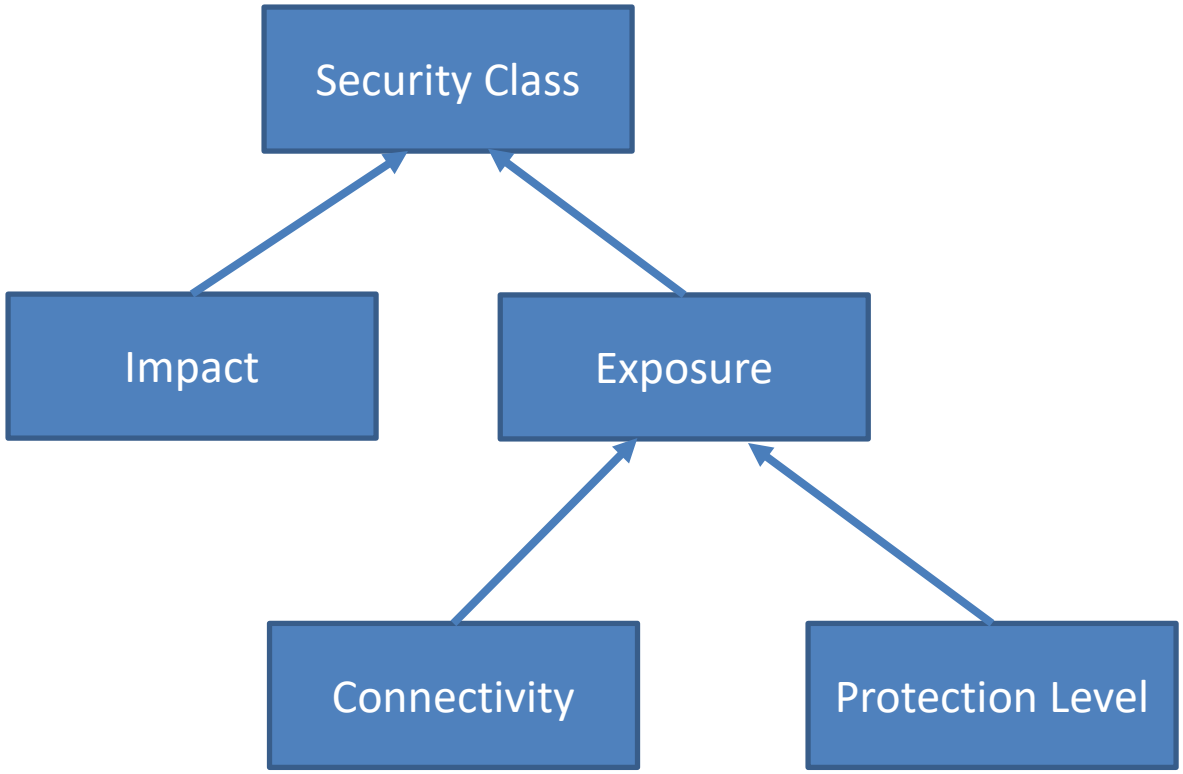
Towards Assurance in Security Classes

Manish Shrestha
Christian Johansen
Josef Noll
Department of Mathematics and Natural Science
University of Oslo

May 15, 2019

Our security class is based on ANSSI classification



Connectivity and Protection Level gives Exposure

P1	E4	E4	E5	E5	E5
P2	E3	E4	E4	E5	E5
P3	E2	E3	E3	E4	E4
P4	E1	E1	E2	E2	E3
P5	E1	E1	E1	E1	E2
Protection/ Connectivity	C1	C2	C3	C4	C5

Impact and Exposure gives Security Class

Catastrophic	A	C	E	F	F
Major	A	B	D	E	F
Moderate	A	B	C	E	E
Minor	A	A	B	D	D
Insignificant	A	A	A	C	C
Impact/ Exposure	E1	E2	E3	E4	E5

