CINELDI

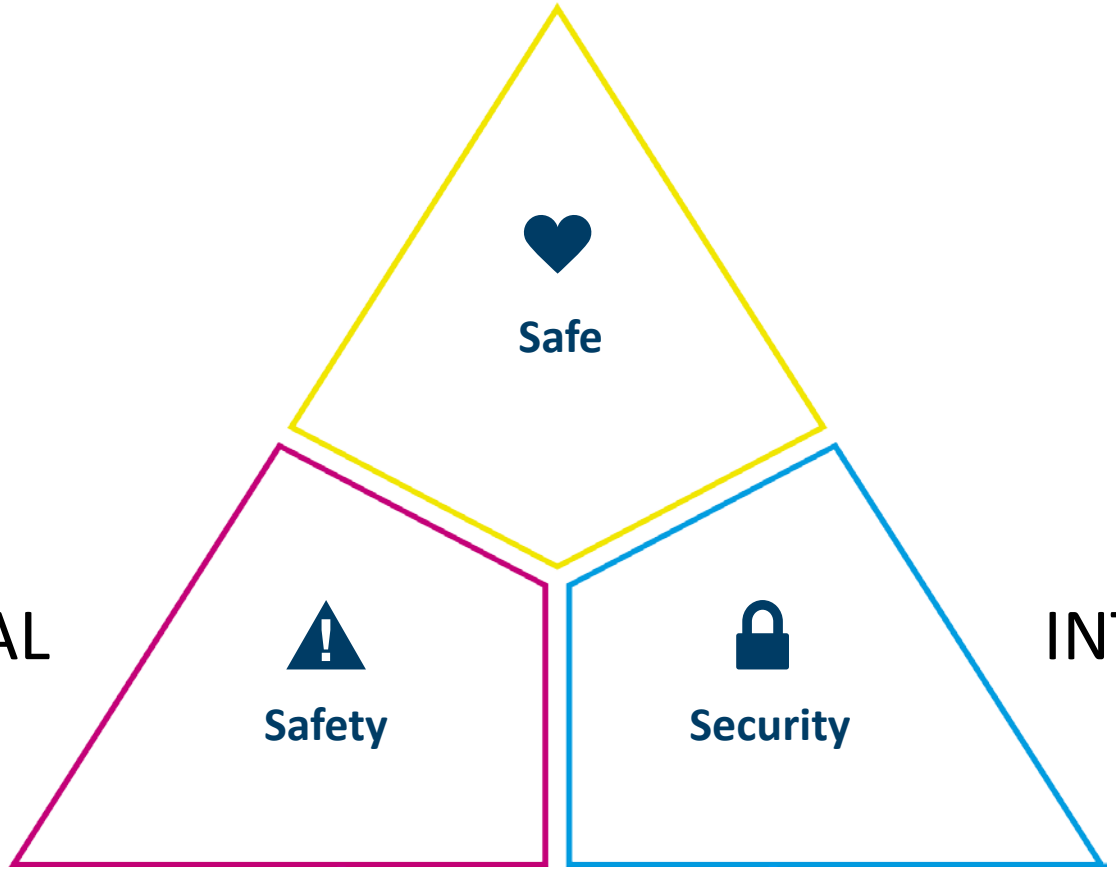
Centre for intelligent electricity distribution
- to empower the future Smart Grid

