WHEN TRUST MATTERS

Cyber sikkerhet for vern i kraftsystemet

Praktiske råd og prioriterte tiltak for å sikre vern i substasjoner

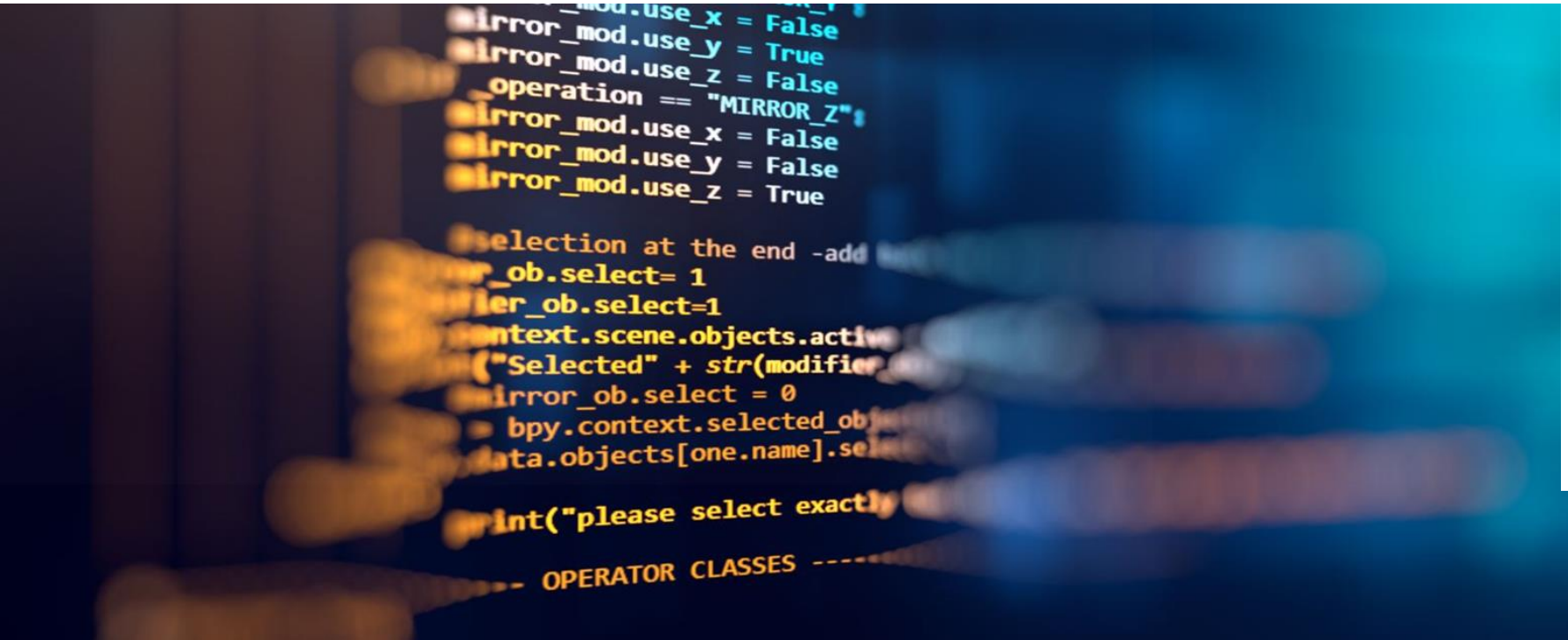
Kirsti Eikeland, Principal consultant, DNV CYBER SECURITY SERVICES