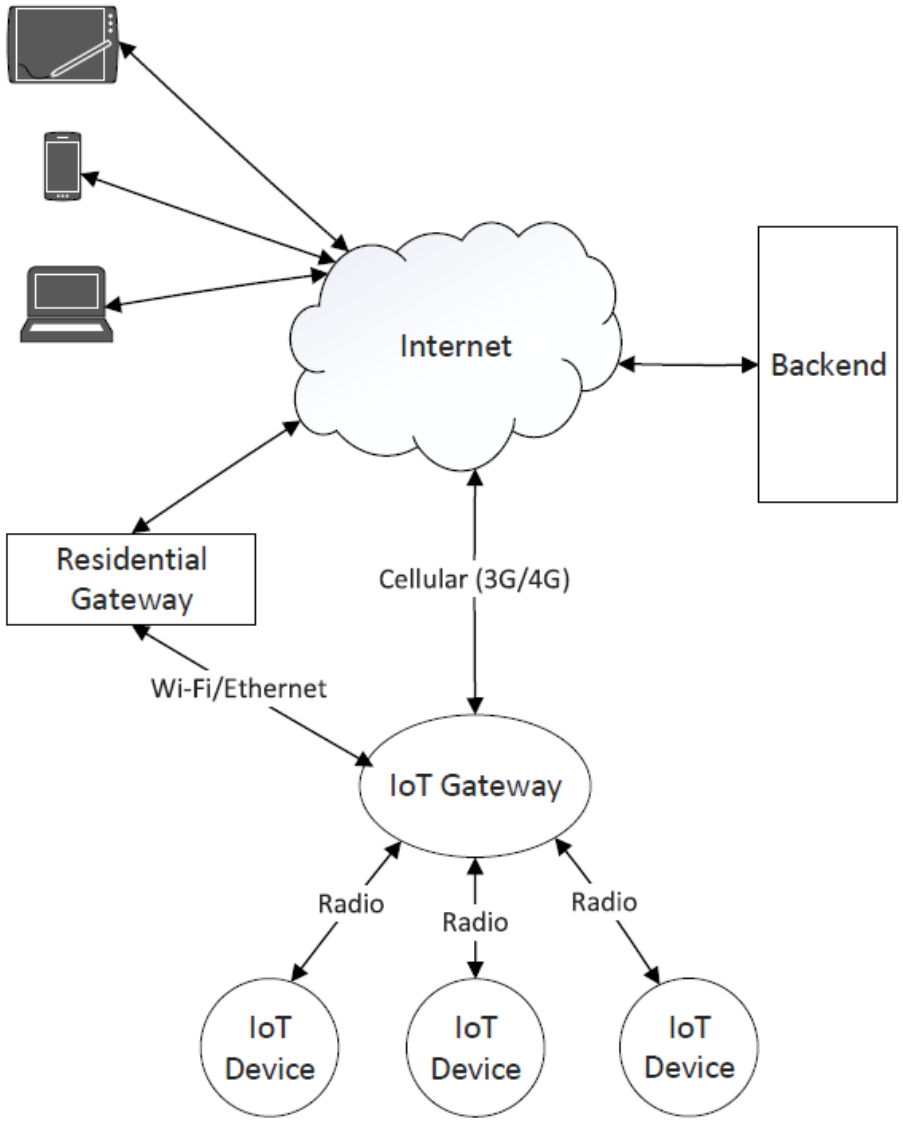
Security Classification in Smart Home Energy Management Systems (SHEMS)

SHEMS Components

- IoT hub
- IoT Devices
- Residential Gateway
- Communication Channels
- Backend System
- Application and Network Data
  - Sensor readings
  - Control Signals
  - …

Impacts

- Safety
- Increased Electricity Bills
- Grid Imbalance
- Agents for other cyberattacks
- Privacy



Protection Criteria are extracted from available standards and guidelines

Protection Criteria	Source
Data Encryption	ISO 27002, OWASP, ETSI
Communication and Connectivity Protection	IIC, ISO 27002, ETSI
Software/Firmware Security	ISO 27002, OWASP, ETSI
Hardware-based Security Controls	CSA
Access Control	ISO 27002, OWASP, IIC, CSA, ETSI
Cryptographic Techniques	IIC, ISO 27002
Physical and Environmental Security	ISO 27002, OWASP, CSAs
Monitoring and Analysis	ISO 27002, OWASP, IIC, CSA, ETSI

Defining protection levels based on security functionalities

Protection Criteria	Security Functionality	P5	P4	P3	P2
Data Encryption	Encryption of data between system components	x	x	x	x
	Strong encryption mechanism	x	x	x	
	Credentials should not be exposed in the network	x	x	x	
	End-to-end encryption	x	x		
	Should not use custom encryption algorithms	x	x		
	Sensitive stored data should be encrypted	x	x		
Communication and Connectivity Protection	Have a minimal number of network ports open	x	x	x	
	Devices should not be accessible from the Internet	x	x	x	
	Only authorized components can join the network	x	x	x	
	Use only standard communication protocol	x	x		
Software /Firmware Security	Updatability of device firmware	x	x		
	Updatability of the operating system	x	x		
	Automatic updates available	x	x		
	Encryption of update files	x	x		
	Signing update files before installing	x	x		
Hardware-based Security Controls	Using Trusted Platform Modules (TPM)	x	x		
	Use of Memory Protection Units (MPUs)	x	x		
	Incorporate Physically Unclonable Functions (PUFs)	x	x		
	Use of Cryptographic Modules	x	x		
Access Control	Disable remote access functionality	x			
	Only authorized devices can join the network	x	x	x	
	Default and weak passwords should not be used	x	x	x	
Cryptography Techniques	Secure bootstrapping	x	x		
	Secure key generation	x	x		
	Secure key storage	x	x		
	Secure key distribution	x	x	x	
	Secure key rotation	x	x		
	Message integrity	x	x	x	
Physical and Environmental Protection	Tamper resistance	x	x		
	Minimal physical ports available	x	x	x	
	Physical security of connections	x	x	x	
	Ability to disable external ports and only minimal-ports enabled	x	x		
	Only authorized physical access	x	x	x	
Monitoring and Analysis	Monitoring system components	x	x		
	Analysis of monitored data	x	x		
	Act on analyzed data	x			

