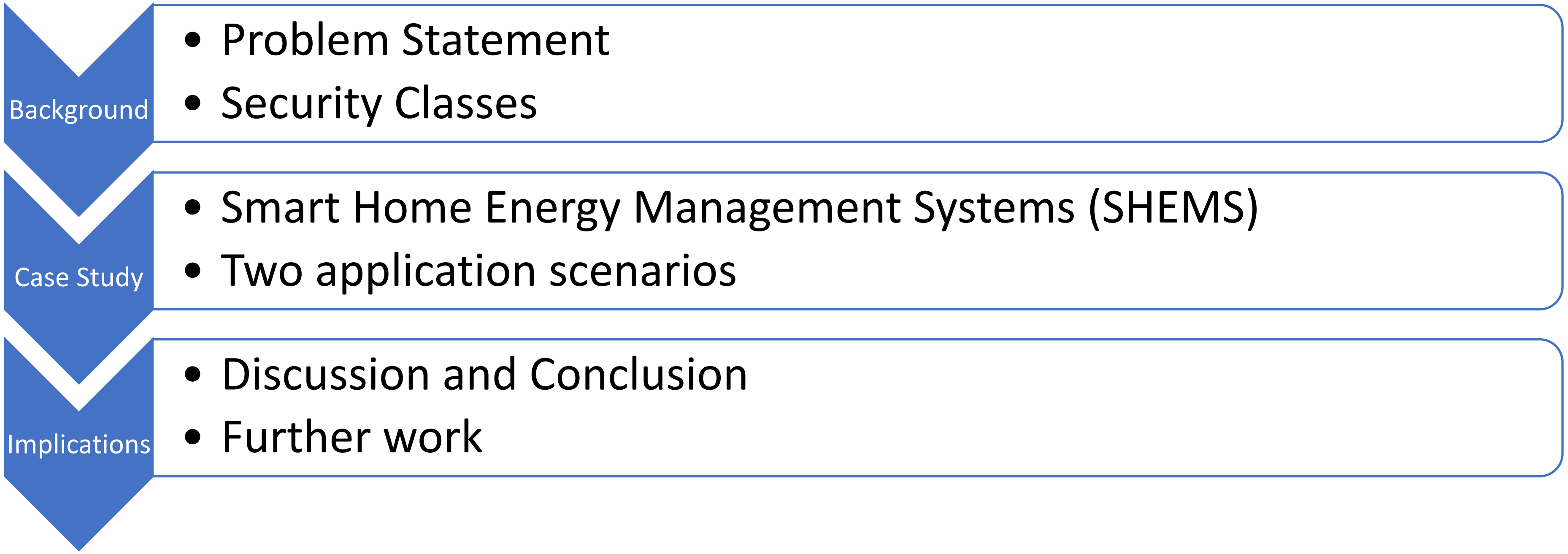
Criteria for Security Classification of Smart Home Energy Management Systems

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

This talk is about applying Security Classification to Smart Home Energy Management Systems



Background

- Problem Statement
- Security Classes

Case Study

- Smart Home Energy Management Systems (SHEMS)
- Two application scenarios

Implications

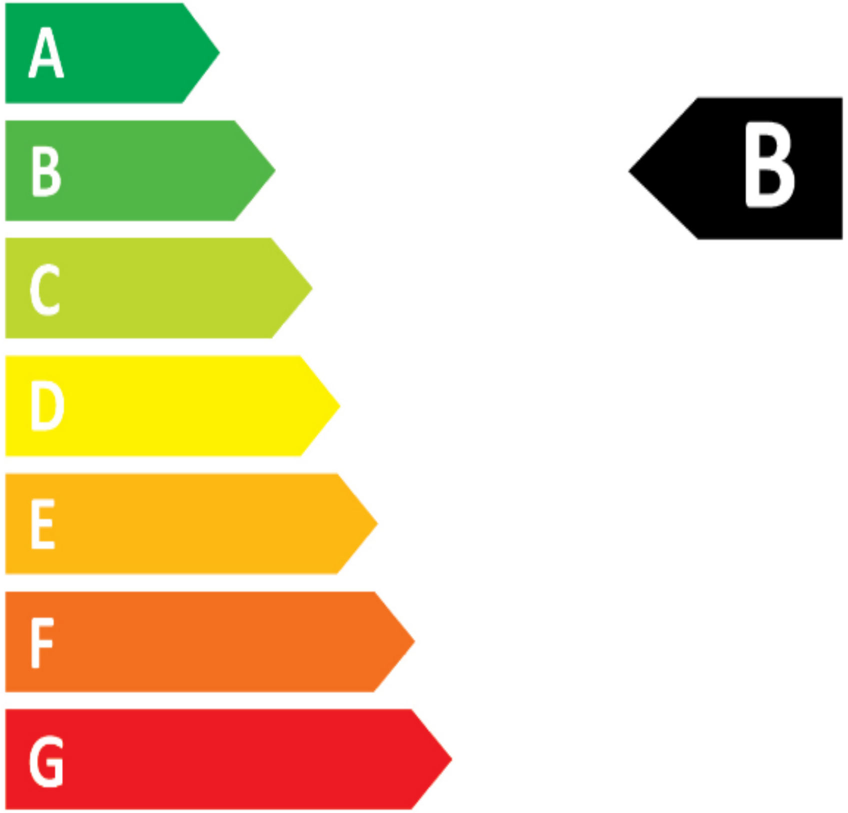
- Discussion and Conclusion
- Further work

Standards and Certifications existing today do not adapt well with changing IoT world

