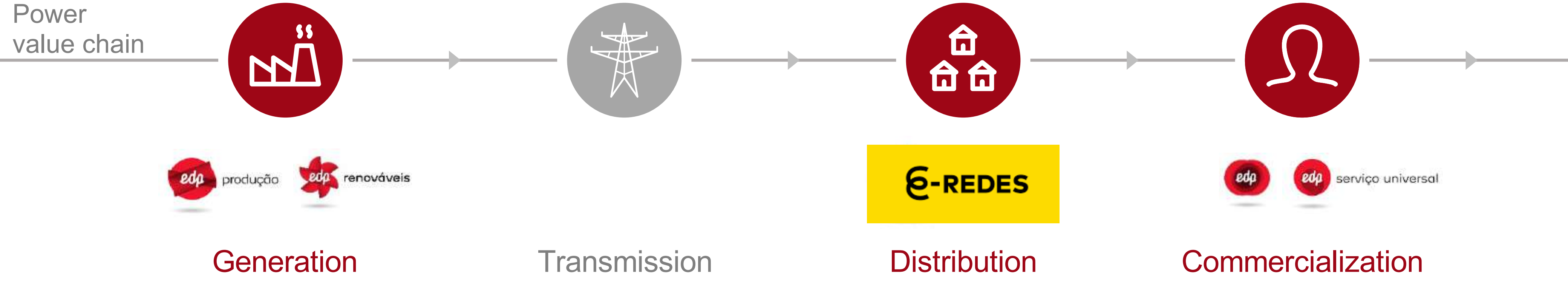
Highly committed and oriented by values



INITIATIVE ...... TRUST .... EXCELLENCE .... SUSTAINABILITY .... INNOVATION

edp distribuição

The Portuguese National Electricity System includes EDP Distribuição as the regulated electricity distribution company, acting under a public service concession.



Power value chain

edp produção edp renováveis

Generation

Transmission

E-REDES

Distribution

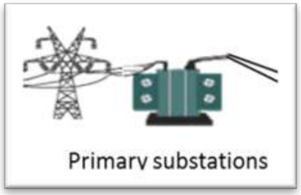
edp edp serviço universal

Commercialization

Mainland Portugal	+ 6 M	+3.200	220k	440	48.392 GWh
Geographic presence	Clients	Employees	KMs of Cable	Primary Substations	Energy entry on grid

edp distribuição

DSOs are facing different and complex threats accompanying its transformation, having to deal with the risks of cyber-based Blackouts. Substations are fully digitized and are no longer oversight



- Key assets for grid exploration and stability
- Average of 12.400 customers connected
- (very) Expensive and complex assets

Are Substations under Physical and Cyber Threat?

December 2015 - Ukraine:

- 3 DSOs – 30 Substations
- 250.000 people affected
- 1 to 6 hours to recover

… and it could have been worse!

December 2016 - Ukraine:

- 1 TSOs – 1 Substation
- People affected – tbc
- Swift recover

The Age of Hacker-Caused Blackouts Is Upon Us

A malware attack left thousands of homes without power in Ukraine and this is only the beginning.

Substation Cybersecurity must follow a Risk Mitigation Strategy assuring the implementation of the right mix of technical and procedural controls

Risk mitigation

Every Risk must be analyzed according to the potential impact of the event on the asset and its probability
The result of this analysis will determine if (and eventually how) the Risk should be reduced or accepted.

How can we reduce the risks?

By implementing controls that:

Prevent

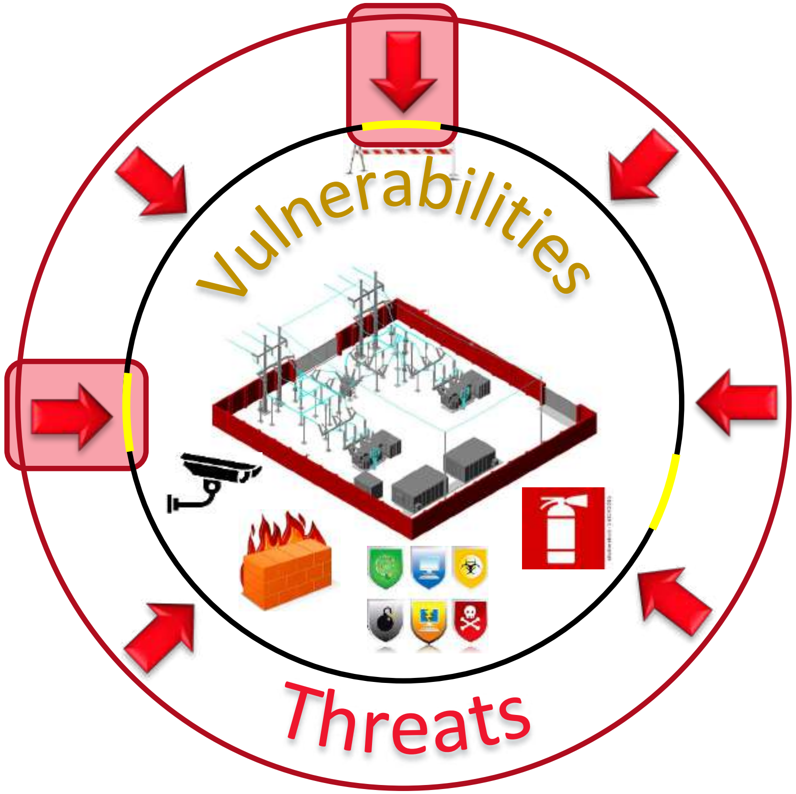
- Eliminate the vulnerability
- Create barriers to the threat
- Mitigate/reduce the impact of the event

Detect

- Deterring malicious activities
- Allow earlier detection of the events

Respond

- Incident response plan
- Redundancy and recovery mechanisms
- Incident forensics



edp distribuição

Easier said than done… this is Operational Technology (OT)
Substations offer a wide range of obstacles for the implementation of traditional controls

- **Diversity:** Different hardware and software solutions (manufacturers + generations)
- **Performance:** Applications run with limited resources and low configuration flexibility
- **Inflexible:** Software is always difficult to patch and vendors disagree with installing software from third parties (e.g. antivirus)
- **Unsecurity by-design:** Software- and Protocols-based security mechanisms are inexistent
- **Physical constraints:** There is limited space for equipment installation
- **Unnatended:** There is no personal ensuring physical security mechanisms

Security cannot degrade the relevant operational functions of technology

Substations represent critical assets for EDP Distribuição and it is fundamental and a priority to assess the maturity level of its cyber-physical security. The SICFSE project was launched.

Project Objectives	Risk Analysis	Controls and Roadmap

Review the current security status of EDP Distribuição substations, taking into account initiatives already underway.

