gridspertise
accelerating your electric future

Cyber Resilience Forum

Safety and security of critical energy infrastructures

13/05/2023

Agenda

01

EU regulation scenario

02

IoT/OT Cyber Security landscape

03

Cyber Security Resilience in Gridspertise portfolio

04

Gridspertise cyber security resilience solutions examples

EU regulation scenario

Network Code

The Network Code on Cybersecurity aims to set a European standard for the cybersecurity of cross-border electricity flows. It includes **rules on cyber risk assessment**, common minimum requirements, **cybersecurity certification** of products and services, **monitoring**, **reporting** and **crisis management**.

NIS 2

Replaces and repeals the NIS Directive (Directive 2016/1148/EC)

CER directive

The **Critical Entities Resilience** Directive (CER) replaces the European Critical Infrastructure Directive of 2008. The new rules were published with the aim to reduce the vulnerabilities and strengthen the resilience of critical entities

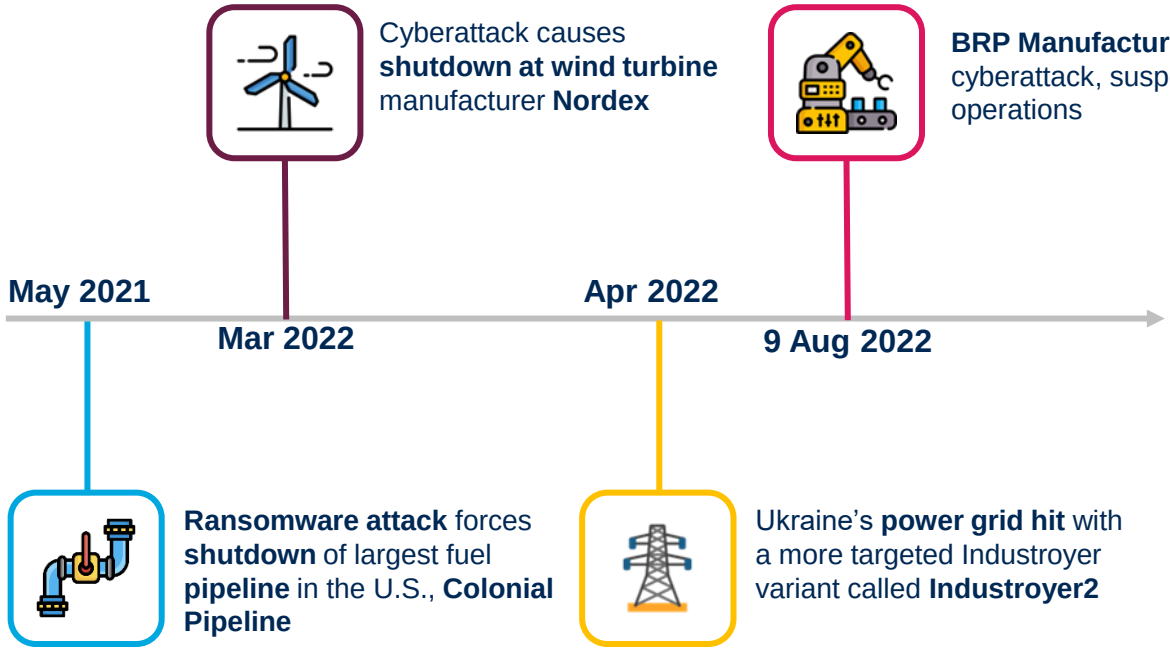
*Normally States have 2 years as deadline for applying the measures after the national publication

IoT/OT Cyber Security landscape

Threat landscape in digital grids[1]

- **Natural events** *(e.g. flooding, earthquake)*
- **Physical damage** *(e.g. environment damage or terrorist/vandalism activity)*
- **Compromise of functions** *(e.g. identity theft, abuse of rights)*
- **Interoperability** *(e.g. loose of control on supply chain)*
- **Compromise of information** *(e.g. tampering with software, malware)*
- **Technical failures** *(e.g. DoS or denial of control action)*
- **Loss of essential services** *(e.g. failure of telecommunication network equipment)*
- **Unauthorized actions** *(e.g. behavioral errors)*
- **Disturbance due radiation**

Examples of relevant IoT/OT cyber events in Y21/22*

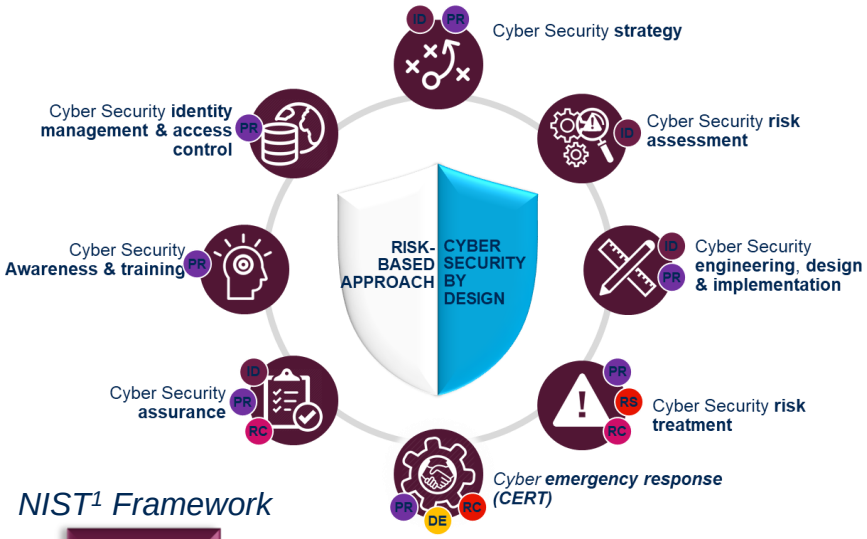


[1]Reference: ENISA Smart Grid Threat Landscape and Good Practice Guide

[2]Reference: Nozomi-Networks-OT-IoT-Security-Report-2022-2H, Security By Design (Politecnico di Milano)