Common Criteria

ISO

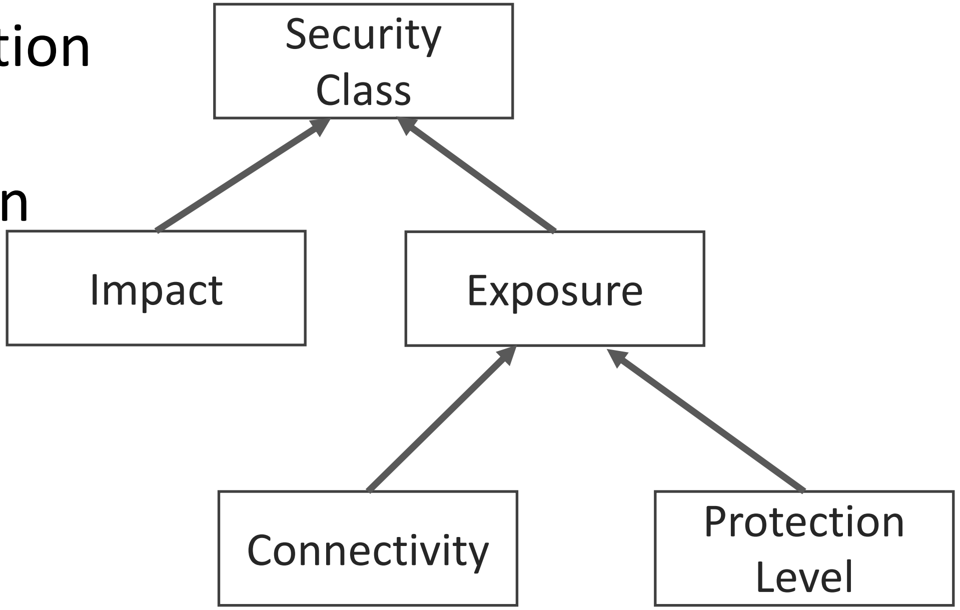
enisa

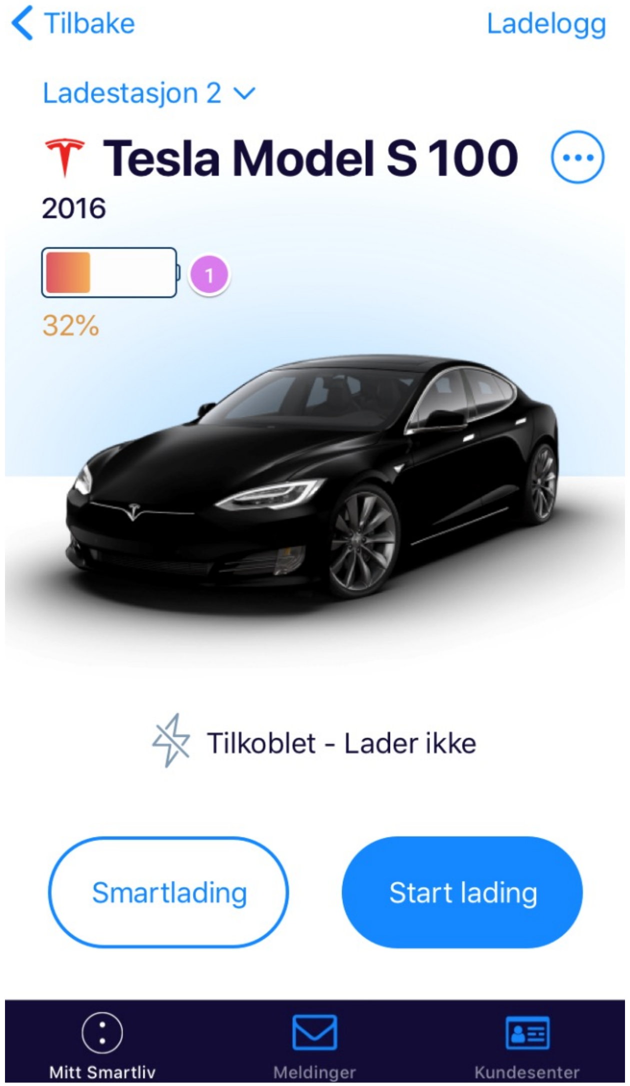


Security Class

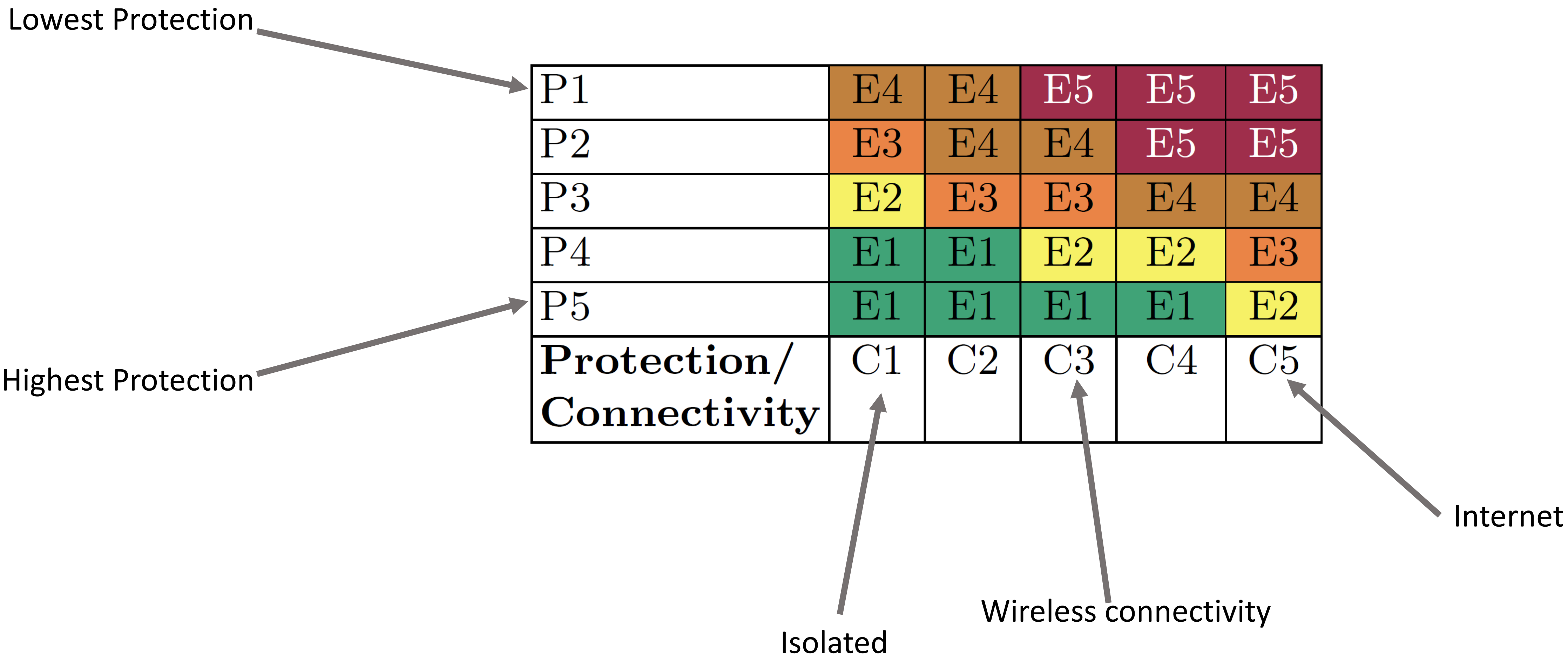
Our Security Classification Methodology

- Based on ANSSI classification
- System decomposition
- Impact evaluation
- Exposure evaluation