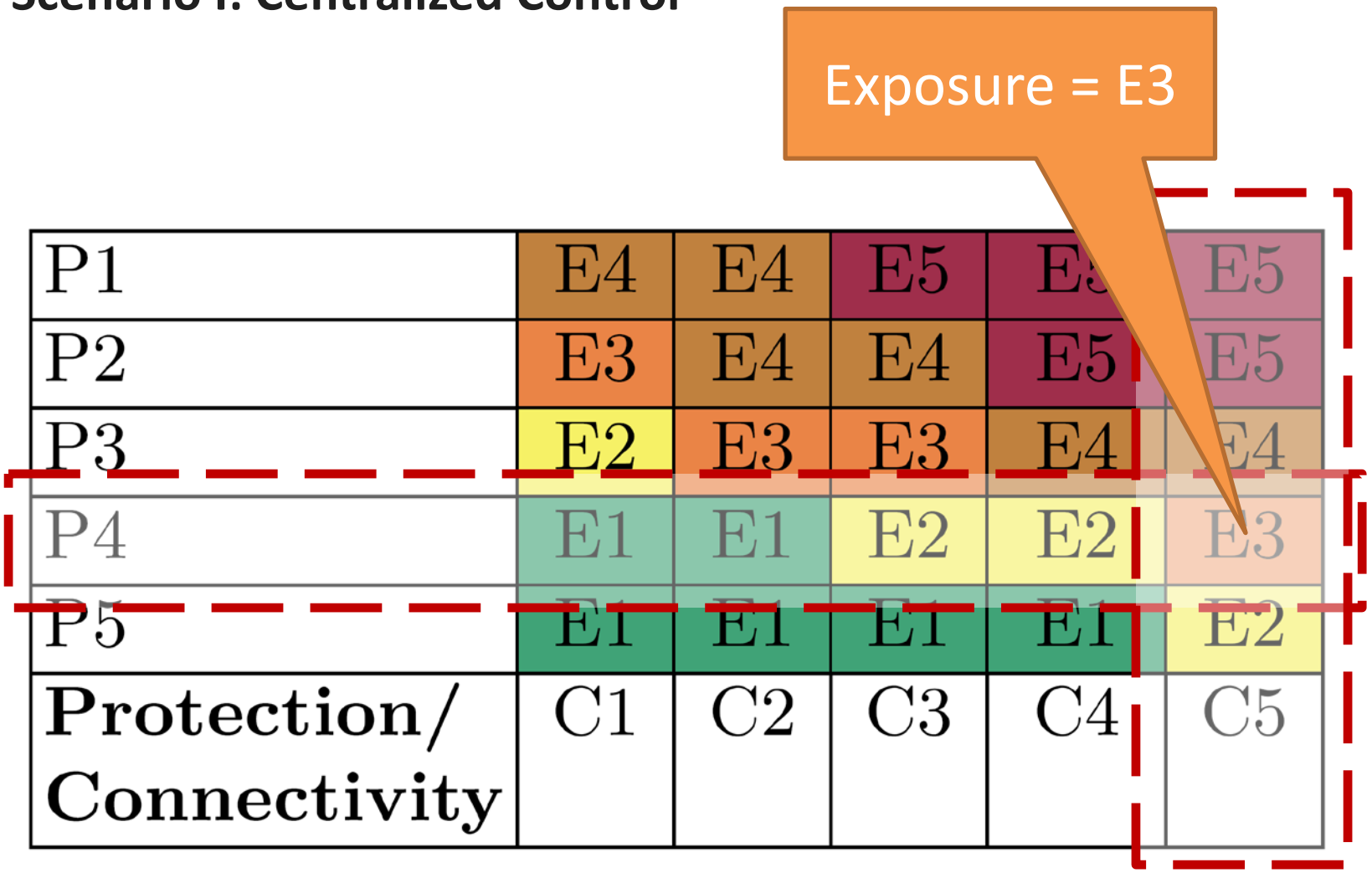
IoTSF also propose checklist based approach in their compliance framework