Cybersecurity misuse cases for future distribution grids

CINELDI konferansen, 9. April

Marie Moe, Research Manager Cyber security, SINTEF Digital

ACCIDENTAL

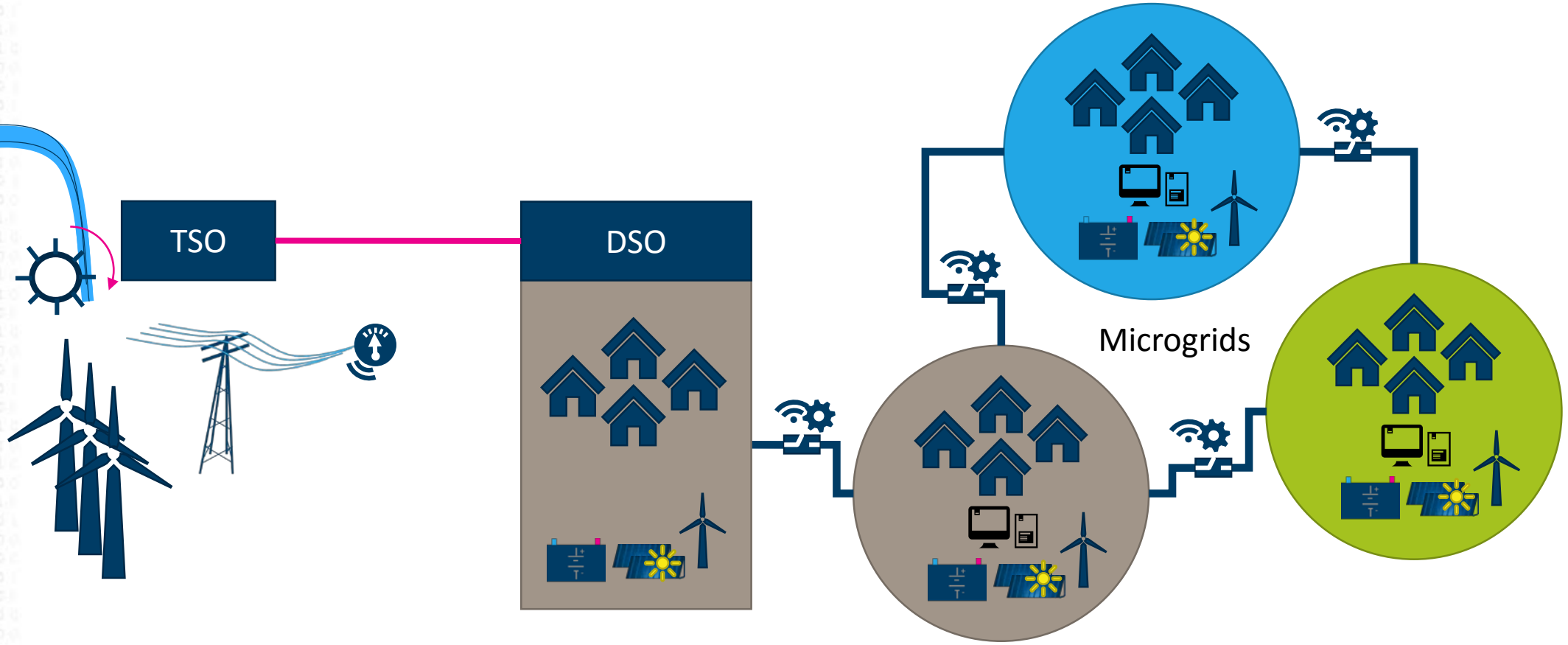


INTENTIONAL