Exposure is calculated from Connectivity and Protection Level



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

Lowest Protection

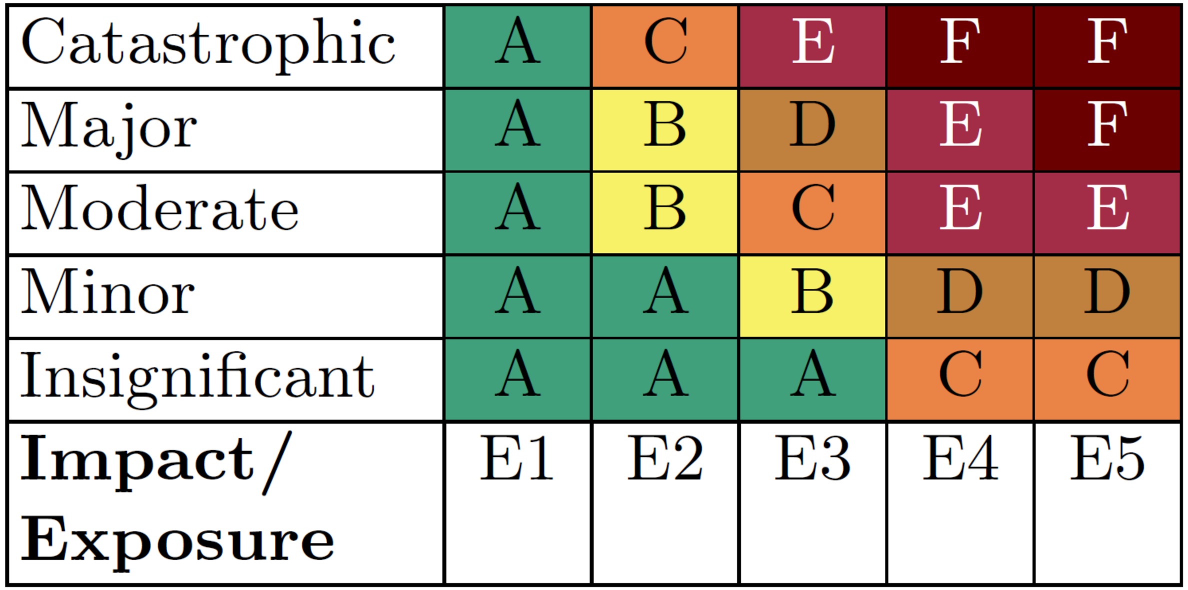
Highest Protection

Isolated

Wireless connectivity

Internet

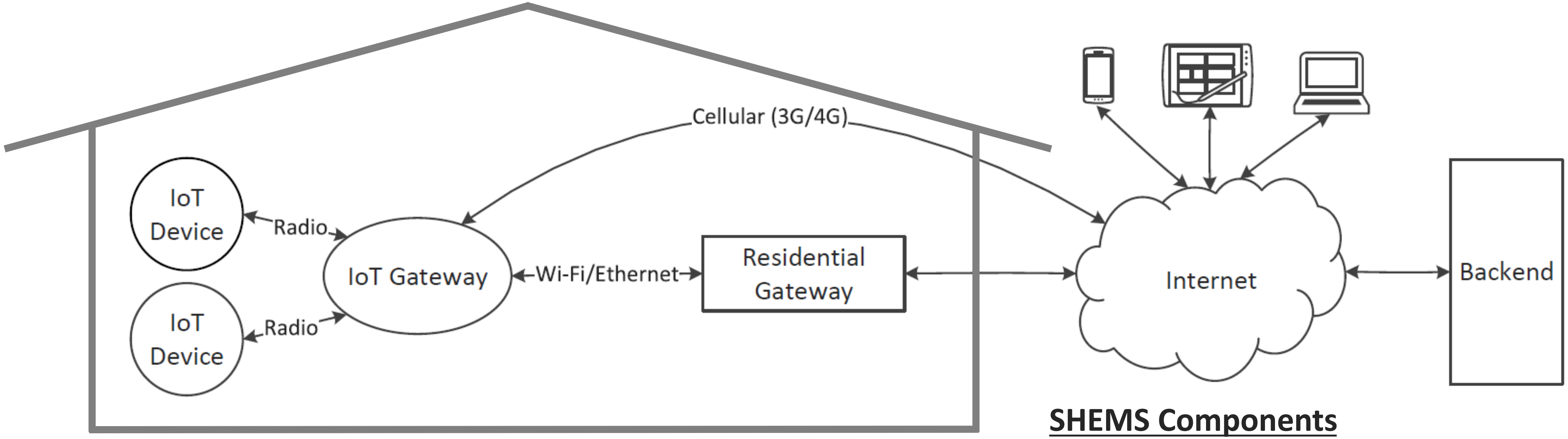
Impact and Exposure gives Security Class



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

Put some examples to pop up

A commercial Smart Home Energy Management Systems (SHEMS) from e2U Systems



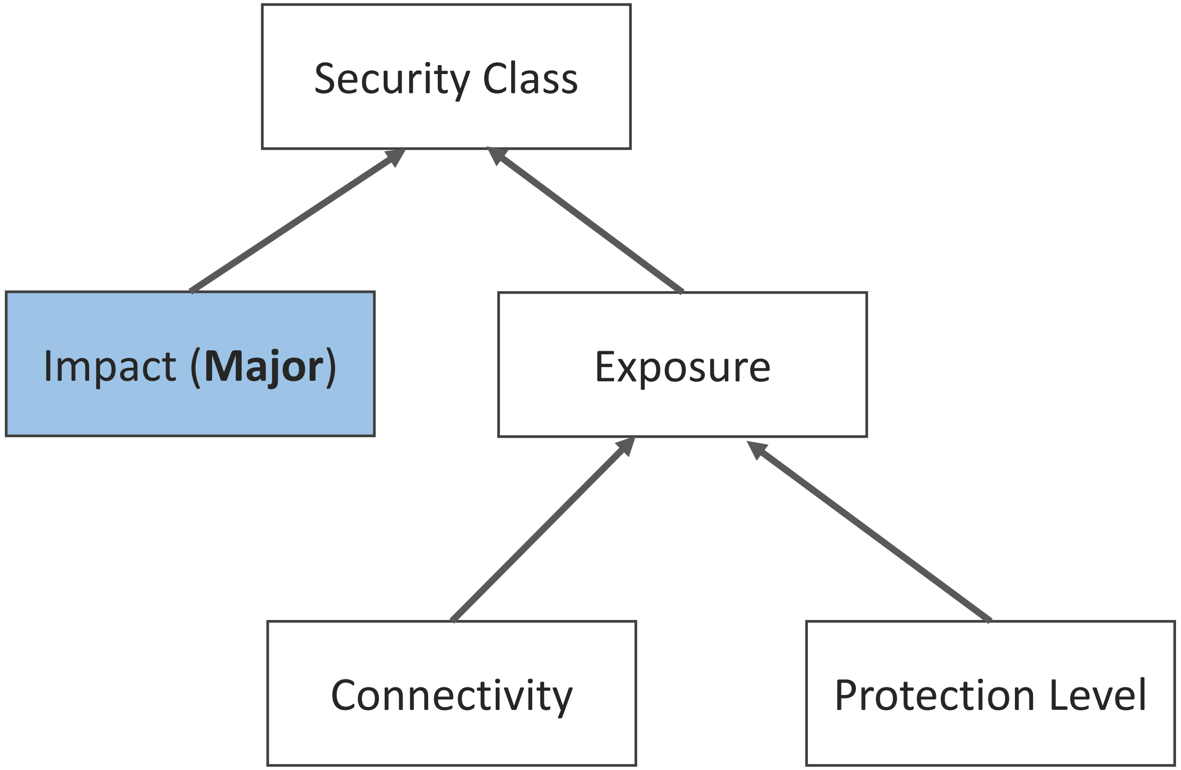
SHEMS Components

- **IoT hub (IoT Gateway)**
- **IoT Devices**
- **Residential Gateway**
- **Communication Channels**
- **Backend System**
- **Application and Network Data**
  - Sensor readings
  - Control Signals
  - ...