Assess the current level of (cyber) security of SEs in the light of the most appropriate International standards, namely ISO27001.

Identify recommendations and complementary controls to be implemented, physically and logically, integrated in a strategic Roadmap.

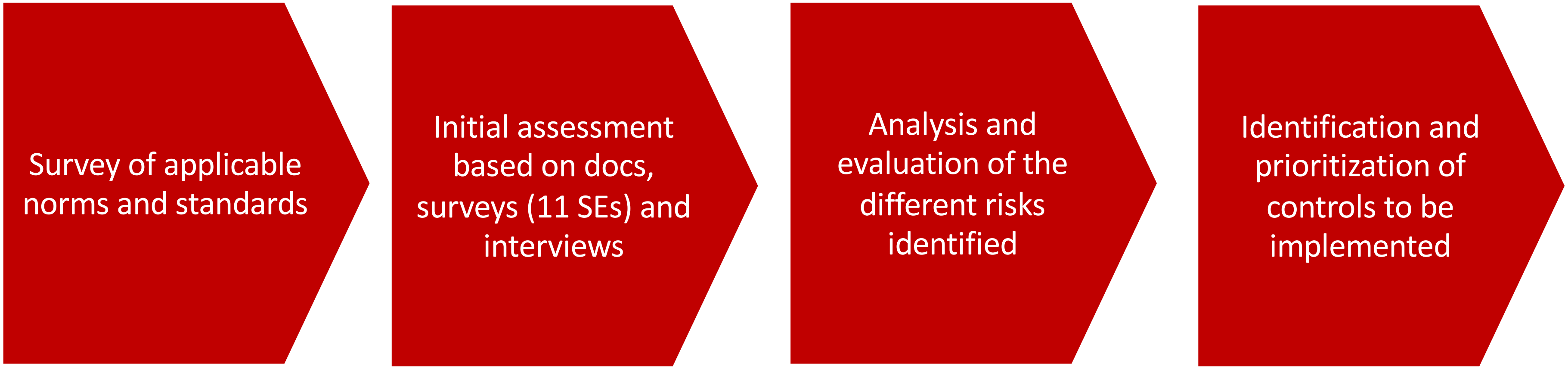
SIEMENS
Ingenuity for life

S2 GRUPO

edp distribuição

The project was divided in 4 stages

Project Objectives | Risk Analysis | Controls and Roadmap



Survey of applicable norms and standards

Initial assessment based on docs, surveys (11 SEs) and interviews

Analysis and evaluation of the different risks identified

Identification and prioritization of controls to be implemented

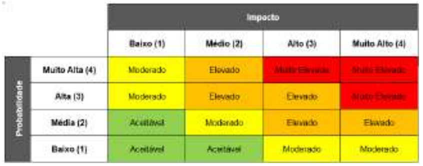
TECHNICAL REPORT

ISO/IEC TR 27019

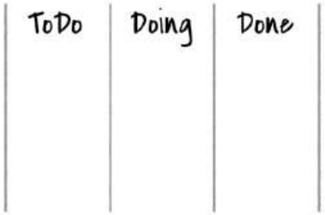
Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

[illegible]

ISO IEC



		Impacto			
		Baixo (1)	Médio (2)	Alto (3)	Muito Alto (4)
Probabilidade	Muito Alta (4)	Moderado	Elevado	Muito Elevado	Muito Elevado
	Alta (3)	Moderado	Elevado	Elevado	Muito Elevado
	Média (2)	Aceitável	Moderado	Elevado	Elevado
	Baixo (1)	Aceitável	Aceitável	Moderado	Moderado



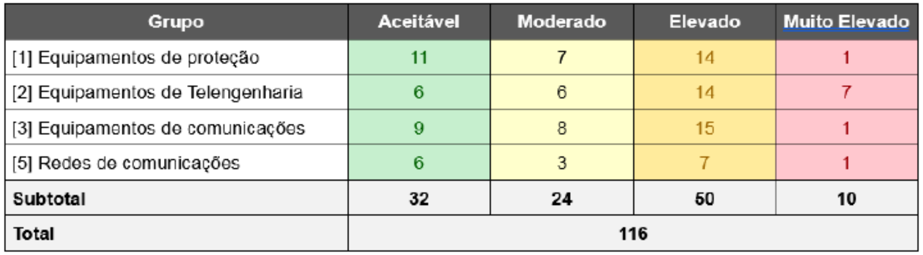
For the most critical substations, from Group 1 and 2, 10 very high-level risks were identified - taking into account the correspondent level of impact

Project Objectives | Risk Analysis | Controls and Roadmap

- **Substations Group 1:** Formally designated as national critical infrastructures – 26 substations
- **Substations Group 2:** Considered critical to Grid Stability for EDP Distribuição – 42 substations
- **Subestações Lote 3**: all other – 383

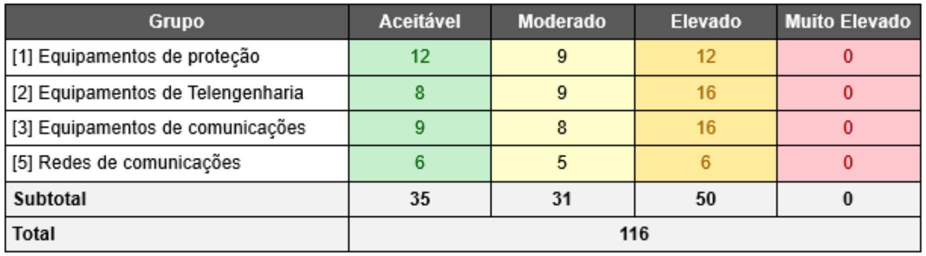
The results of the risk analysis are presented by each group:

Substations Group 1 and 2:



Grupo	Aceitável	Moderado	Elevado	Muito Elevado
[1] Equipamentos de proteção	11	7	14	1
[2] Equipamentos de Telengenharia	6	6	14	7
[3] Equipamentos de comunicações	9	8	15	1
[5] Redes de comunicações	6	3	7	1
Subtotal	**32**	**24**	**50**	**10**
Total	**116**			

Substations Group 3 (383):



Grupo	Aceitável	Moderado	Elevado	Muito Elevado
[1] Equipamentos de proteção	12	9	12	0
[2] Equipamentos de Telengenharia	8	9	16	0
[3] Equipamentos de comunicações	9	8	16	0
[5] Redes de comunicações	6	5	6	0
Subtotal	**35**	**31**	**50**	**0**
Total	**116**			

The conclusions of the risk analysis pointed out that the main cause for the existence of high risks is the low level of physical access control