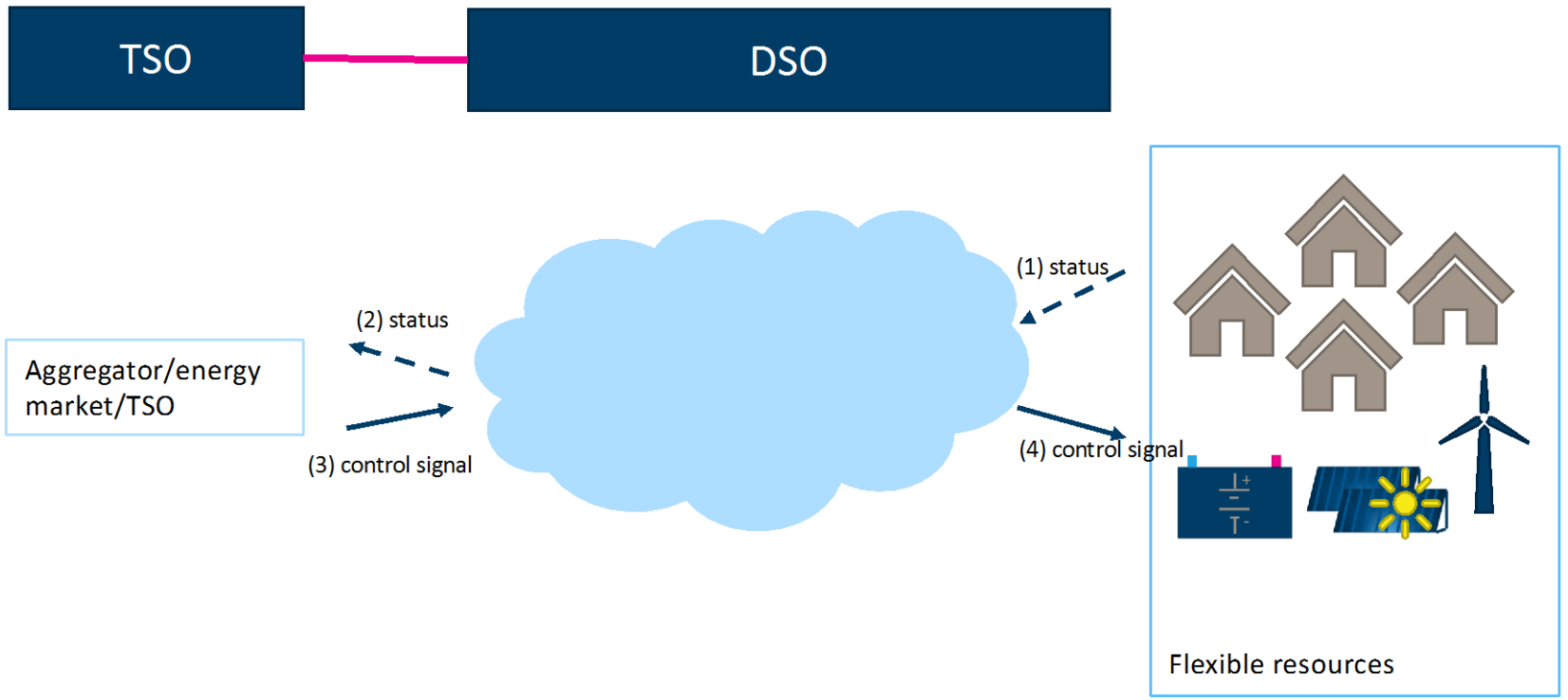
Misuse cases: Methodology

- Workshop with industry partners
- Misuse cases identified
- Literature study on cybersecurity threats in smart grids
- Interaction with other CINELDI WPs

