Security Classification for Smart Grid

Manish Shrestha

Why Security Class?

- A secure device may not always mean a secure system
- Vulnerabilities are discovered all the time
- We cannot protect our systems from all threats which we do not know about
- Need to redefine the design of the network based on security classes

Security Classes

- Instead of looking after the attacks, we rather propose to group our security model or system after security priorities

ANSSI Security Classification for ICS Parameters

- Impact (Insignificant, Minor, Moderate, Major, Catastrophic)
- Likelihood
- Attackers (Non-targeted, Hobbist, Isolated, Private Organizations, State Organizations)
- Users/Accessibilities
- Connectivity
- Functionalities
- Exposure

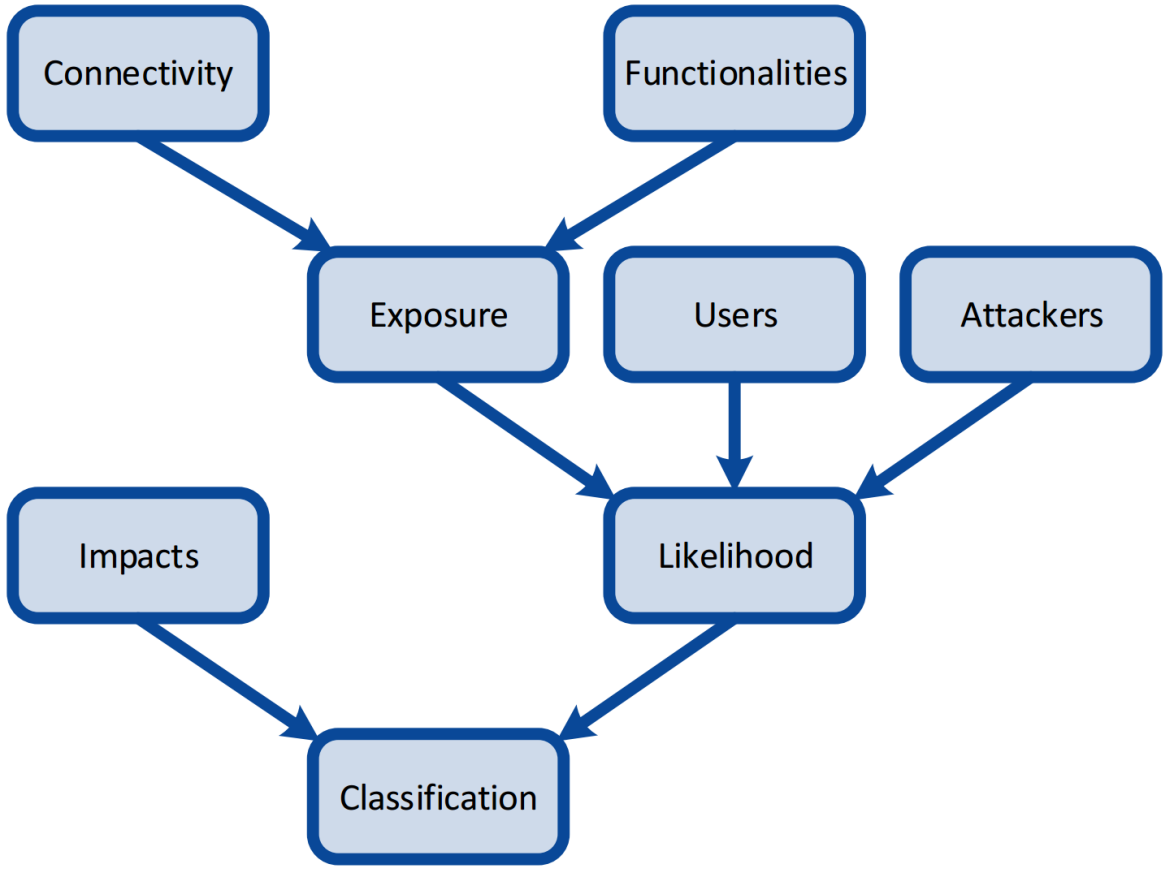
Connectivity

- **Connectivity 1 (C1)**: includes completely closed isolated ICS.
- **Connectivity 2 (C2)**: includes ICS connected to an corporate network but does not permit any operations from outside the network.
- **Connectivity 3 (C3)**: includes the all ICSs using wireless technology
- **Connectivity 4 (C4)**: includes the ICS with private infrastructure which may permit operations from outside(VPN, APN, etc.)
- **Connectivity 5 (C5)**: includes Distributed ICS with public infrastructure.