Project Objectives | **Risk Analysis** | Controls and Roadmap

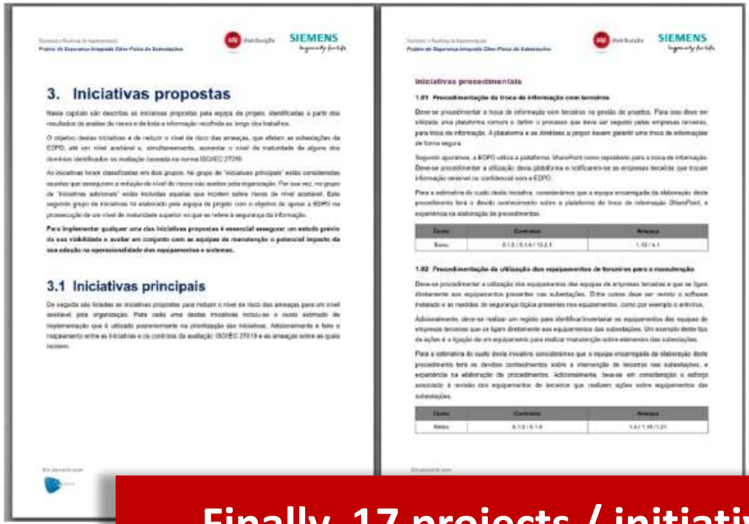
After the Risk Analysis carried out, it is possible to conclude:

- The results of the risk analysis reflect a set of high or very high risk threats to the assessed business process;
- The need to carry out a set of actions that allow the reduction of risks to an acceptable level;
- The most likely threats are a consequence of easy access to equipment (physical access to facilities or equipment) and security settings;
- The vulnerabilities were heterogeneously identified in the different types of substations, with no correlation between their criticality and the security measures implemented.

Following the risk analysis, 33 complementary controls were proposed to guarantee the reduction of the risk level of the installations

Project Objectives	Risk Analysis	Controls and Roadmap

Controls were identified, categorized into procedural, logical and physical security initiatives, and their estimated cost of implementation and impact on risks were assessed

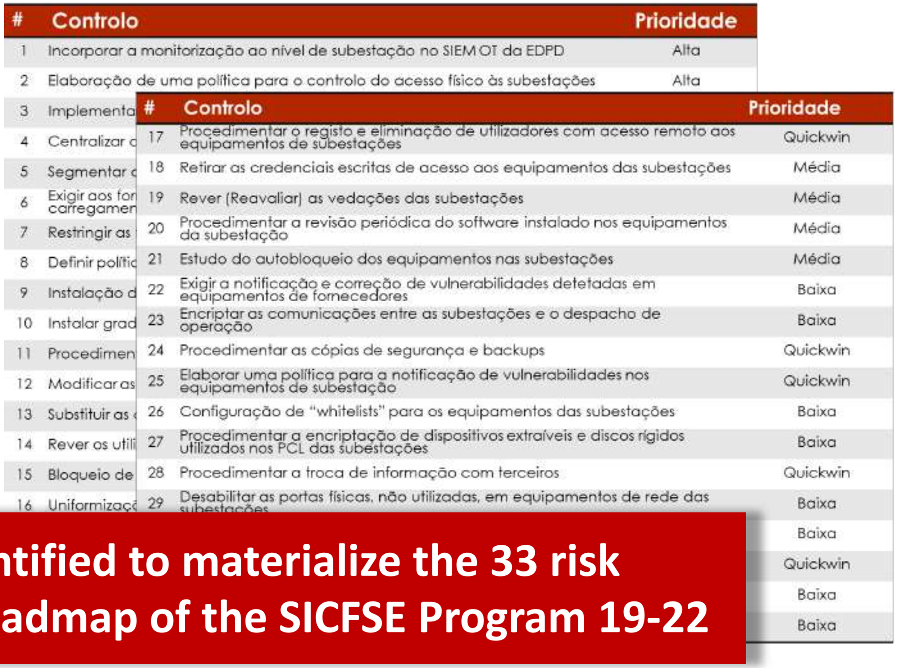


3. Iniciativas propostas

3.1 Iniciativas principais

Iniciativas procedimentais

After assessing the cost of implementing each control and its effect on risk reduction, the priority index of all controls was determined



#	Controlo	Prioridade
1	Incorporar a monitorização ao nível de subestação no SIEM OT da EDPD	Alta
2	Elaboração de uma política para o controlo do acesso físico às subestações	Alta
3	Implementa	
4	Centralizar c	
5	Segmentar c	
6	Exigir aos for carregamen	
7	Restringir as	
8	Definir politic	
9	Instalação d	
10	Instalar grad	
11	Procedimen	
12	Modificar as	
13	Substituir as	
14	Rever os utili	
15	Bloqueio de	
16	Uniformizaç	

#	Controlo	Prioridade
17	Procedimentar o registo e eliminação de utilizadores com acesso remoto aos equipamentos de subestações	Quickwin
18	Retirar as credenciais escritas de acesso aos equipamentos das subestações	Média
19	Rever (Reavaliar) as vedações das subestações	Média
20	Procedimentar a revisão periódica do software instalado nos equipamentos da subestação	Média
21	Estudo do autobloqueio dos equipamentos nas subestações	Média
22	Exigir a notificação e correção de vulnerabilidades detetadas em equipamentos de fornecedores	Baixa
23	Encriptar as comunicações entre as subestações e o despacho de operação	Baixa
24	Procedimentar as cópias de segurança e backups	Quickwin
25	Elaborar uma política para a notificação de vulnerabilidades nos equipamentos de subestação	Quickwin
26	Configuração de "whitelists" para os equipamentos das subestações	Baixa
27	Procedimentar a encriptação de dispositivos extraíveis e discos rígidos utilizados nos PCL das subestações	Baixa
28	Procedimentar a troca de informação com terceiros	Quickwin
29	Desabilitar as portas físicas, não utilizadas, em equipamentos de rede das subestações	Baixa
		Baixa
		Quickwin
		Baixa
		Baixa