[1] Ghirardello, K., Maple, C., Ng, D., Kearney, P.: Cyber security of smart homes:Development of a reference architecture for attack surface analysis (2018)

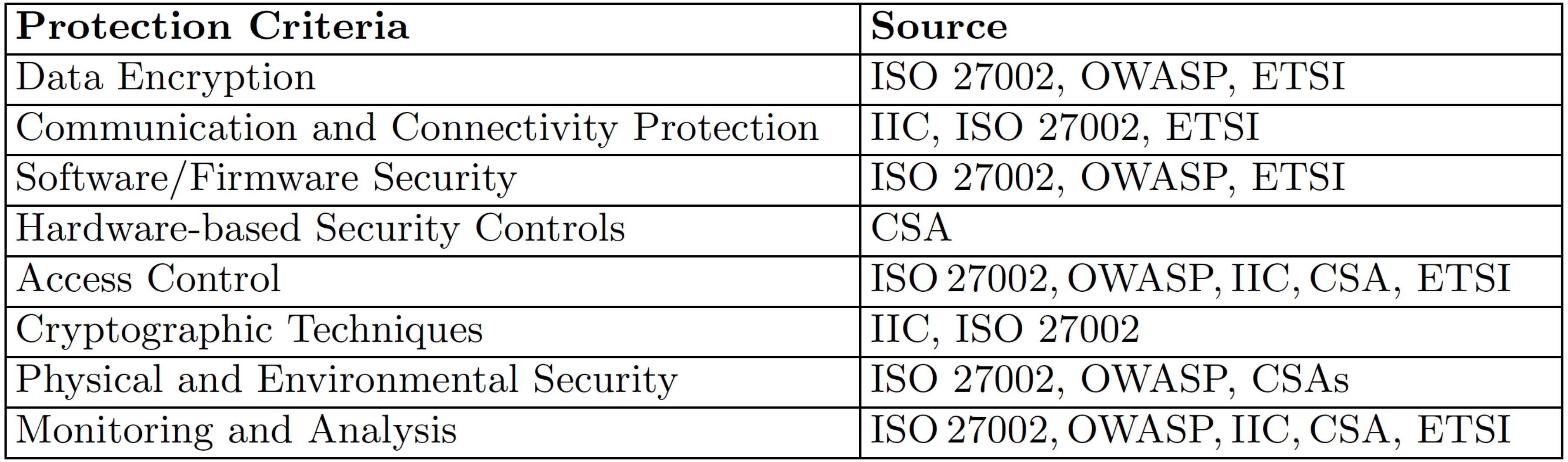
Impacts

- Safety
- Increased Electricity Bills
- Grid Stability [2]
- Agents for other cyberattacks
- Privacy



[2] Soltan, S., Mittal, P., Poor, H.V.: Blackiot: Iot botnet of high wattage devices can disrupt the power grid, 2018

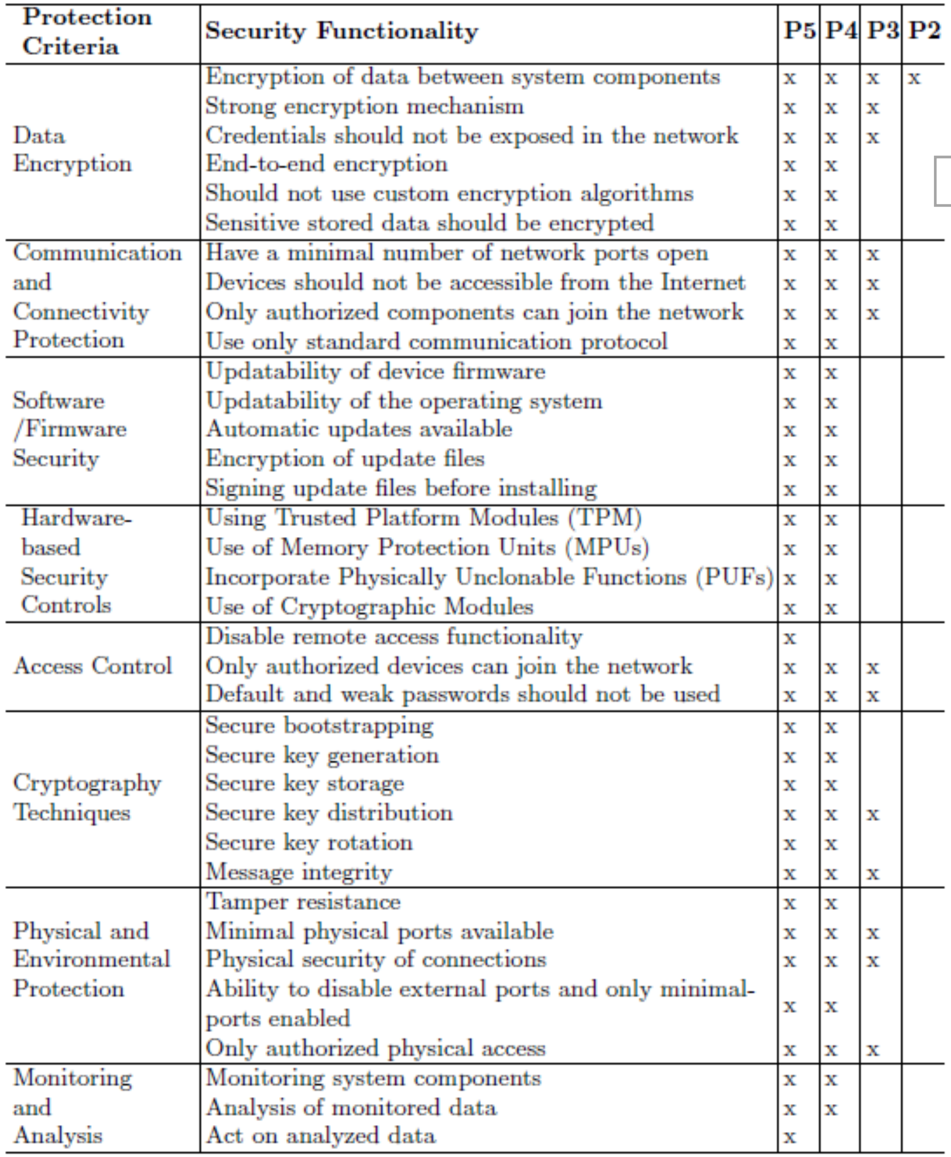
Protection Criteria are extracted from available standards and guidelines