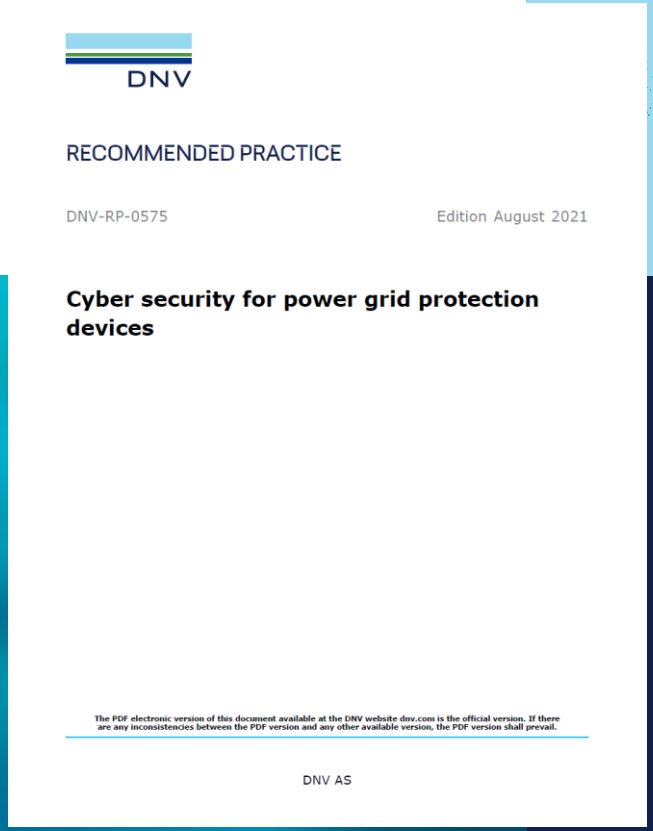
01 November 2021

WHEN TRUST MATTERS

DNV Recommended Practice

Cyber security for power grid protection devices




DNV

RECOMMENDED PRACTICE

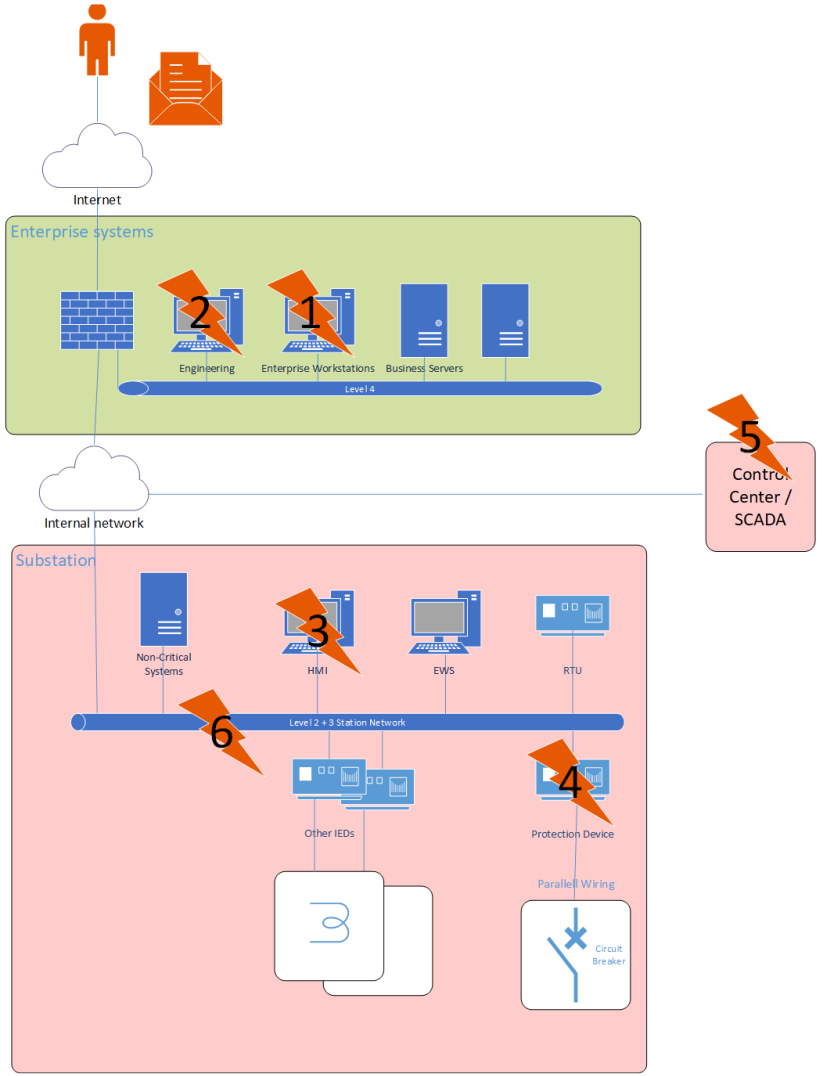
DNV-RP-0575 Edition August 2021

Cyber security for power grid protection devices

The PDF electronic version of this document available at the DNV website dnv.com is the official version. If there are any inconsistencies between the PDF version and any other available version, the PDF version shall prevail.

DNV AS

The Ukraine cyber attack revealed new vulnerabilities



Ukraine power grid attack in 2015/2016 is the first known successful cyber attack to take down a power grid

Attackers were, after a long, multistage attack able to access the HMI to control the protection devices and trip circuit breakers, causing a 6-hour power outage

The attack investigation exposed the vulnerability of, amongst other things, protection systems.

Two main attack surfaces : network level and device level

Protection devices

- The objective of power system protection is to isolate a faulty section of electrical power system from rest of the live system.