Finally, 17 projects / initiatives were identified to materialize the 33 risk mitigating controls, incorporating the Roadmap of the SICFSE Program 19-22

edp distribuição

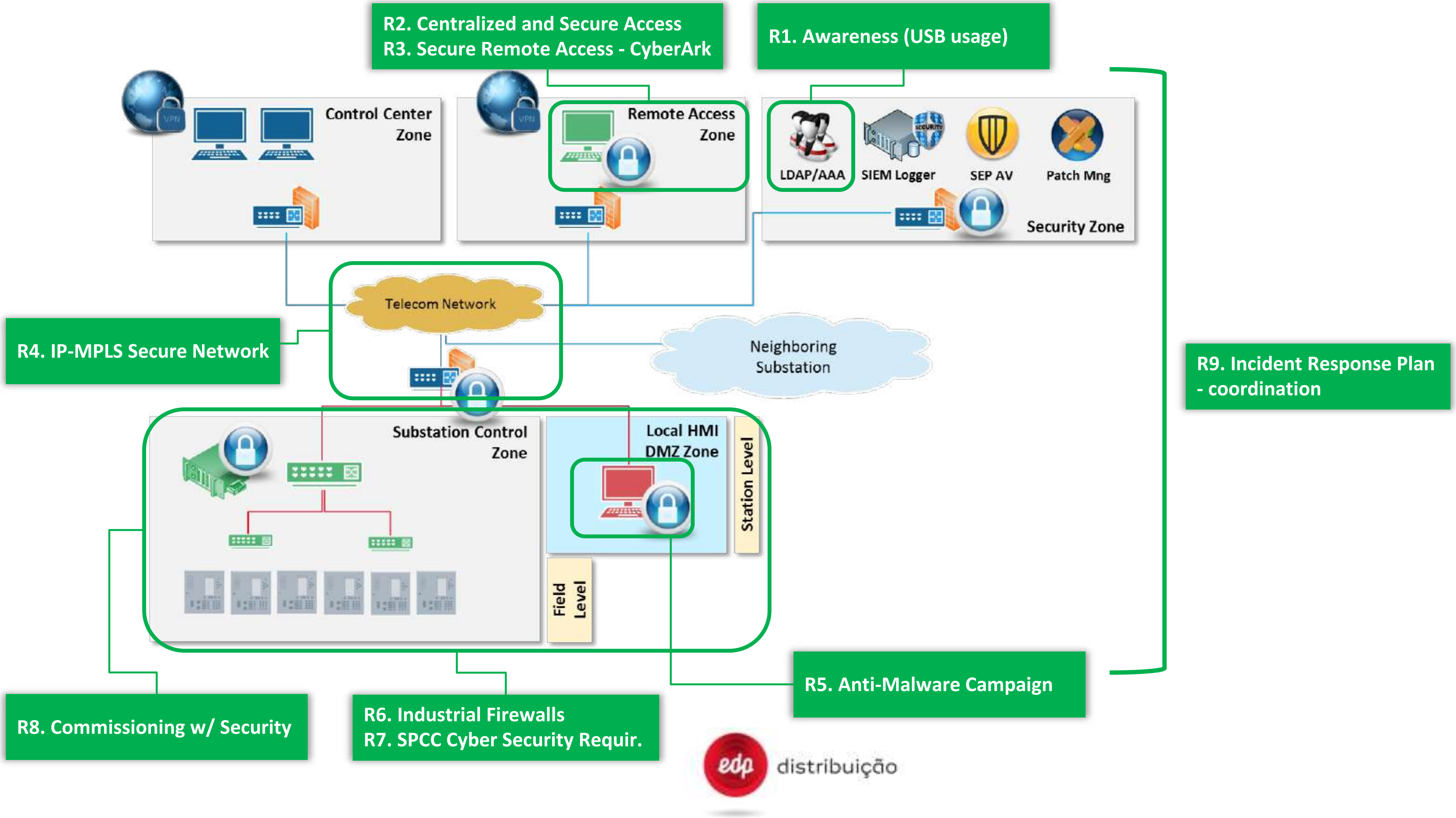
The strategy behind the SICFSE Program

Objectives

1. **Establish an Integrated Security Strategy for EDPD Substations –** through segmentation by security levels and respective applicable requirements to each substations group
2. **Integrated Substation Cyber-Physical Risk Management –** ensure the mitigation of unacceptable risks for these facilities, in line with a strategy and EDPD's risk matrix.
3. **Implementation of Fundamental Controls –** systematically implement the most relevant controls in line with the rationale of the previous analysis.
4. **Programming with an Holistic View –** monitoring of all initiatives and projects, favoring communication with internal and external entities (regulator., NCSC).
5. **Global Financial Planning –** ensure global insight of the investment plan aimed at the resilience of substations
6. **Extending the scope of ISO27001 –** implementation of the SICFSE program is a fundamental element for the certification of these installations, scheduled for Dec2021

Substation Cyber-Physical Security can only be achieved by implementing various complementary controls, within a Strategic Roadmap, assuring a one-size-fits-all overall solution

SICFSE Program: Roadmap for new and existing systems



R2. Centralized and Secure Access
R3. Secure Remote Access - CyberArk

R1. Awareness (USB usage)