Control Signals are used to reduce demand during peak hours

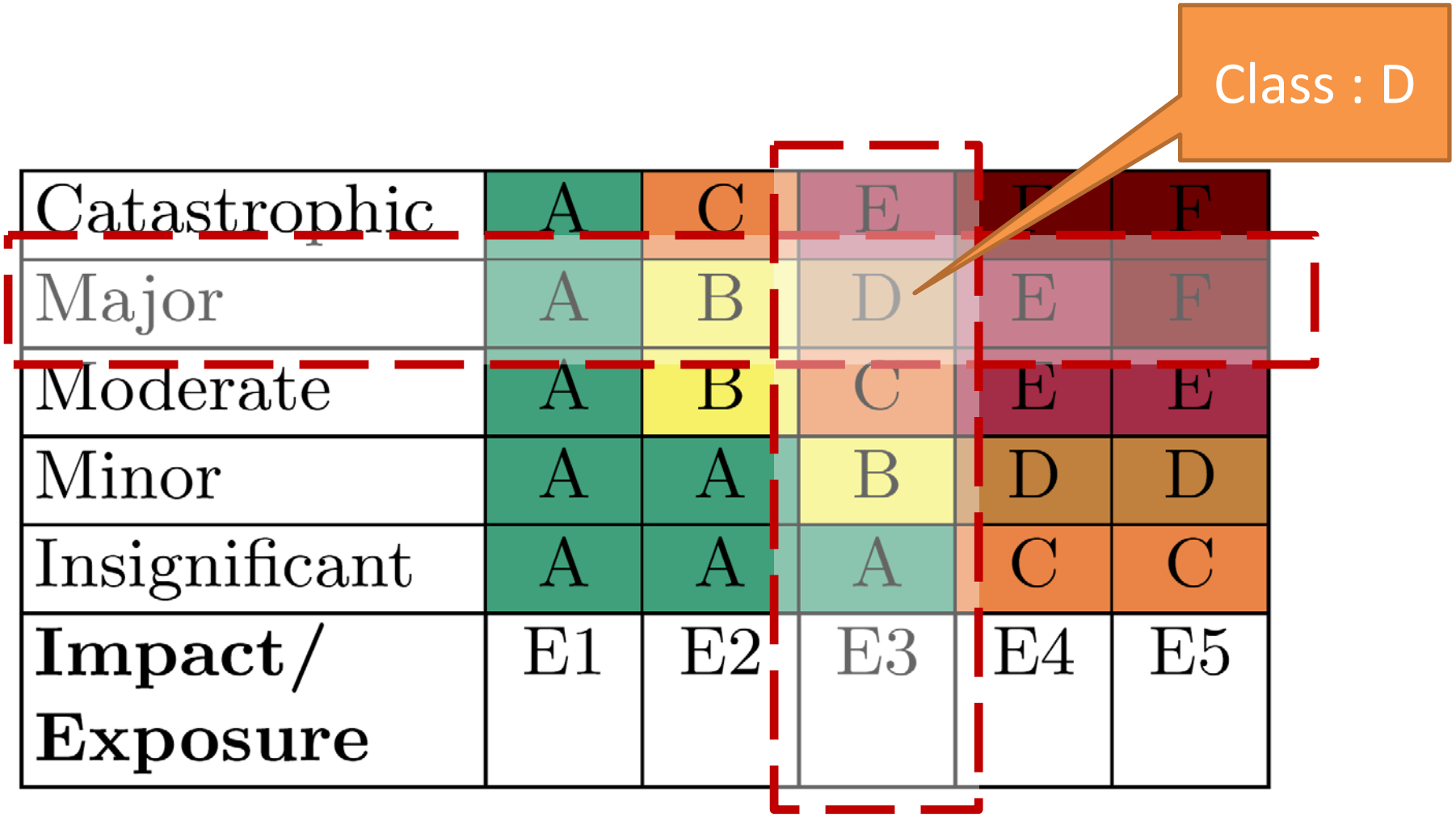
- **SHEMS may consists of smart plugs and batteries**
- **Selected devices should be turned off during peak hours**
- **Currently, devices are centrally controlled**