Security challenges in 2nd/3rd gen. substations

- Complex management and protection efforts
  - Newer, software-based devices exist alongside older devices in substations.
  - the old ones not being updateable (patch, anti-malware)
  - SW dependent devices potentially introducing new vulnerabilities
  - Security measures are limited by constraints of up-time requirements & limitations of modifications

Joining forces…

- Statnett (Norwegian TSO) supported a DNV led R&D project to investigate what grid operators should/could do to prevent such an attack from happening again
- Joined by Fingrid (Finnish TSO) and Svenska Kraftnät (Swedish TSO)

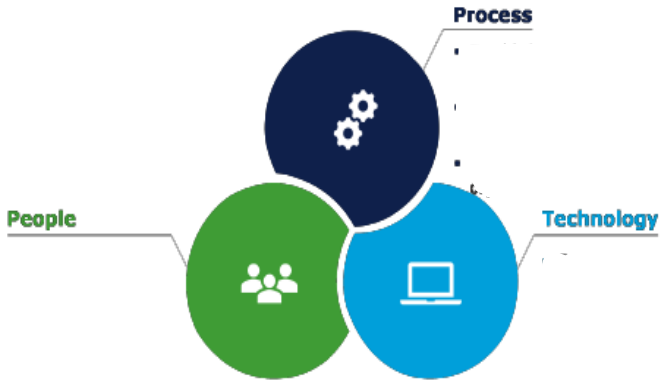
- The results of this R&D project is the foundation for the Recommended Practice.
- Updated & adjusted, peer- reviewed

To solve an **immediate** challenge

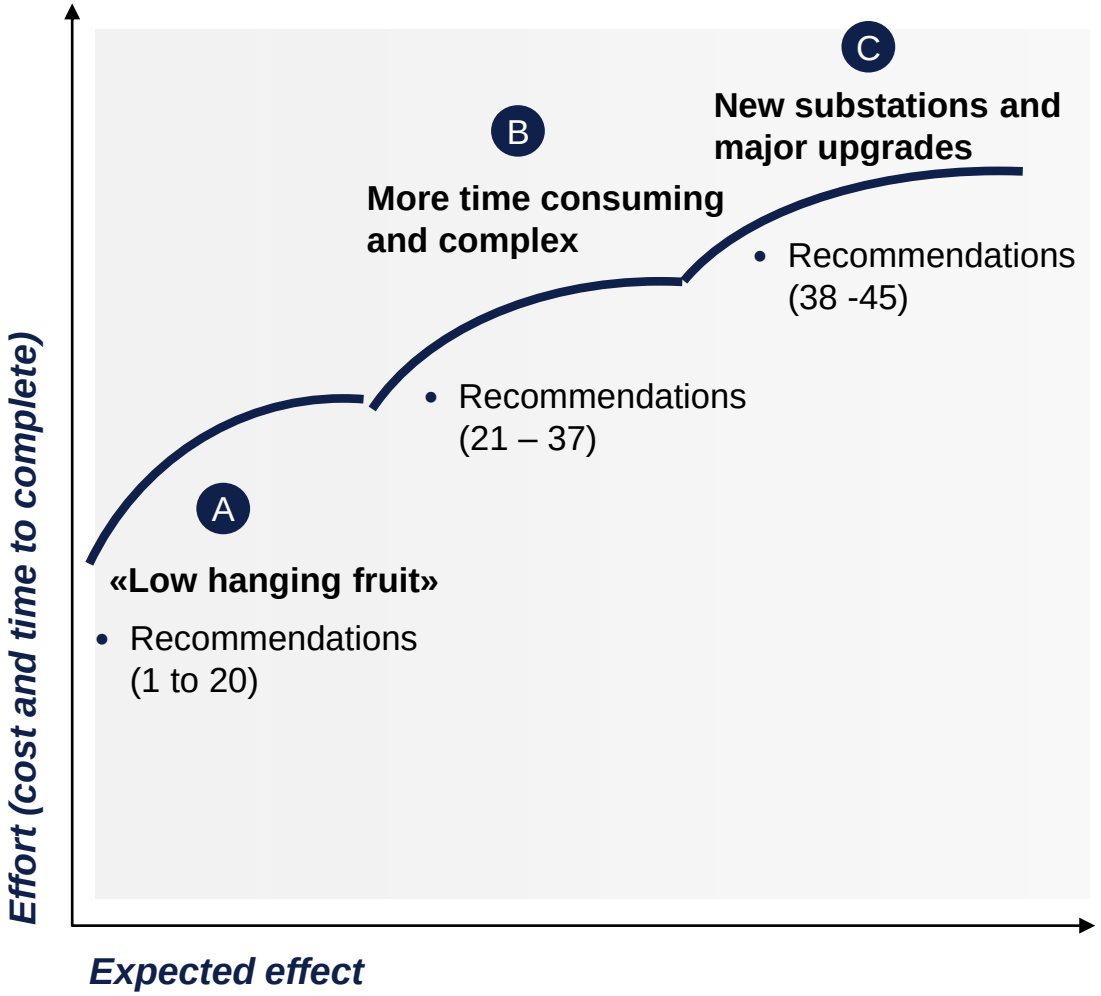
- the need to improve security in existing substations : where to start?