R4. IP-MPLS Secure Network

R9. Incident Response Plan - coordination

R5. Anti-Malware Campaign

R8. Commissioning w/ Security

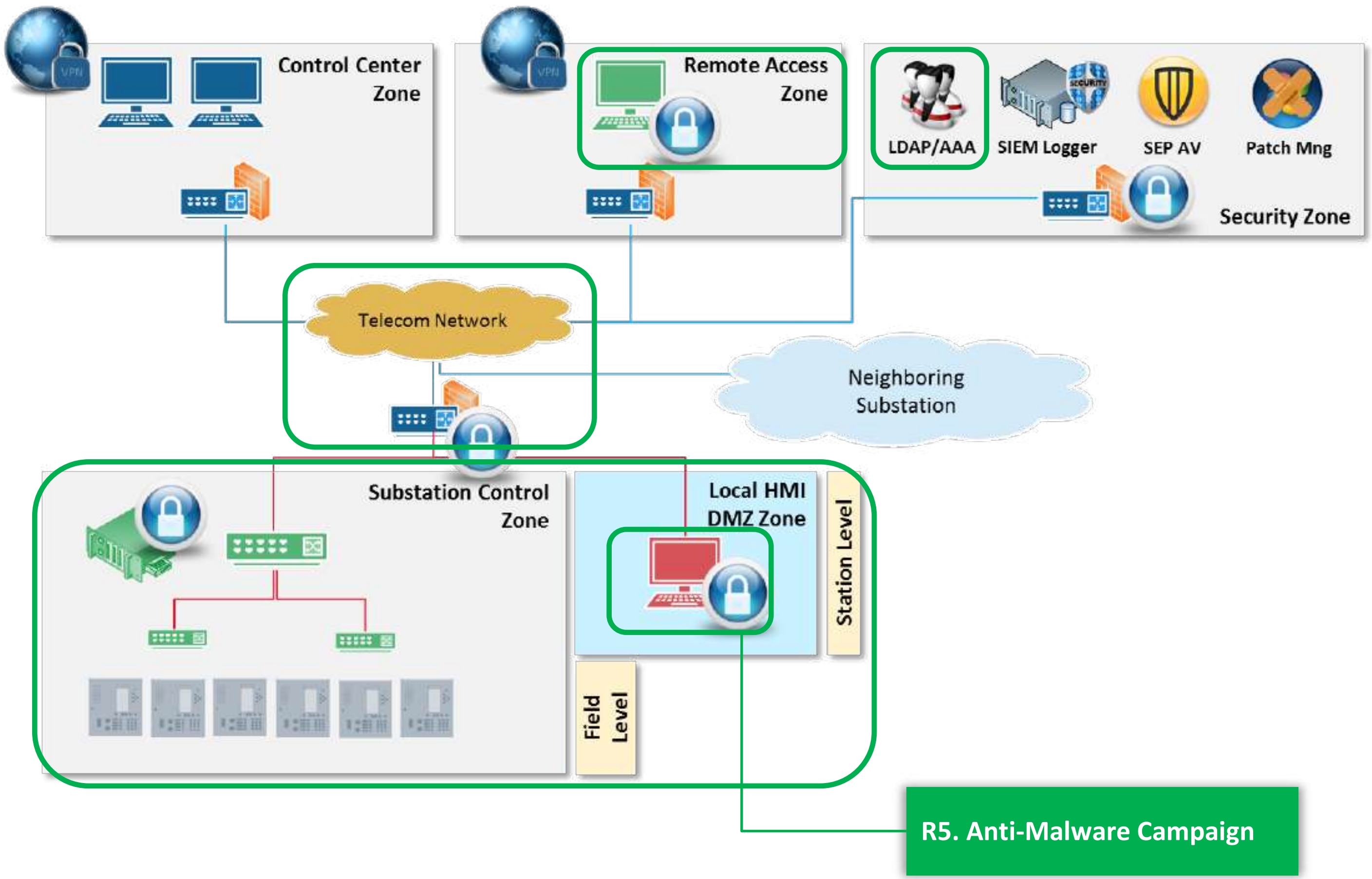
R6. Industrial Firewalls
R7. SPCC Cyber Security Requir.

EDPD Substations Cyber-Physical Security Roadmap

ON-GOING

R5. Anti-Malware Campaign

Initiative: Malware Control on Substation Workstations (HMI/PCL)