Functionalities

- **Functionality 1 (Minimal Systems)** It includes the system which has components limited to devices like sensors,PLCs, HMIs, embeded systems
- **Functionality 2 (Complex Systems)**: : It includes ICSs which have functionality 1 components and SCADA systems but excluding programming consoles and engineering workstations.
- **Functionality 3 (Very Complex Systems)**: This includes all other ICS that do not fall into the Functionality 1 and Functionality 2 category

ANSSI Security Classification for ICS

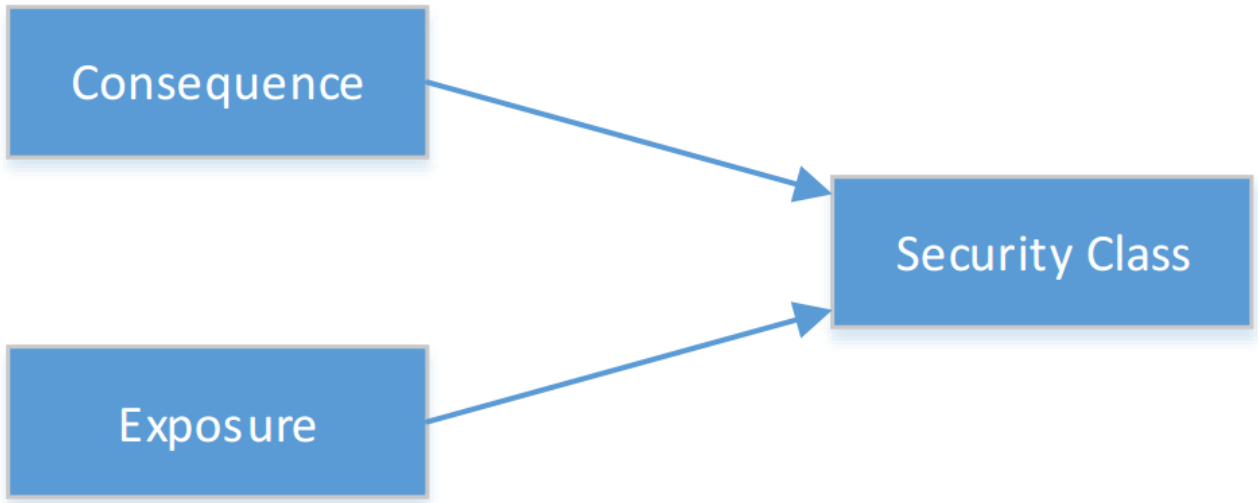


Class

5+	Class 2	Class 2	Class 3	Class 3
4	Class 2	Class 2	Class 2	Class 3
3	Class 1	Class 2	Class 2	Class 2
2	Class 1	Class 1	Class 2	Class 2
1	Class 1	Class 1	Class 1	Class 1
Impact/Likelihood	1	2	3	4+