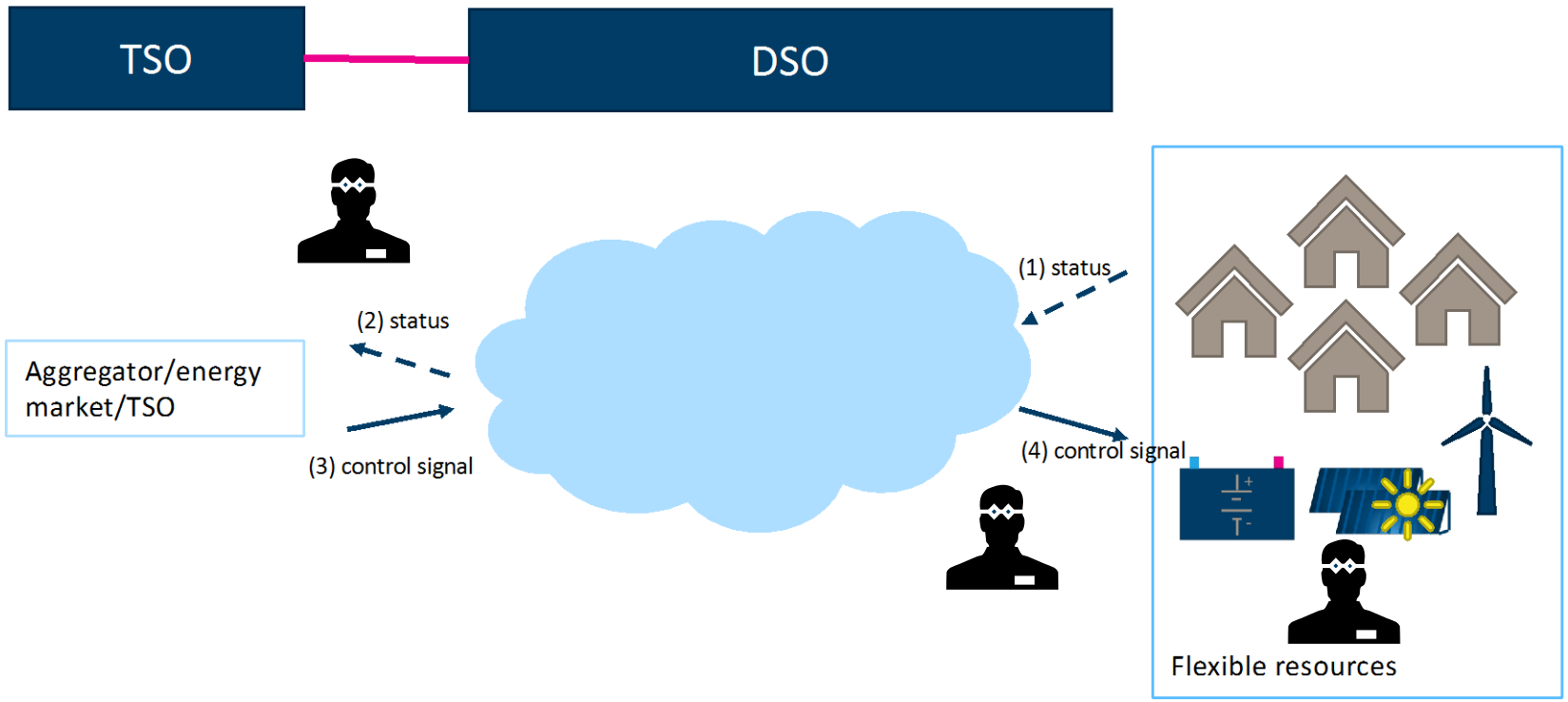
Scope



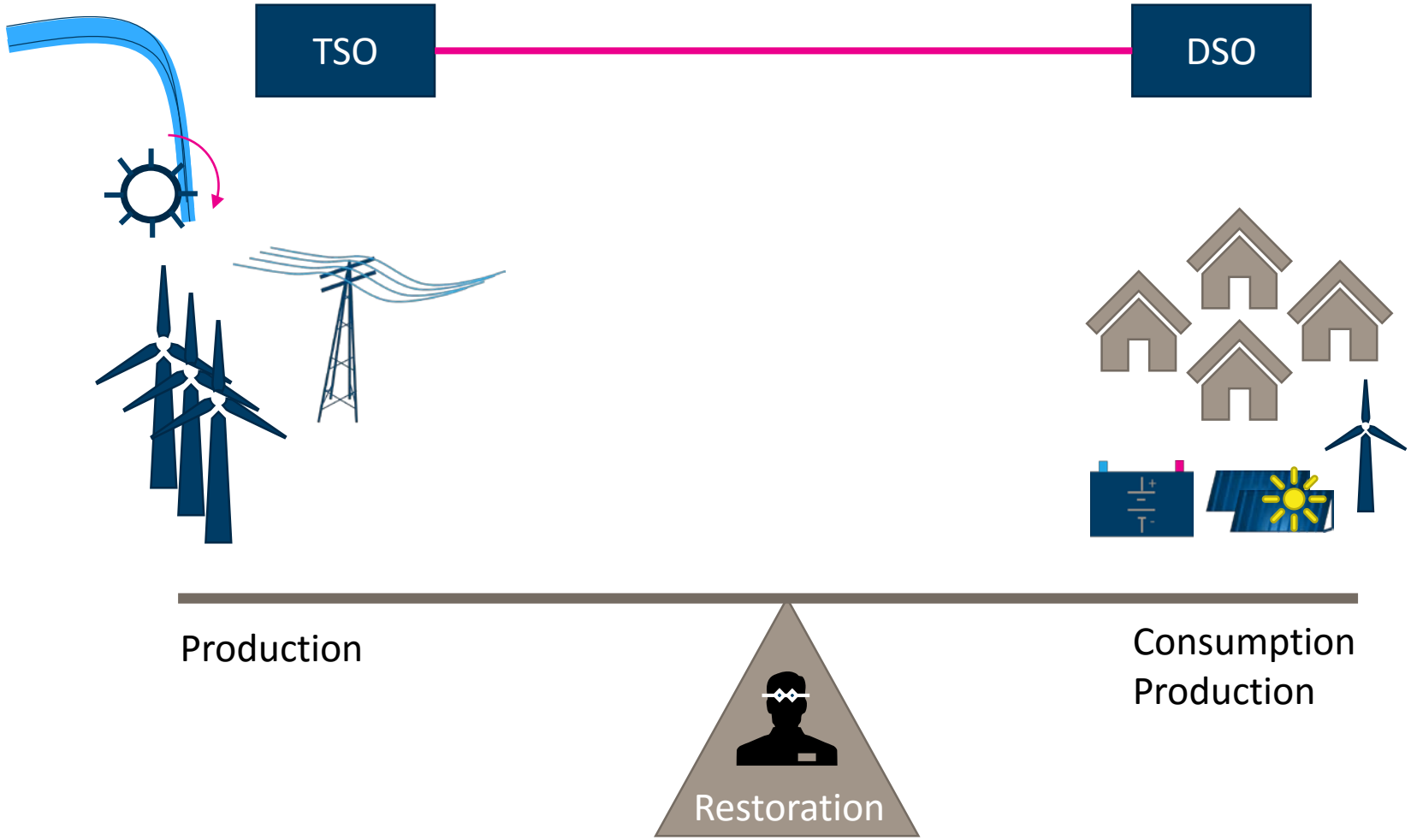
Flexibility in the TSO-DSO relation



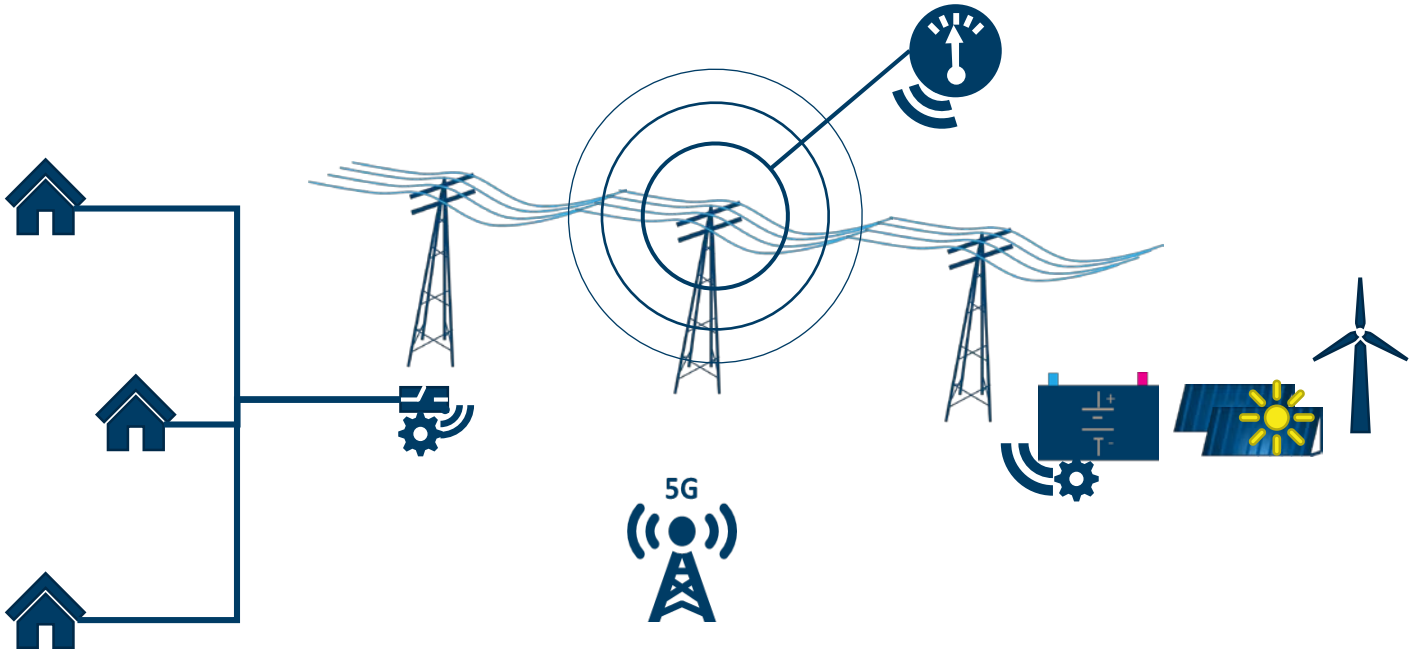
Flexibility in the TSO-DSO relation



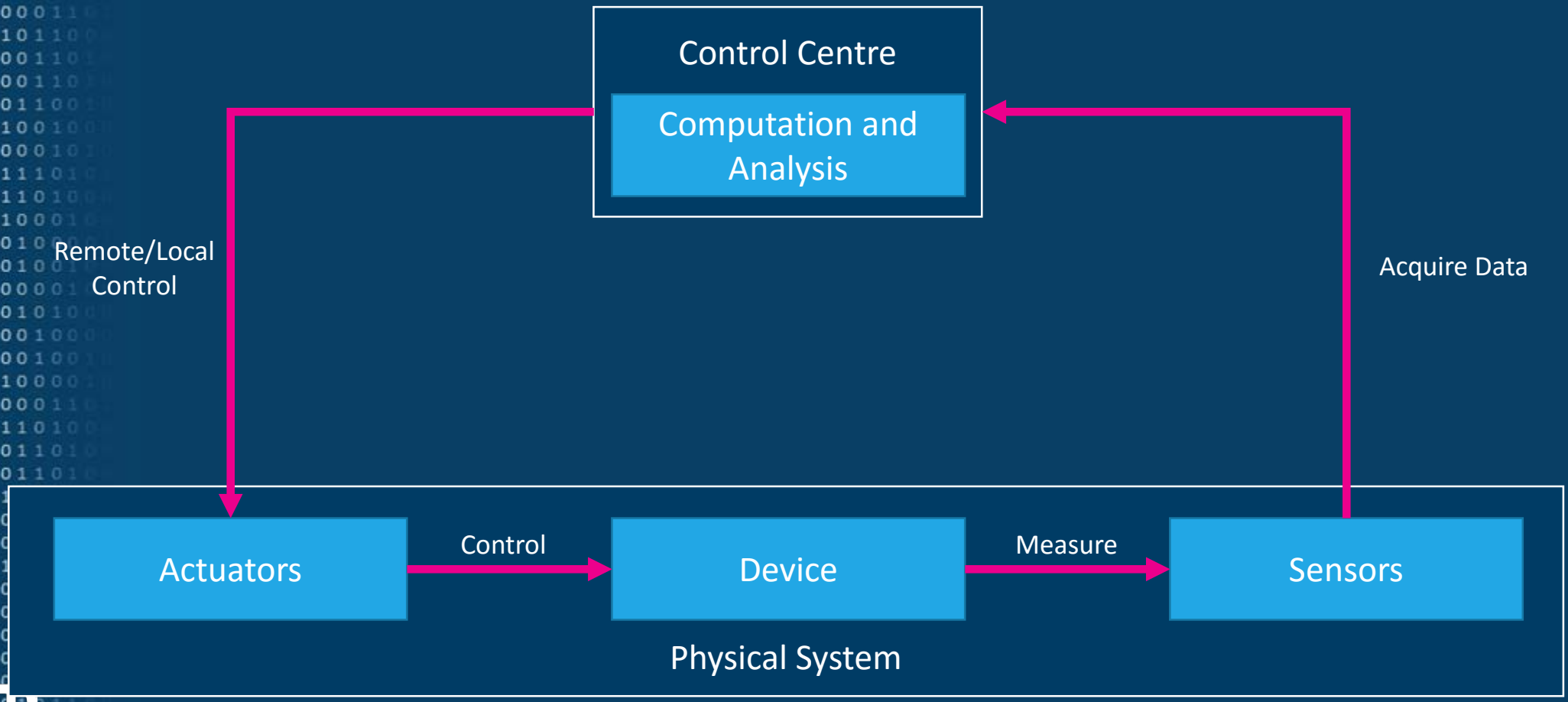
TSO/DSO – Restoration



Smart Grid Operations



Data flow


Control Centre
Computation and Analysis
Remote/Local Control
Acquire Data
Actuators
Control
Device
Measure
Sensors
Physical System

Misuse case: Injection of false measurement data

1. The attacker gains access to an unprotected substation
2. The attacker attaches a portable computer to the internal substation network, ensuring all communication has to go via this computer
3. The attacker will read all messages from sensors used for state estimation, and modify sensor values to systematically show lower values

Consequences

- Wrong data from enough of the sensors can result in wrong decisions that harm the power delivery.