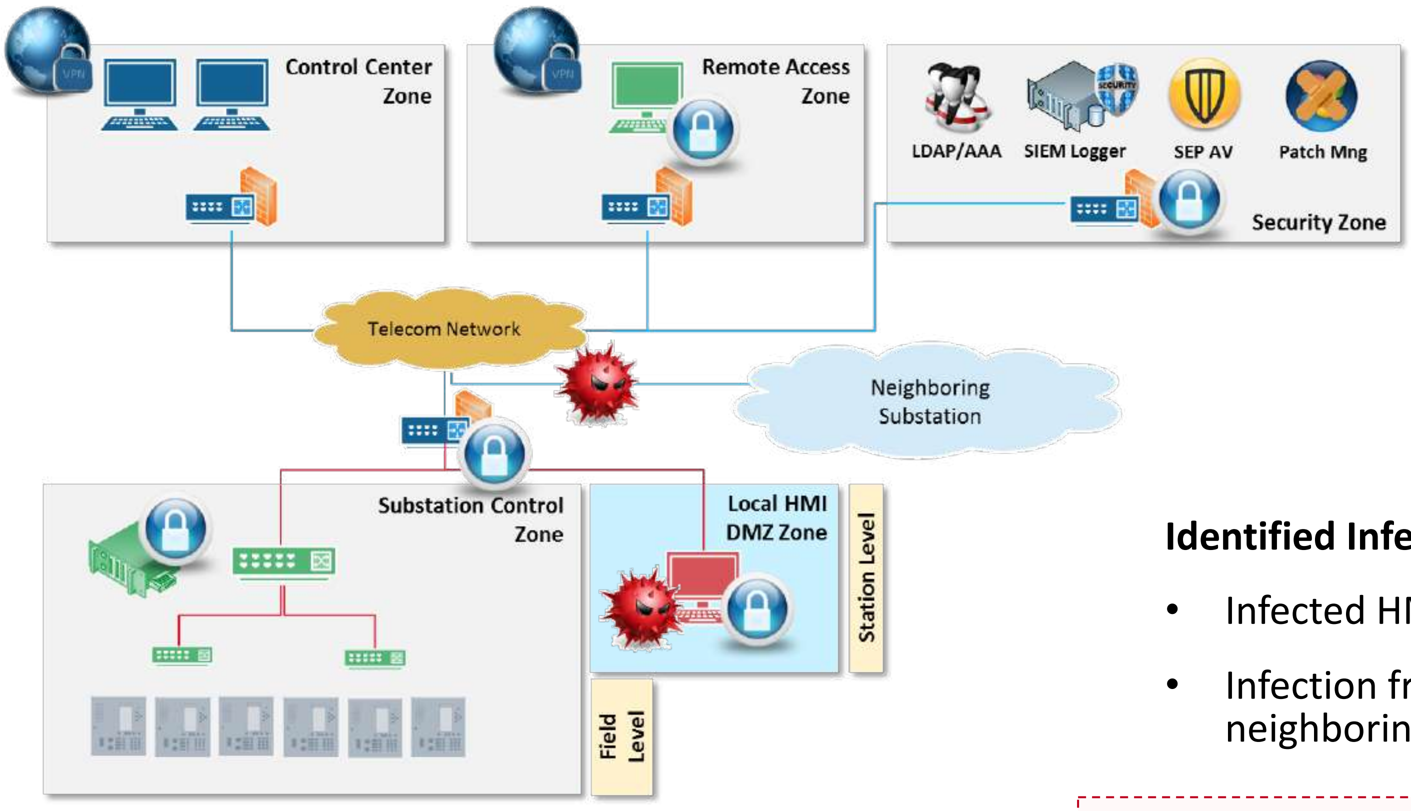


edp distribuição

EDPD Substations Cyber-Physical Security Roadmap

ON-GOING

R5. Anti-Malware Campaign



Identified Infection Scenarios

- Infected HMIs (directly)
- Infection from neighboring substations

⚠ **Not Normal but not Unusual**

edp distribuição

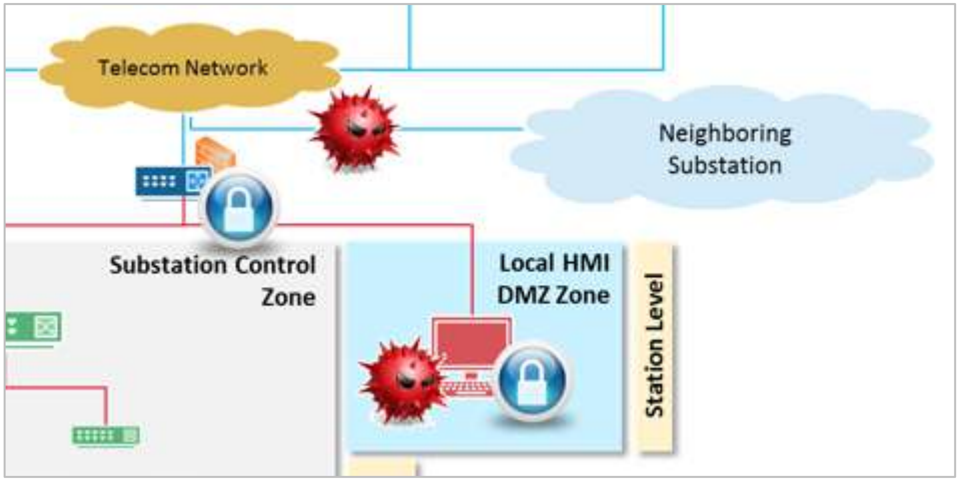
EDPD Substations Cyber-Physical Security Roadmap

ON-GOING

R5. Anti-Malware Campaign

Existing constraints

- Technological limitations: HMIs are outdated – not all have AV compatibility
- Obsolete Telecom solutions
- USB stick usage for Maintenance (internal and external users)
- High costs for technological upgrade (unit cost and volume)
- Solutions require centralized management (due to scale and complexity)



edp distribuição

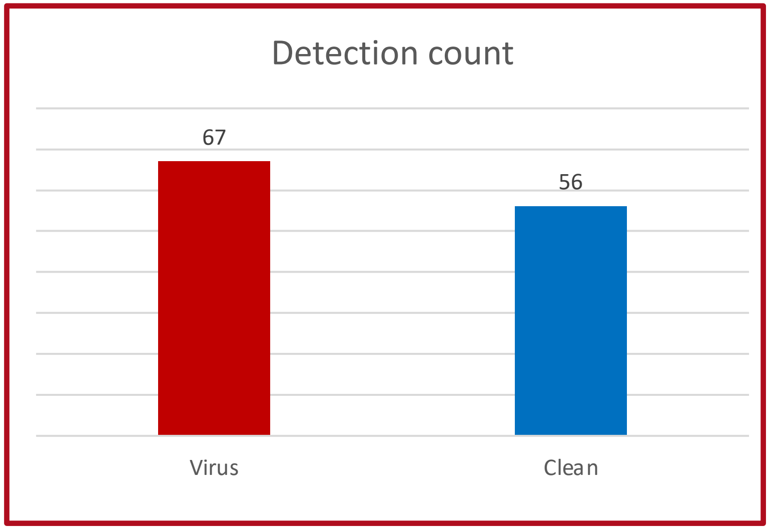
EDPD Substations Cyber-Physical Security Roadmap

ON-GOING

R5. Anti-Malware Campaign

EDP Substation anti-malware approach

- Conditioned to SEs with IP communications
- No heuristics (only known malware signatures are blocked –> no false positives)
- “light” execution for limited impact on performance
- AV client continuously adjusted for specific usage (HMI criticality)
- Vendor and generation-agnostic