New Security Class

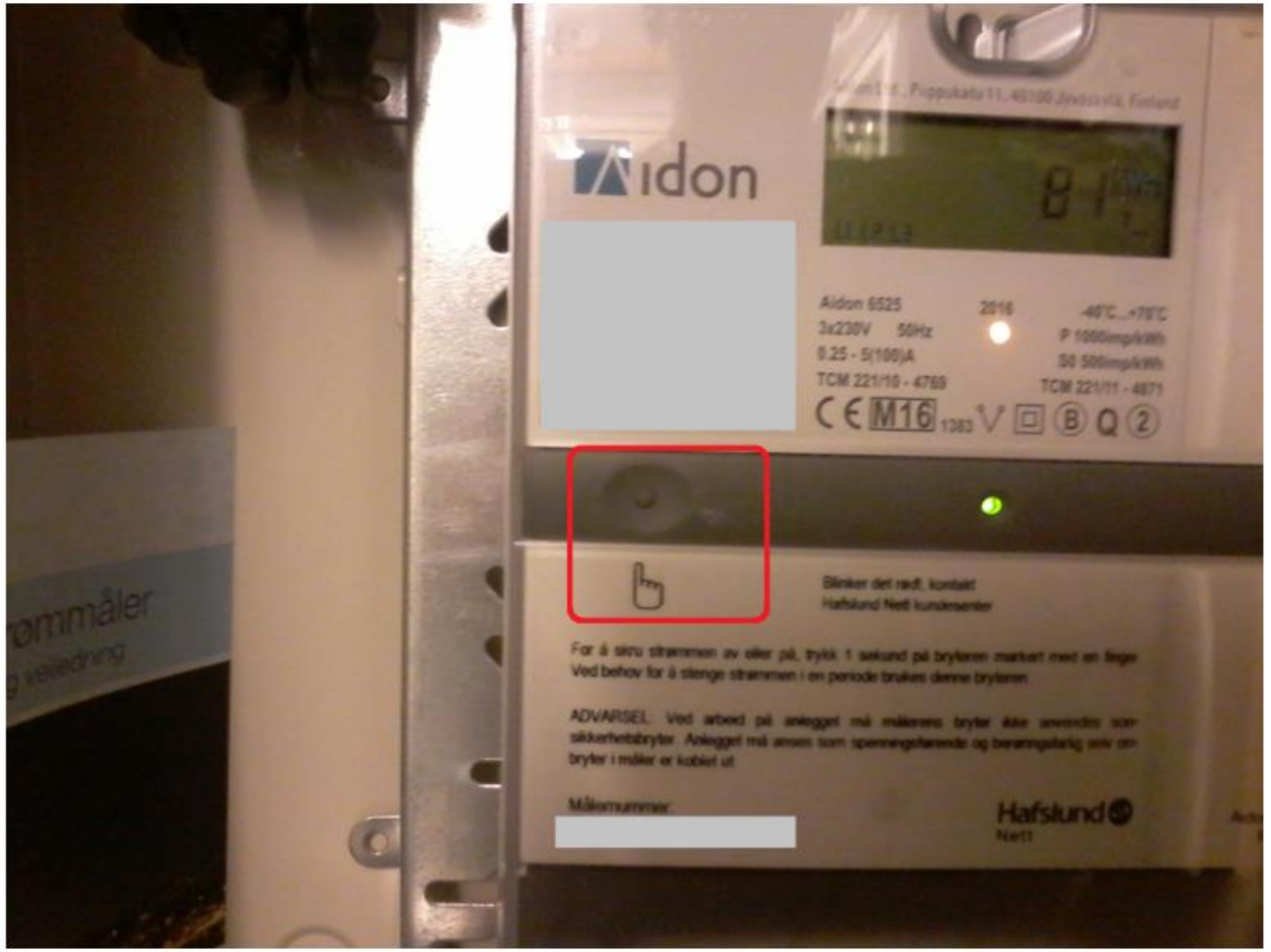
- Security class is the result of consequence of attack on a given system and the exposure



Exposure(Level 1-5)

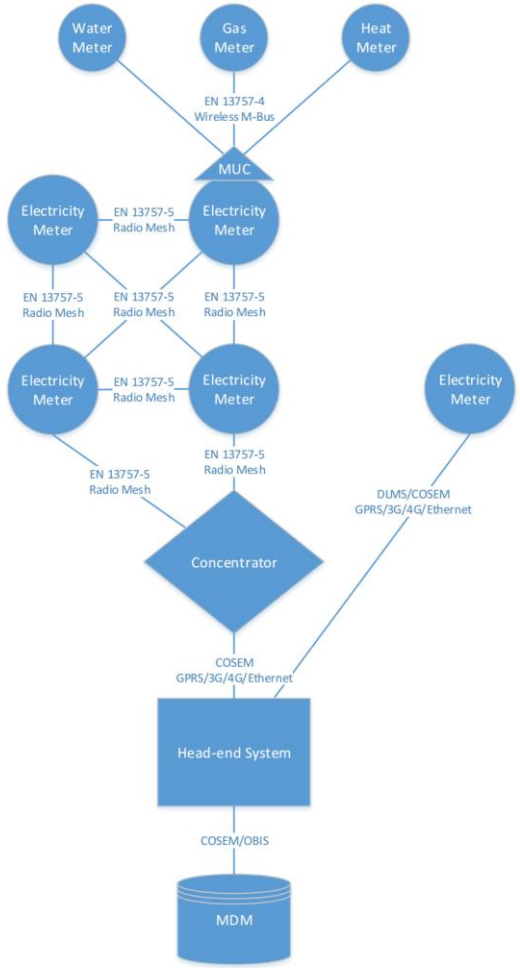
- Physical Exposure
  - People (e.g. dishonest employees)
  - Building
  - Located in public area
  - Home
  - Physical ports

- IT Exposure
  - Ports
  - Firewalls
  - Connectivity
  - Configuration
  - Complexity
  - People (e.g., phishing)...



Mapping Security Class with AMI

- Impact (High, i.e., 4): kile kost, industries, end users
- Exposure (4):
  - Connectivity level 4
  - physical (people, home, public)
  - IT



5	Class 5	Class 5	Class 5	Class 5
4	Class 4	Class 4	Class 4	Class 5
3	Class 3	Class 4	Class 4	Class 4
2	Class 1	Class 3	Class 3	Class 3
1	Class 1	Class 1	Class 2	Class 2
Impact/Exposure	1	2	3	4+

Next Steps

- Redefine exposure
- Map security classes with security functionalities