- Economic consequences?

Misuse case: Malicious software update

1. A vendor uses a website to distribute software updates to its customers.
2. This website has vulnerabilities that allows an attacker to upload files
3. The attacker creates trojanized versions of several firmware updates to the vendor's equipment, and uploads these to the vendor website with the current date.

CINELDI

Misuse case: Malicious software update

4. The DSO update manager discovers that there are new updates available for the vendor's equipment, and downloads the trojanized updates (there is nothing to tell that the updated are malign)
5. The update process places malware in the DSO network, and also on the vendor's equipment
6. The attacker gets real-time access to the DSO network and the vendor's equipment in that network

CINELDI

Misuse case: Malicious software update Consequences

- If no propagation
  - local outages, increased manual workload and potentially the cost of replacing any affected equipment
- With propagation
  - potentially giving the threat actor control of the whole grid
- Both
  - fires, personnel injuries, components no longer fulfilling their purpose, and wrongful information being reported to the control centre

Misuse case: Malware in delivered equipment from vendor

Insider at supplier:

1. Insider is either extorted or have malicious intent
2. Insider installs backdoor/malware in equipment that allows remote access
3. Use backdoor to gain unauthorized access

Misuse case: Malware in delivered equipment from vendor

Test access functionality not removed:

1. Test account and/or debug ports not removed before equipment is delivered to DSO, by intent (insider) or neglect
2. Open backdoor into the system might be exploited to deliver malware, either by targeted attack or «drive by exploit»

Misuse case: Malware in delivered equipment from vendor

Equipment infected at the supplier:

1. Malware at the supplier (e.g. in test network) infects the equipment before it is delivered to the DSO
2. Malware not detected before the equipment gets installed at DSO

CINELDI

Misuse case: Malware in delivered equipment from vendor

Infected equipment moved from one facility to another:

1. Equipment (e.g. laptop used for software patching) gets infected with malware
2. When plugged into environment that is lacking virus detection (or advanced malware) the infection spreads

Misuse case: Malware in delivered equipment from vendor

Vendor that cannot be trusted:

1. The vendor implements a backdoor in the equipment on purpose (nation state sponsored attack)
2. Vendor might share information about how to access the backdoor with their allies