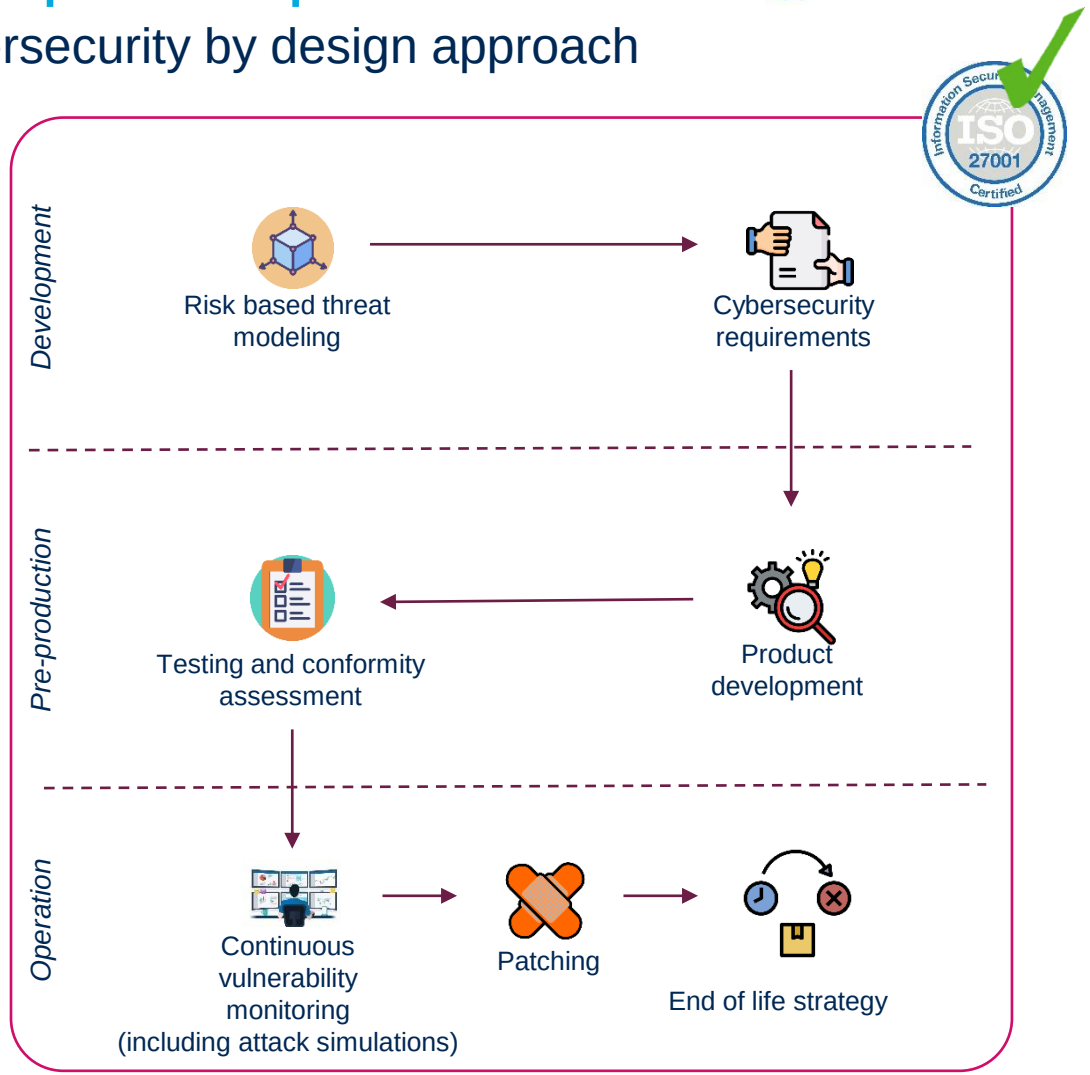
Cyber Security Resilience in Gridspertise porfolio

Cybersecurity Framework – Risk based and Cybersecurity by design approach



NIST[1] Framework

The Cyber Security Framework of the ENEL Group was issued in 2017 by the Group's CEO (Policy No. 17 v2 of December 2018)



1. National Institute of Standards and Technology

Gridspertise cyber security resilience solutions

Hands-on in our portfolio

Development

Risk based threat modeling

Cybersecurity requirements

Pre-production

Testing and conformity assessment

Product development

Operation

Continuous vulnerability monitoring (including attack simulations)

Patching

End of life strategy

Hardware/Software requirements (some examples)

- **Antitamper** — Evidence, resistance, response
- **Encryption** — For data-in-transit and data-in-storage
- **Hardening** — Physical and software level
- **Monitoring** — Security events logging
- **Patching** — Complete and secure patching capabilities
- **Access control** — RBAC approach, centralized access control
- **Wireless security** — Specific measures to protect wireless communication channels

Secure development and conformance testing

- **Test at developers**
- **Security development guidelines**
- **Preproduction tests** — Static and dynamic code review; Penetration test
- **Technical conformity assessment**

Continuous vulnerability management

- **Vulnerability early warning system**
- **Periodic testing** — Penetration test, vulnerability analysis, red vs blue team, cyber exercise, etc
- **Risk based vulnerabilty patching**
- **End of life strategy**

gridspertise
accelerating your electric future

Cyber Resilience Forum

Safety and security of critical energy infrastructures

13/05/2023