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

- **Talk abouto iso, owasp what they are and short description**

Defining protection levels based on security functionalities

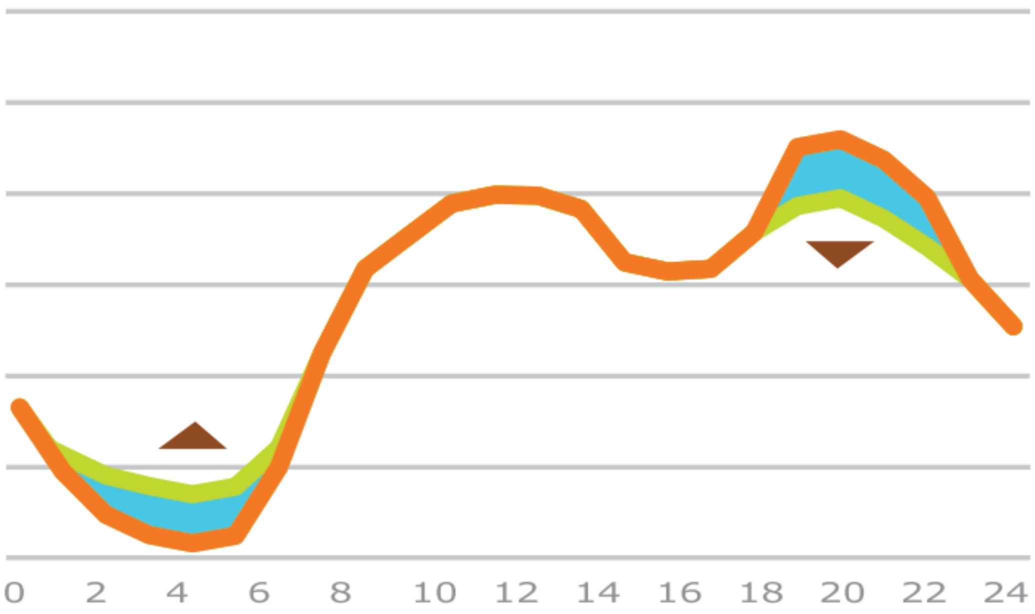


Protection Criteria	Security Functionality	P5	P4	P3	P2
Data Encryption	Encryption of data between system components	x	x	x	x
	Strong encryption mechanism	x	x	x	
	Credentials should not be exposed in the network	x	x	x	
	End-to-end encryption	x	x		
	Should not use custom encryption algorithms	x	x		
	Sensitive 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			

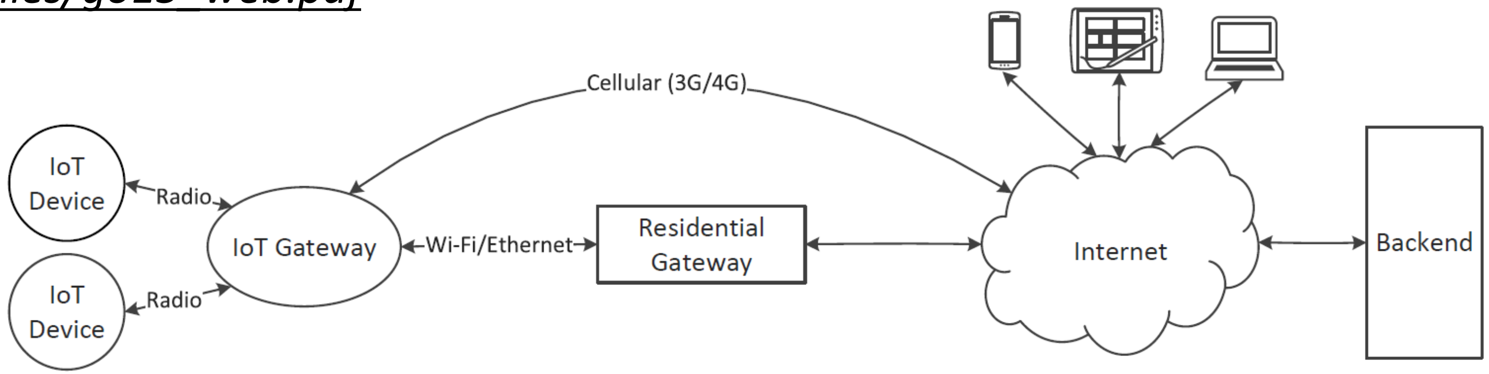
- Enycryption of data between components
- Strong encryption mechanism
- Credentials should not be exposed in the nw
- End-to-end encryption
- Should not use cunsom encryption mechanism
- Stored data should be encrypted

IoTSF also propose checklist based approach in their compliance framework

We evaluate security class for control signals component typically used for demand control in household



https://www.ree.es/sites/default/files/go15_web.pdf

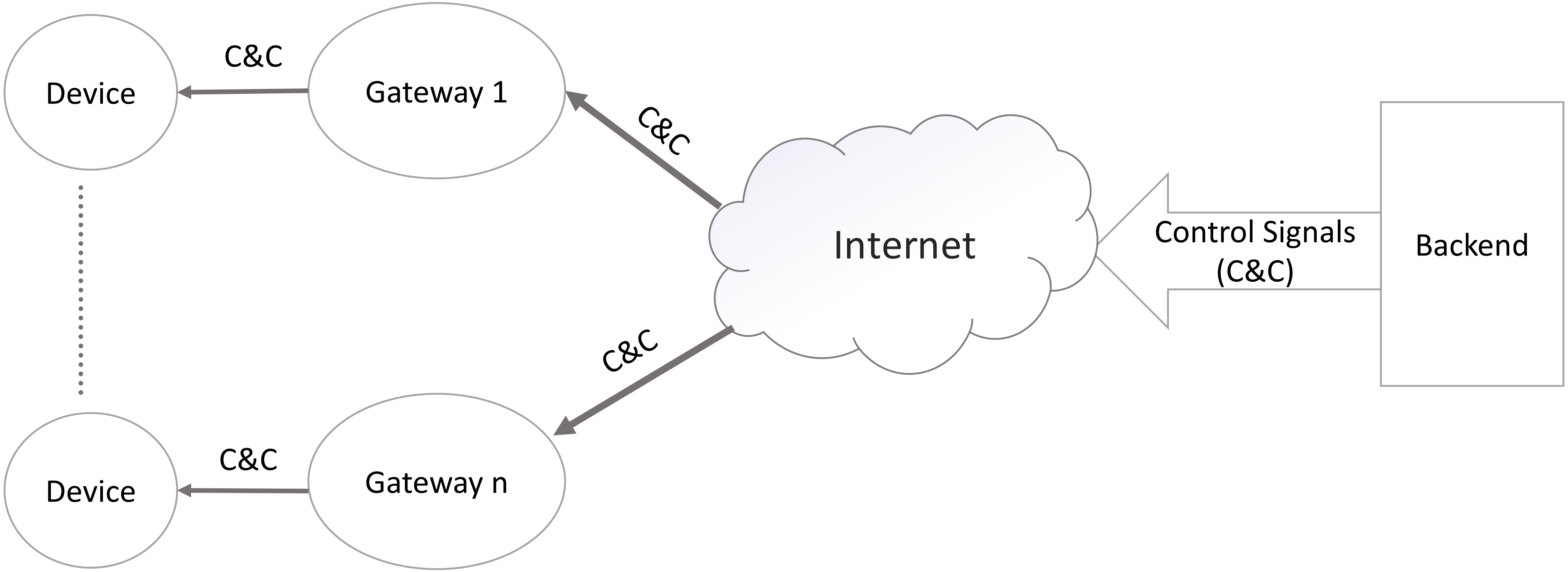


Applying the security class methodology on:

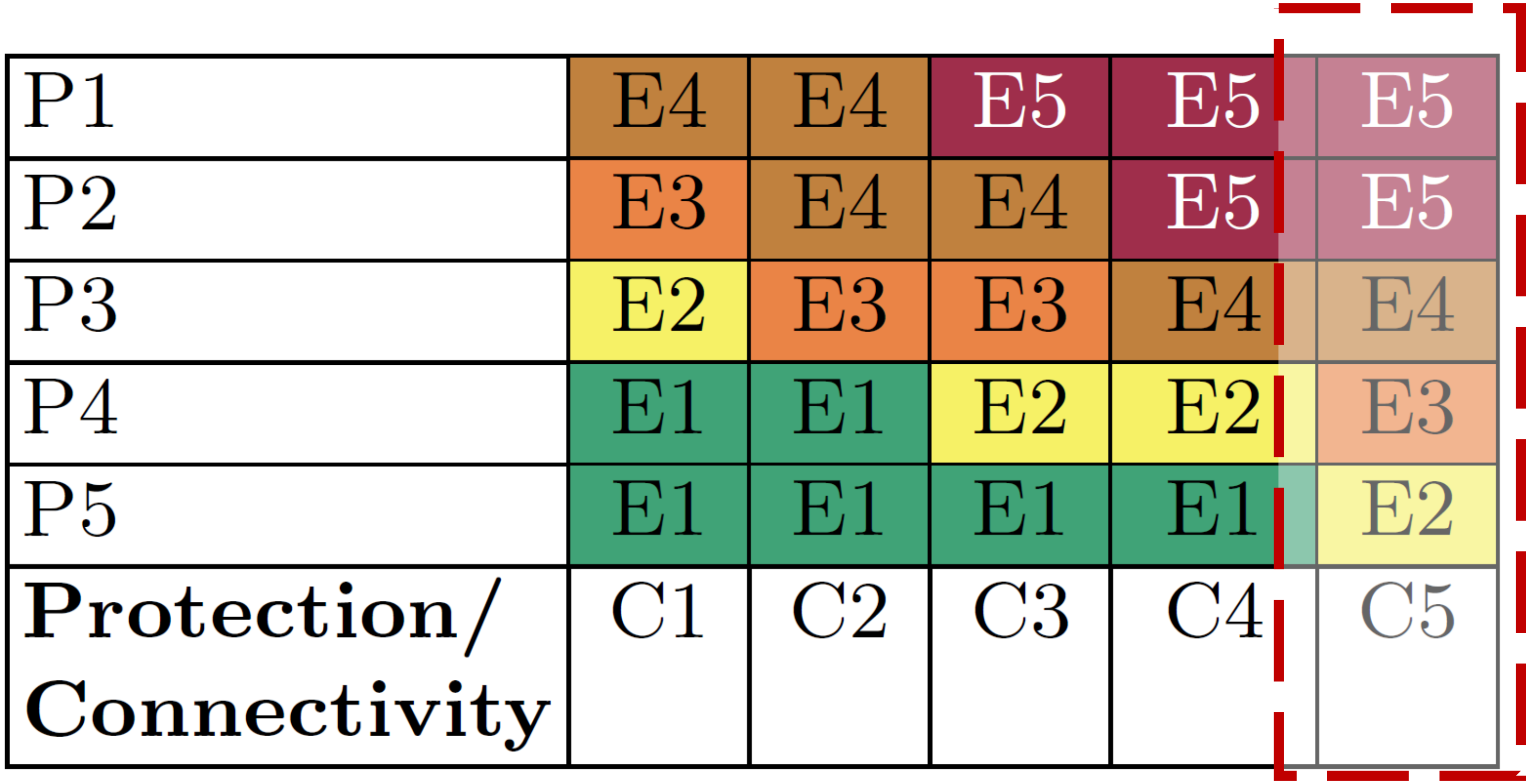
Scenario I: Centralized Control

Scenario II: Edge control

Scenario I: Centralized Control

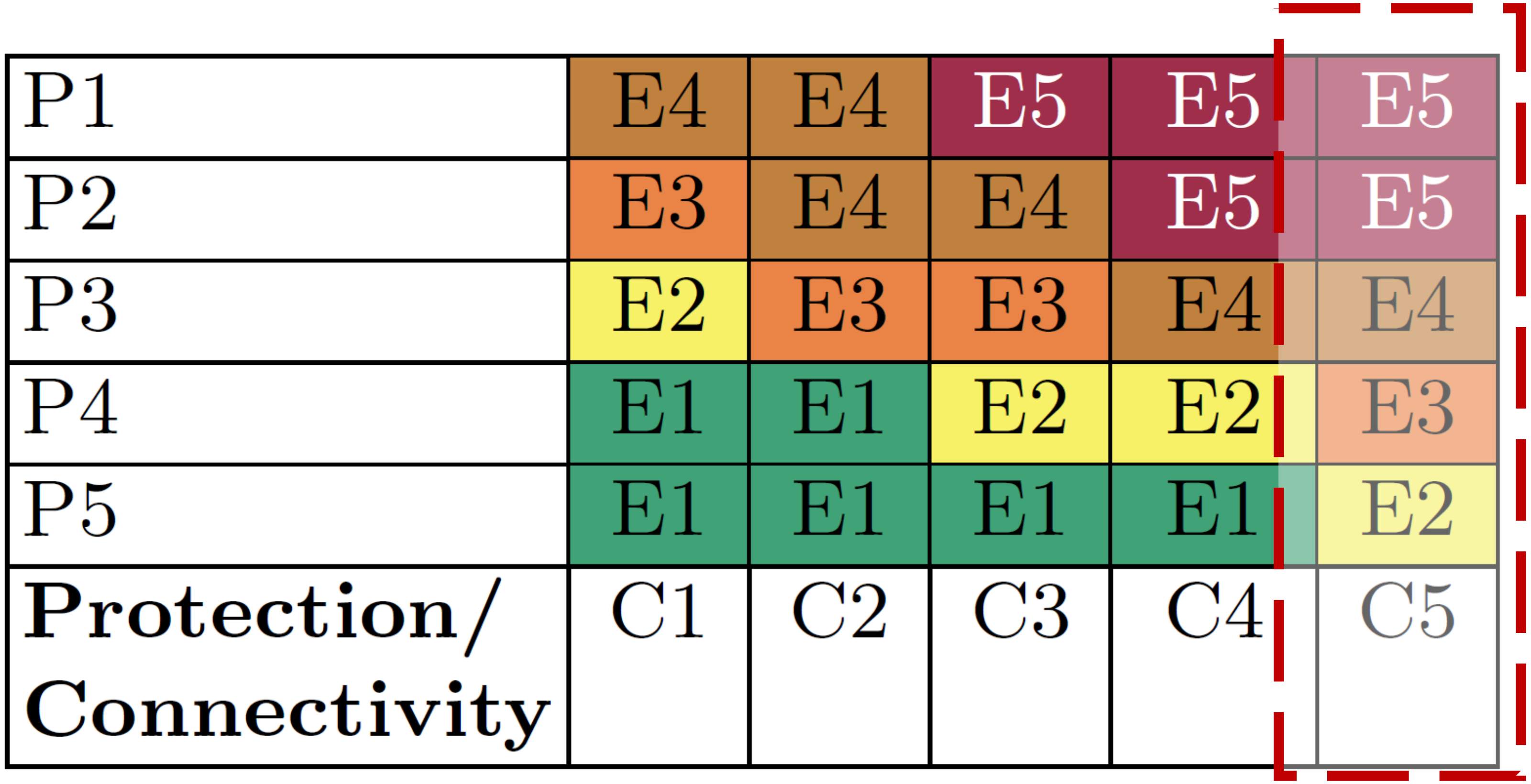


Scenario I: Centralized Control has Exposure E3



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

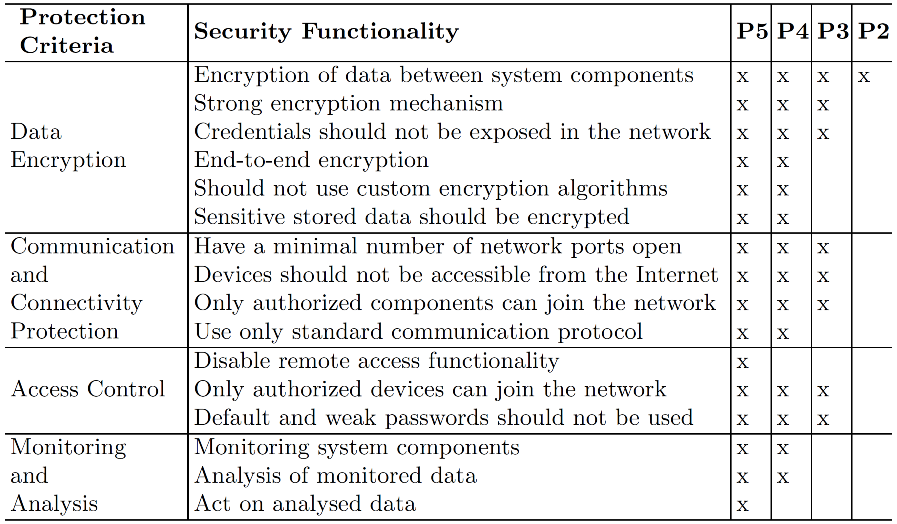
Scenario I: Centralized Control has Exposure E3



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

Data encryption, communication and connectivity protection, access control and monitoring and analysis are relevant protection criteria for this component