CINELDI

Consequences of malware delivered in equipment

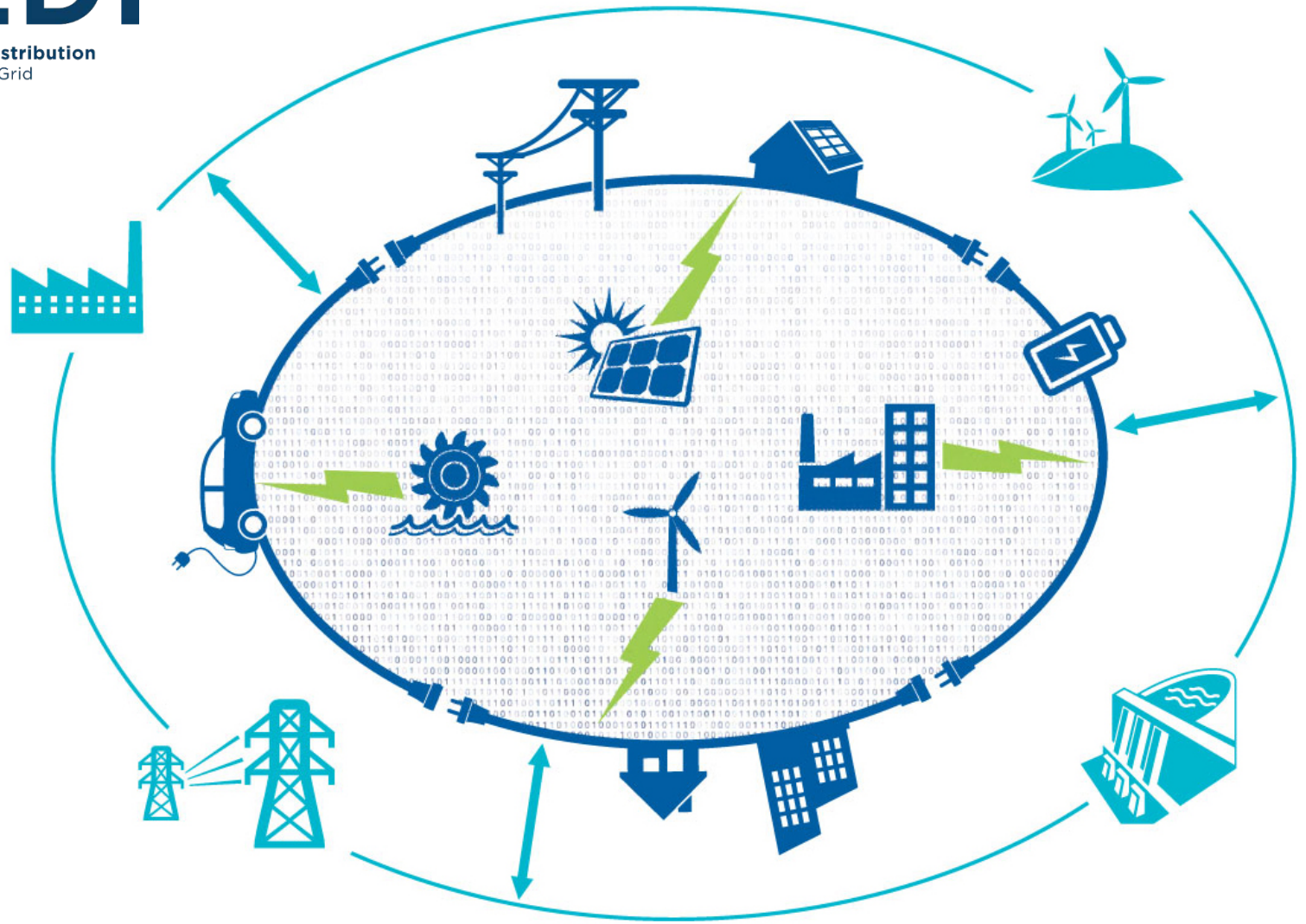
- Risks of unauthorized access to control systems, information gathering attacks or sabotage (targeted attacks)
- Malware might effect production, safety systems and even cause physical harm
- Non-targeted malware might cause unexpected network problems or equipment malfunction
- Vendor trust and reputation will be effected

Thank you!

Questions and feedback: marie.moe@sintef.no 

CINELDI

Centre for intelligent electricity distribution
- to empower the future Smart Grid



This work is funded by CINELDI - Centre for intelligent electricity distribution, an 8 year Research Centre under the FME-scheme (Centre for Environment-friendly Energy Research, 257626/E20). The authors gratefully acknowledge the financial support from the Research Council of Norway and the CINELDI partners.