.

Projeto n.º 47210

A2 - Requisitos e Especificações Técnicas

E2.4 – Requisitos e especificações técnicas para o módulo de cibersegurança

Autor	Francisco Falcão [Armis], Bruno Pinho [Armis], José Querido [Armis], Ana Cristina Aleixo [Efacec], Nuno Rodrigues [Efacec]
Nível de Divulgação	Confidencial
Data	2022-05-26
Revisão	1.0
Páginas	31
Palavras-Chave (*keywords*)	

Resumo do Projeto

O projeto SCALE perspetiva o desenvolvimento de uma plataforma para subestação de distribuição digital, que permita o controlo, monitorização e proteção de redes energéticas de média tensão de forma centralizada. Esta solução, projetando e desenvolvendo sistemas de proteção centralizados para subestações, desafia, não só, as arquiteturas de subestação digital atuais, baseadas em comunicações óticas, mas também outras temáticas basilares, como as infraestruturas e soluções cloud-based, big data e data privacy. A solução a desenvolver consistirá, assim, numa arquitetura inovadora e de alto valor acrescentado face aos atuais sistemas disponibilizados.

Projeto SCALE é financiado por

Documento

Projeto	SCALE	
Nome do Projeto	*Scalable Centralized Grid Protection, Automation and Control*	
Número do Projeto	47210	
Título do Documento	Requisitos e especificações técnicas para o módulo de cibersegurança	
Revisão e Data	1.0	2022-05-26
Editor	Bruno Pinho [Armis]	
Revisor	Francisco Falcão [Armis], Bruno Pinho [Armis], José Querido [Armis], Ana Cristina Aleixo [Efacec], Nuno Rodrigues [Efacec]	
Autores	Francisco Falcão [Armis], Bruno Pinho [Armis], José Querido [Armis], Ana Cristina Aleixo [Efacec], Nuno Rodrigues [Efacec]	
Páginas	31	

Revisões

Rev.	Data	Comentários	Autor
1.0	2022-05-26	Lançamento do documento.	Francisco Falcão [Armis], Bruno Pinho [Armis], José Querido [Armis], Ana Cristina Aleixo [Efacec], Nuno Rodrigues [Efacec]

Sumário Executivo

O presente documento pretende apresentar um conjunto de soluções a problemas da área de cibersegurança, a implementar durante o desenvolvimento do projeto SCALE. Durante a fase de planeamento do projeto foram delineados requisitos e processos chave para a implementação da CPC. Neste documento é descrita a análise feita aos requisitos identificados, com o intuito de apoiar o desenvolvimento dos componentes de segurança do sistema.

Depois da análise é recomendada a implementação de *firewalls* para filtragem de dados em trânsito e segmentação dos componentes da rede. Será implementado também um servidor LDAP que servirá para autenticação dos utilizadores do sistema, assim como um servidor *syslog* que será utilizado como repositório central de *logs*. As comunicações serão encriptadas com chaves públicas, para garantir a confidencialidade das mensagens face a ataques. É também recomendada a implementação de um sistema de deteção de intrusões, ou *Intrusion Detection System* (IDS). Adicionalmente, será implementado um sistema de *White-listing*, para evitar a execução de aplicações não aprovadas.

Em suma, garantir a segurança das infraestruturas críticas relacionadas com os equipamentos inteligentes e subestações contra os riscos e vulnerabilidades inerentes é de máxima prioridade. *Hardening* dos equipamentos e a adoção de técnicas de defesa em profundidade são exemplos de mecanismos de mitigação de danos ao sistema e aos dados em circulação.

Índice