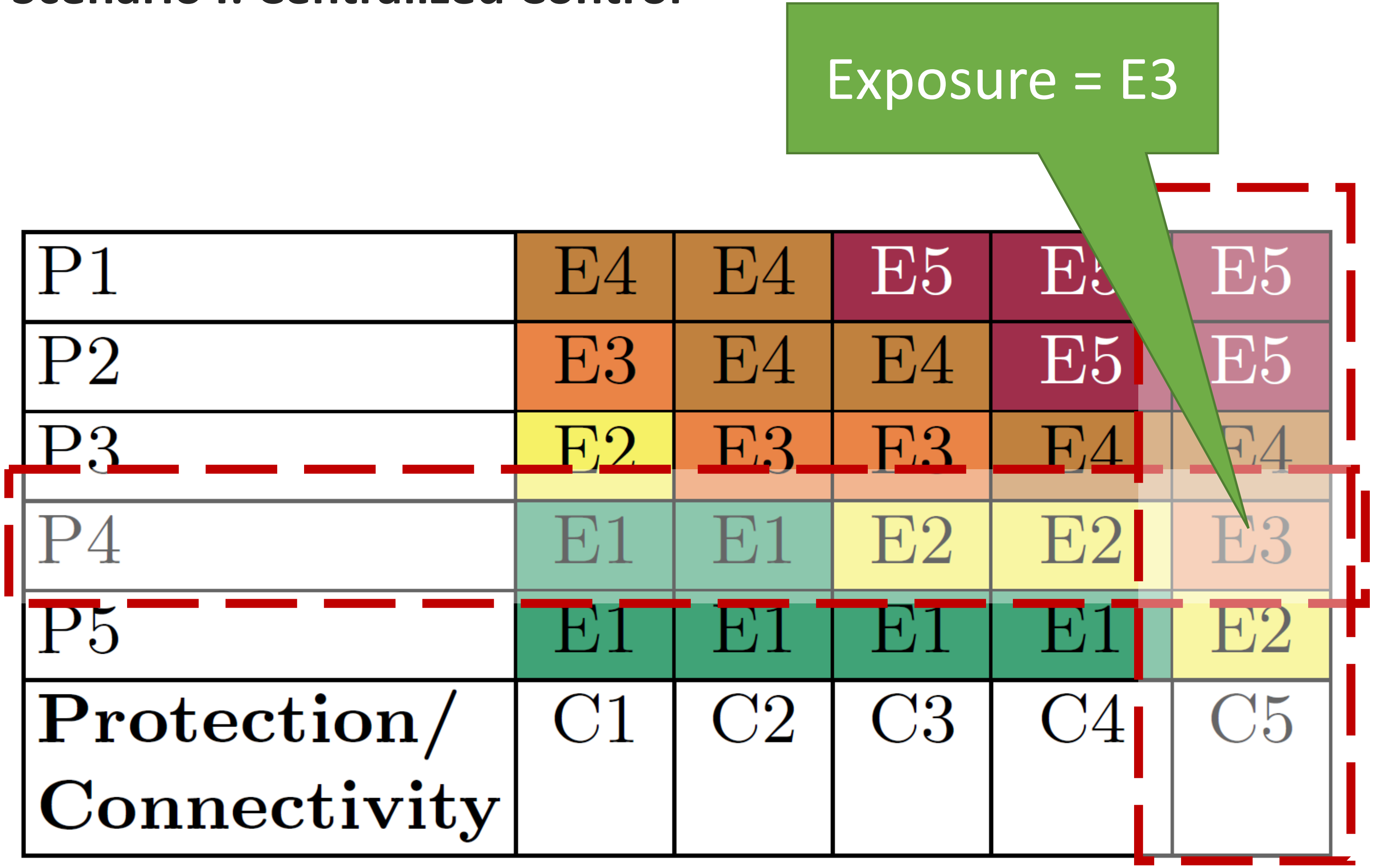
Data encryption, communication and connectivity protection, access control and monitoring and analysis are relevant protection criteria for this component



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		
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	
Monitoring and Analysis	Monitoring system components	x	x		
	Analysis of monitored data	x	x		
	Act on analysed data	x			

- Disable remote access functionality
- Only authorized devices can join the network
- The APIs calls should be authenticated and authorized
- Default and weak passwords should not be used