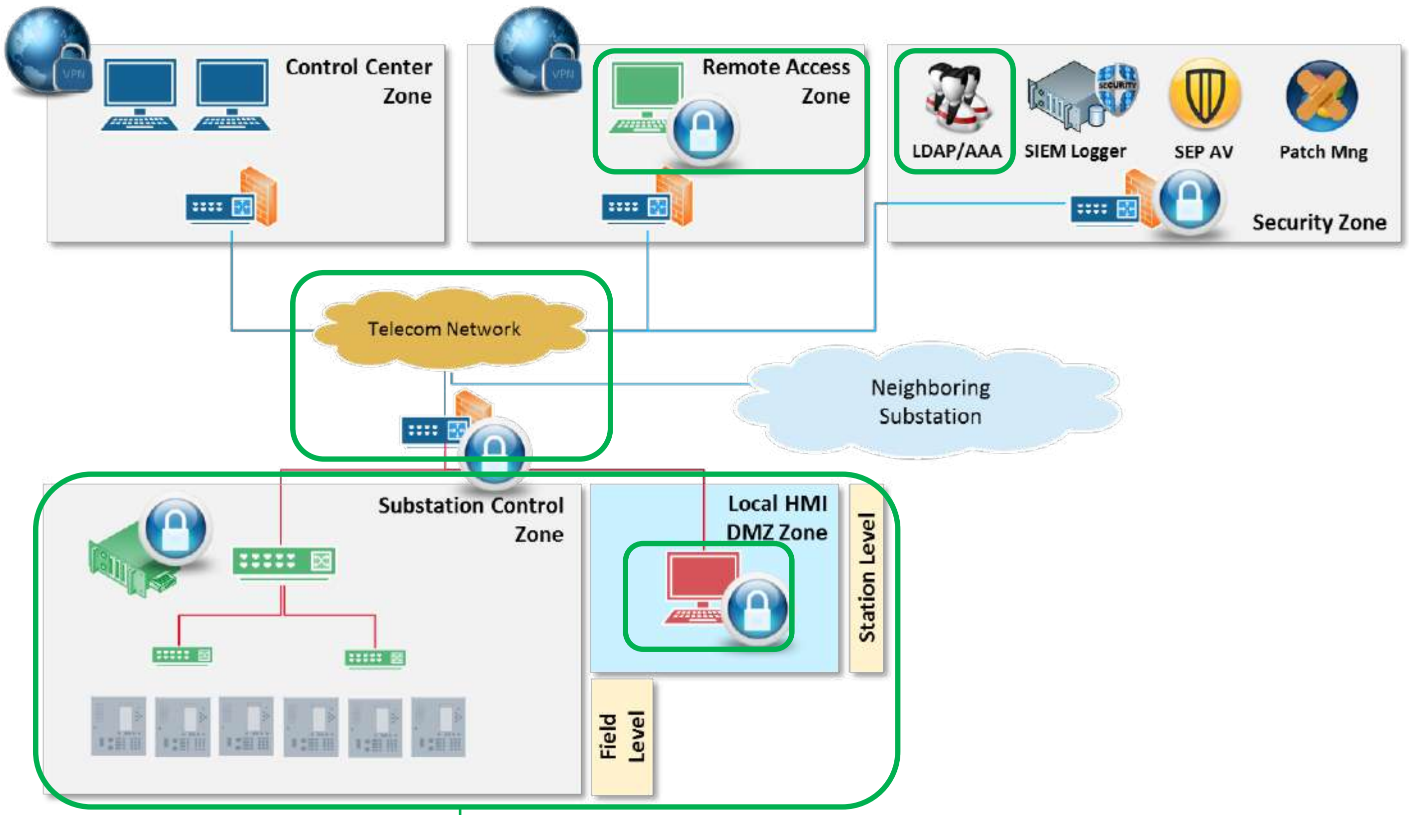


EDPD Substations Cyber-Physical Security Roadmap

ON-GOING

R6. Industrial Firewalls

Project: Implementation of Industrial NextGen Firewalls at Substations



R6. Industrial Firewalls

edp distribuição

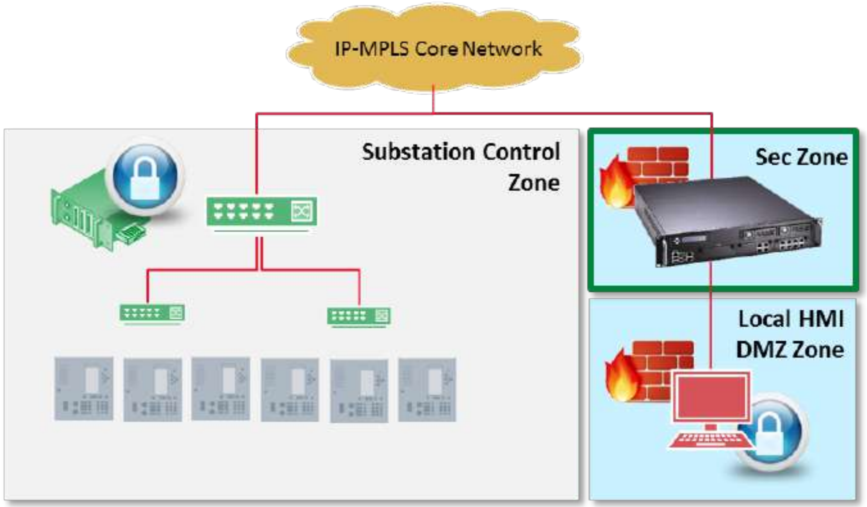
EDPD Substations Cyber-Physical Security Roadmap

ON-GOING

R6. Industrial Firewalls

A solution that can be built-in every substation:

- Ensure the Minimum Security Requirements
- Independent of existing technology;
- Be vendor- and solution- agnostic;
- Be simple to manage;



1 **Network Segregation**

Segregation of the internal networks allows controlling and monitoring of all devices traffic avoiding a free proliferation of malware and DoS attacks.

2 **Malware Protection**

The lack of antivirus in substation machines can be mitigated by performing network based malware control.

3 **Logging**

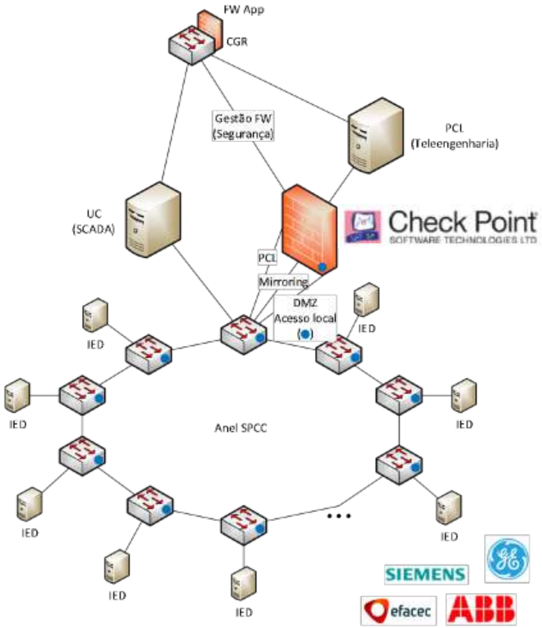
The collection of system and security events, and network traffic increases substation visibility, allowing the analysis and correlation in a central SIEM.

EDPD Substations Cyber-Physical Security Roadmap

ON-GOING

R6. Industrial Firewalls

The Architecture



The Features

Control of communications between HMI and LAN

Application of firewall rules and application control rules.

Visibility over LAN traffic

LAN traffic replication and analysis. Visibility over traditional protocols (HTTP, RDP, NTP) and industrial protocols (IEC 61850).

Control of communications between dispatchers laptops and the LAN (through DMZ)

New VLAN for local access authentication to LAN switches.

Application of control rules between the access VLAN and the substation LAN

Detection of threats on the LAN

Stateful firewall

Application control (Layer 7) *

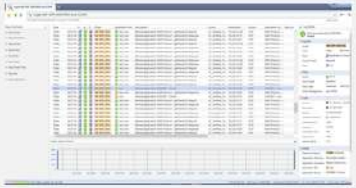
Anti-malware and Anti-Bot *

Next generation IPS *

* Atualização contínua.

Reporting of Cybersecurity events to the SIEM platform

Sending logs and notifications to the logging and correlation servers.



Centralized Management of the Firewalls

Update security policies and malware signatures.

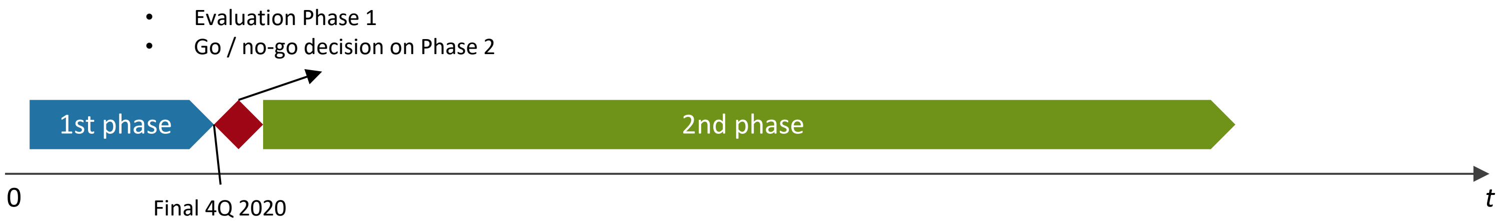
User and alarm management.