- support in prioritization of actions & mitigating measures

Improving security – getting the basics right



4.1 Cyber security management system
4.2 Substation lifecycle
4.3 Zones, conduits and barrier devices
4.4 Secure remote access
4.5 Malware control
4.6 Hardening
4.7 Patching
4.8 Production data export
4.9 Inventory management
4.10 Incident response and recovery
4.11 Intrusion detection system
4.12 User authentication and authorization
4.13 Logging and alarming



4.3 Zones, conduits and barrier devices

A **Mitigating measures: Low cost, short time to complete, no downtime "low hanging fruit"**

1. Assign a security level target to zones & conduits (i.e IEC/ISA 62443 part 3-2)
2. Regularly audit (e.g. yearly) firewall rules
3. Regularly pen test (e.g. yearly) firewalls
4. Implement 'management of change' on firewall rules

Improving protection against:

- Attack from the internet
  - Unauthorized network scanning, probing and modifications
  - Default/ weak credentials enables sniffing and/or hashing
  - DoS

B **More time consuming & complex / for major upgrades**

Securing IEC 101/104 protocols upgraded with secure versions or secured in e.g. virtual private network (VPN) tunnels or in dedicated networks with monitoring of firewalls and network traffic.

Renew substation zone model

Enable substations to run in «island mode»

4.4 Secure remote access

A **Mitigating measures: Low cost, short time to complete, no downtime "low hanging fruit"**

1. Regularly audit (e.g. 6m/yearly) remote access users and rights
2. Regularly pen test (e.g. yearly) the remote access system
3. Implement 'management of change' on remote access users and rights. e.g. defined limited lifetime

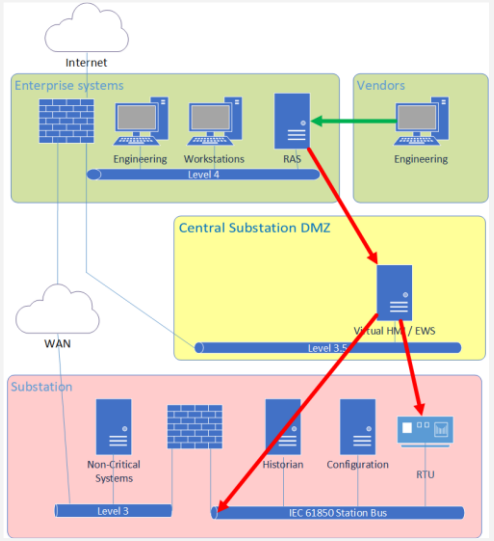
Remote access shall require multifactor authentication

Improving protection against

- Attack through vendor/partner maintenance services
- Decrease the risk of attackers utilizing vulnerabilities in open service accounts

B **More time consuming & complex / for major upgrades**

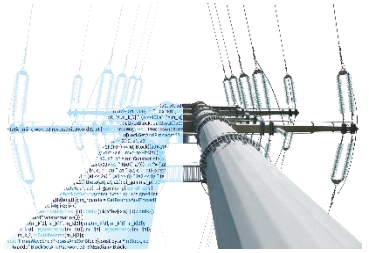
Establish a common secure remote access system (Dedicated or virtual RAS)



How to improve the RP?

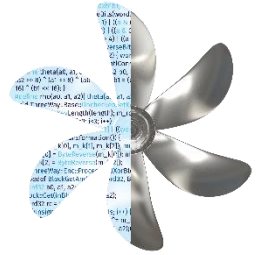
CYBER SECURITY FOR THE REAL WORLD

- In this first edition the focus is on practical measures solving some immediate cyber security challenges
  - The feedback has been very positive
- Improvements to RP – areas, topics etc are much welcome!
- https://www.dnv.com/cybersecurity/recommended-practices/dnv-rp-0575-cyber-security-for-power-grid-protection-devices.html
- Looking towards the future…!

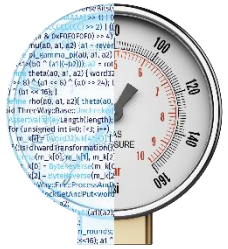


Electricity infrastructure & distribution

Renewables



Maritime



Oil and gas

DNV

Thank you

Kirsti.Eikeland@dnv.com

www.dnv.com

Cyber Security fra DNV

- Industry insight and a holistic security view is our specialty. DNV guides when the speed of digitalization challenges both safety and security.
- Combining IT, OT and domain knowledge to support our industry customers