Scenario I: Centralized Control

Scenario I: Centralized Control

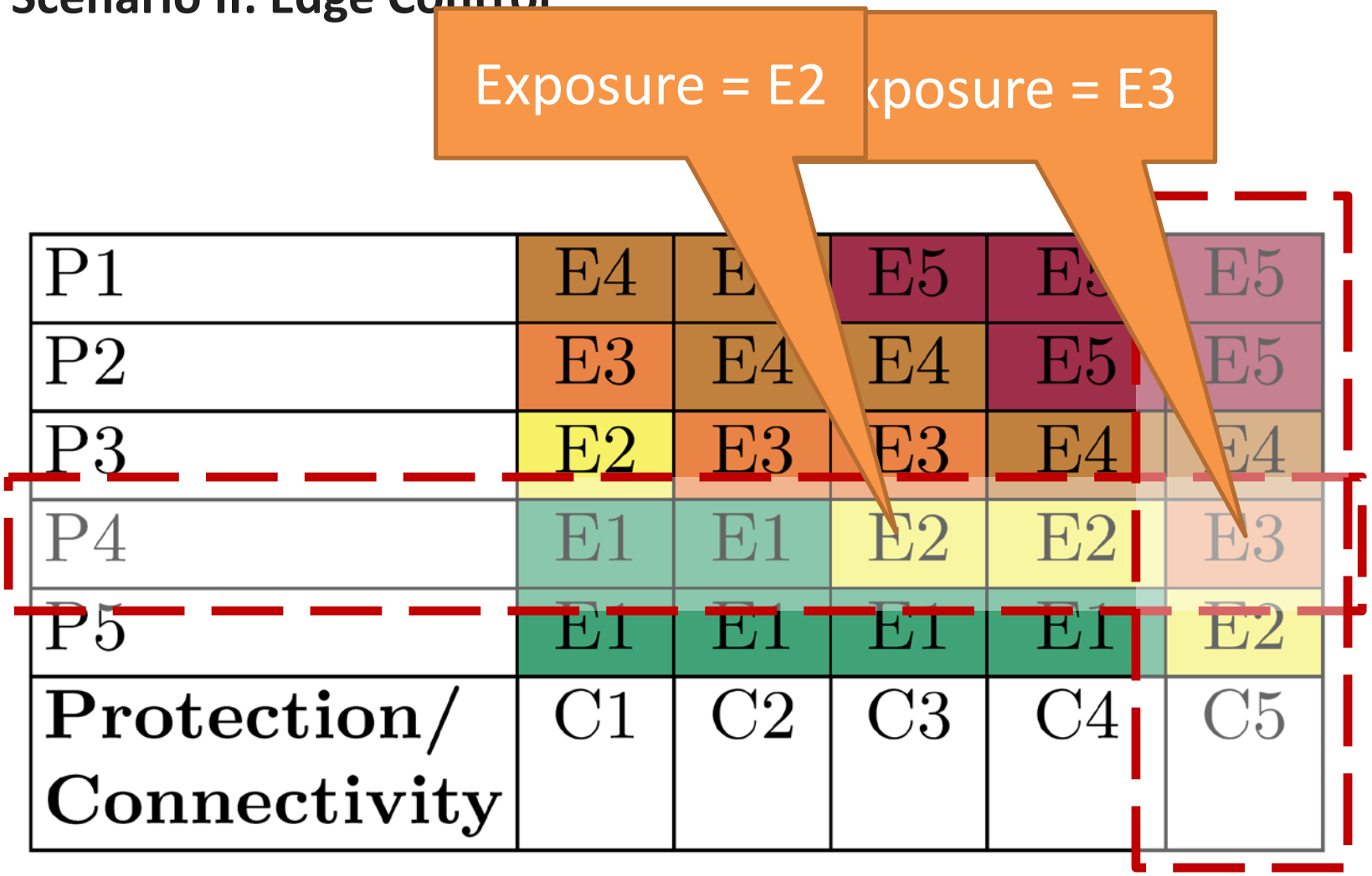


Scenario I: Centralized Control

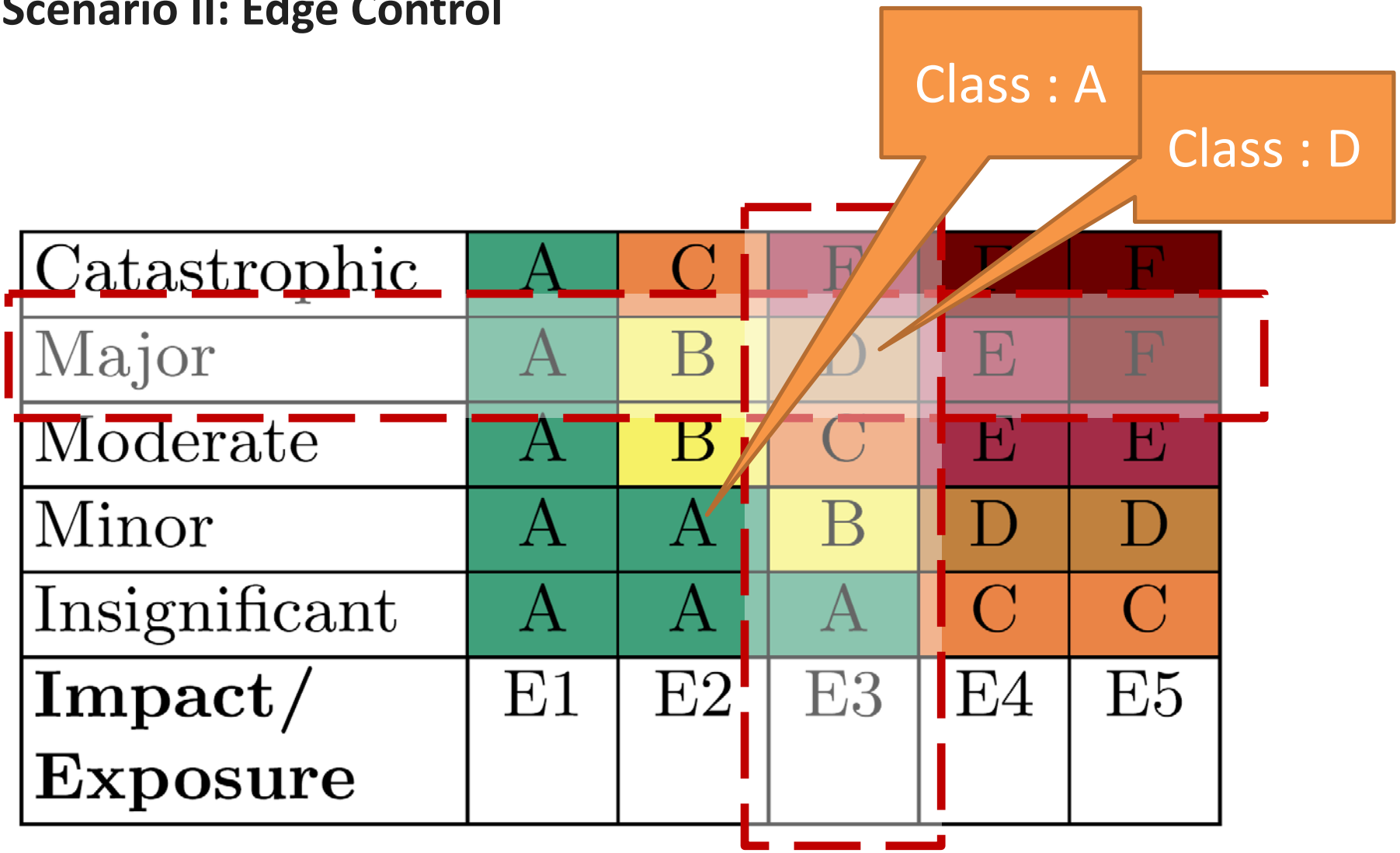