EDPD Substations Cyber-Physical Security Roadmap

ON-GOING

R6. Industrial Firewalls

The 1st phase of the Project is underway, with a scope centered on central systems and the installation of Firewalls in the Group 1 and 2 Substations. The 2nd phase will be dependent on the success of the project and will ensure expansion to the remaining 383 installations



- Evaluation Phase 1
- Go / no-go decision on Phase 2

Scope

- Installation of central systems
- Installation of Industrial FWs
    - N1: 26 criticisms for society (PSO)
    - N2: 42 critical to the stability of the system.
- Updating Substation Automation "type" Project
- Creating a new Alarm Source for PARIS
- Implementation of Security policy and corresponding processes

Objectives

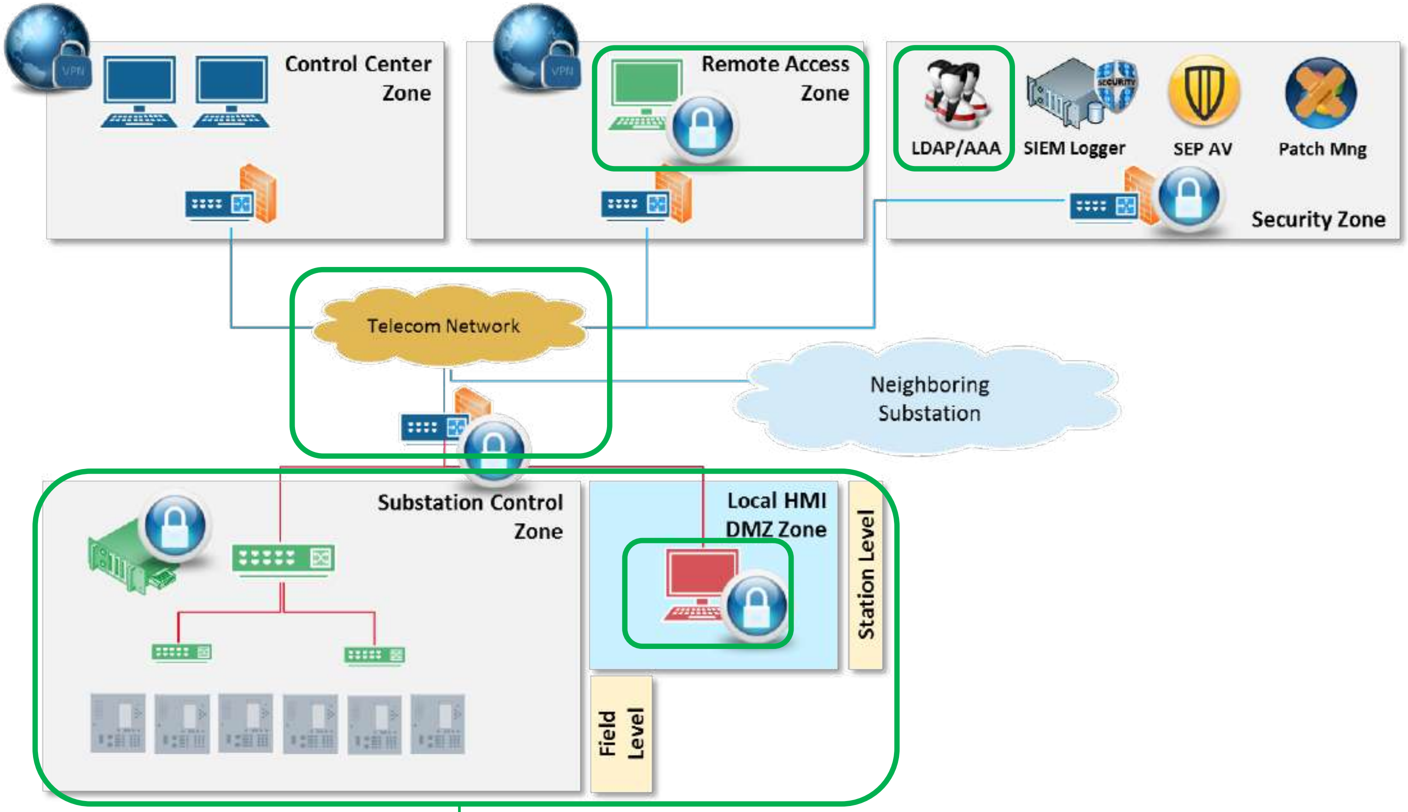
- Centralized solution management
- Traffic control between HMI and substation infrastructure (LAN network)
- Traffic visibility on the substation's LAN network, including industrial traffic
- Automatic threat detection at substations (signature and behavior-based)
- Log integration with the SIEM platform
- Local access control for the Substation network through DMZ
- Authentication of users on the DMZ network

edp distribuição

EDPD Substations Cyber-Physical Security Roadmap

R7. RTU Cyber Security Requir.

Initiative: Substation Automation Cyber Security Requirements (new substations)



R7. RTU Cyber Security Requir.

edp distribuição

EDPD Substations Cyber-Physical Security Roadmap

✓ R7. RTU Cyber Security Requir.

ENCS

Requirement Set

Components Security Requirements

for the Substation components (RTUs, IEDs, HMI, etc.)

New Substations - Critical Components

Control Systems Manufacturers

High (*Mission Critical*)

- Requirement List: security controls that are "Mandatory" or "Recommended" to specific components.

SFR. Future-Proof Design
SFR.01 Future-Proof Design
SFR.02 Remote Firmware Updates

SPR. Cryptographic Algorithms and Protocols
SPR.01 Cryptographic Algorithms and Key Lengths
SPR.02 Cryptographic Number Generation
SPR.03 Key Management

SHR. System Hardening
SHR.01 Device Hardening
SHR.02 Interface Minimization
SHR.03 Account Hardening
SHR.04 Security-enhancing features

SLR Logging
SLR.01 Logging Security Events

SUR Assurance
SUR.01 Design Evidence
SUR.02 Security Testing
SUR.03 Secure Coding Practices

SCR. Communication Security
SCR.01 Confidentiality
SCR.02 Message Integrity
SCR.03 Firmware Integrity
SCR.04 Message Freshness
SCR.05 Message Authentication
SCR.06 Non-Repudiation

SRR. Resilience
SRR.01 Message Validity Verification
SRR.02 Fail-Secure Operation

SAR Access Control
SAR.01 Role-Based Access Control (RBAC)
SAR.02 User Authentication

SDR Product Lifecycle and Governance
SDR.01 Information Security Management System
SDR.02 Configuration Management System
SDR.03 Secured Versioning
SDR.04 Vulnerability Handling Process
SDR.05 Security Updates and Patching
SDR.06 Security Training and Awareness
SDR.07 Production Security & Credential Provisioning

Key Takeaways

- Substations are digitized and therefore prone to cyber threats
- Very complex ecosystems – real time critical, ubiquitous, diverse, legacy & IT
- Risk Management is always the best approach – systematize and communicate
- There is no silver bullet for the security of Substations
- Assure global strategy for all substations
  - Start anticipating the future
  - Assure agnostic solutions for the present

Substation Security
Developing an integrated cyber & physical security strategy

Nuno Medeiros
nuno.medeiros@edp.pt

edp distribuição