Scenario II: Edge Control

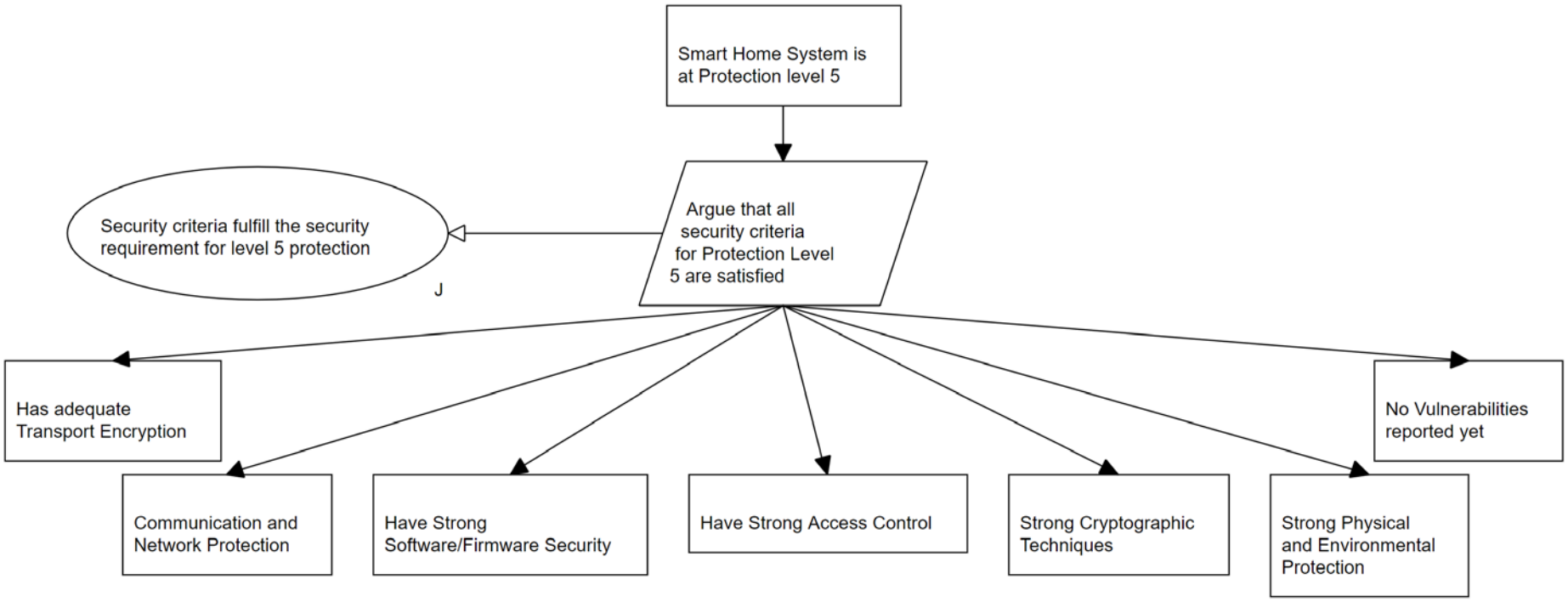
Scenario II: Edge Control



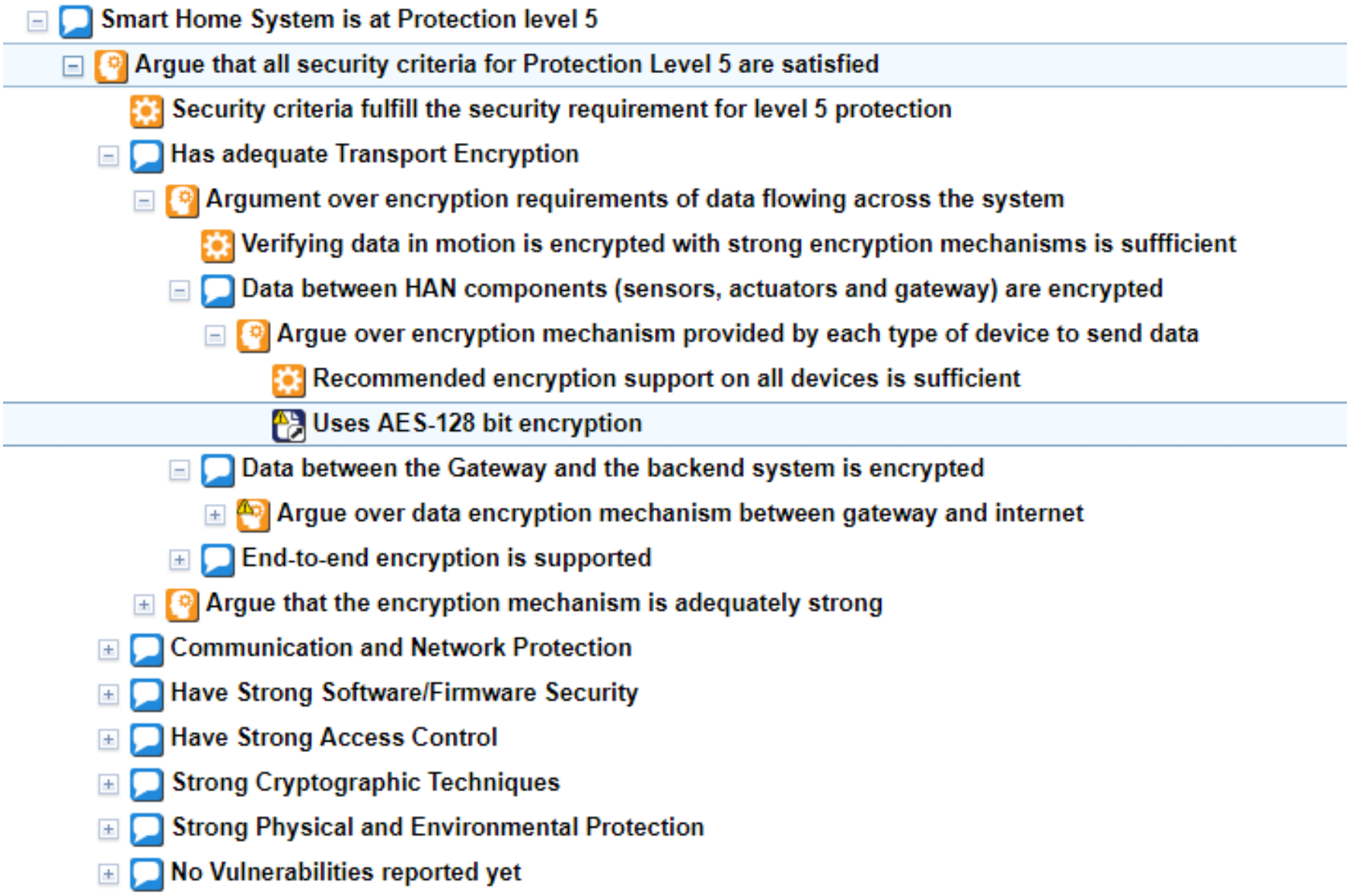
Scenario II: Edge Control



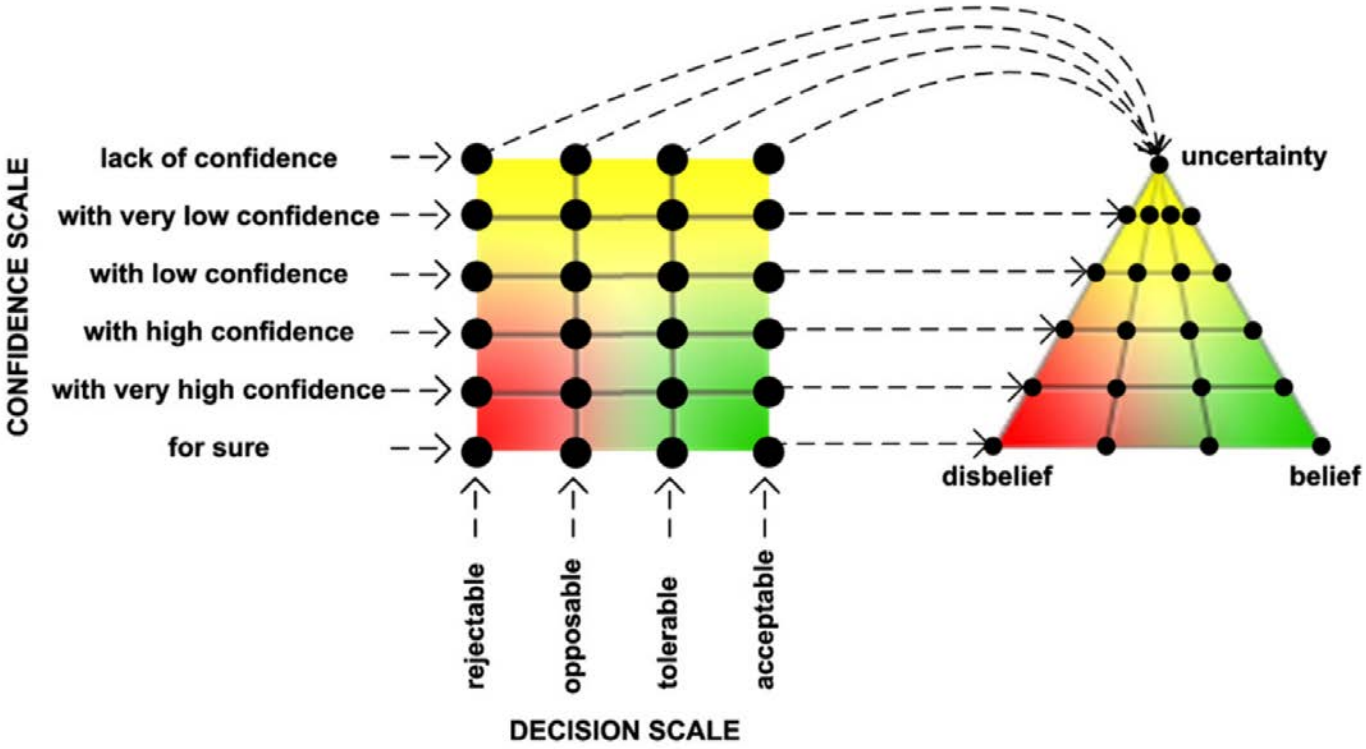
Security requirements for protection levels can be refined and evaluated finding adequate arguments with adequate evidence



NOR-STA tool can be used for templating protection level requirements



The Assessment Triangle



Future works

- **Multi-metrics and belief in Security Classes**
- **(Semi-)Automation of security class evaluation**

Questions?