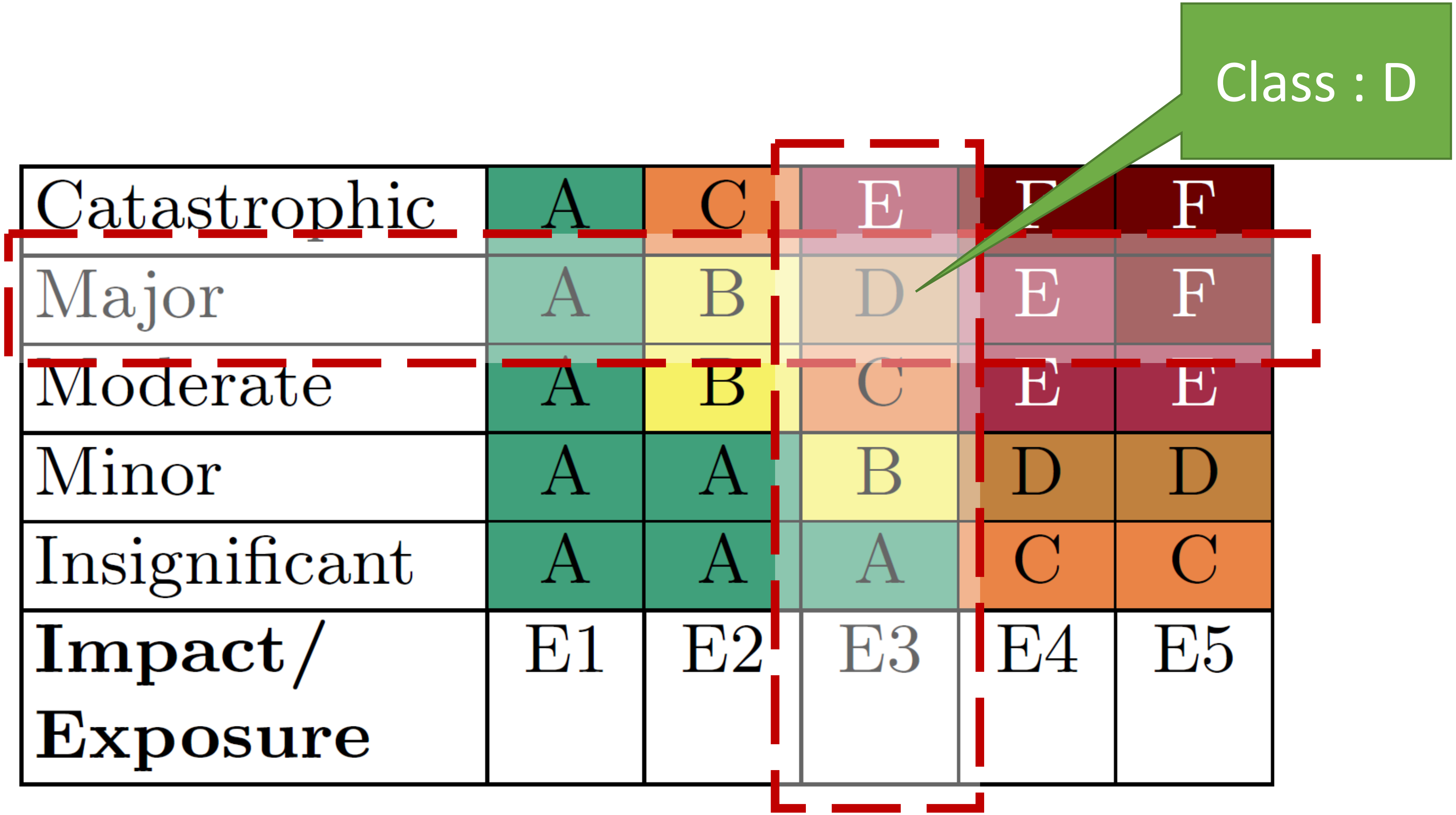
Scenario I: Centralized Control



Exposure = E3

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

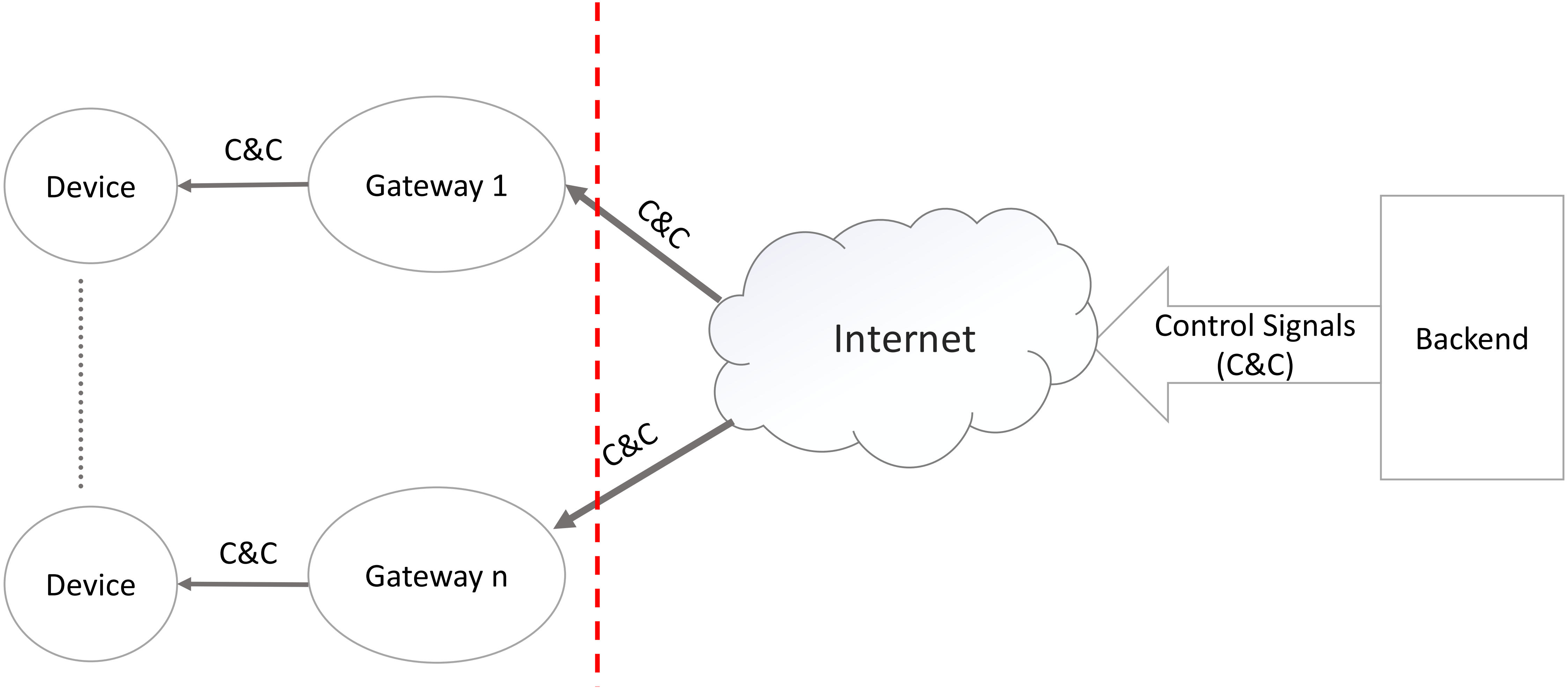
Scenario I: Centralized Control



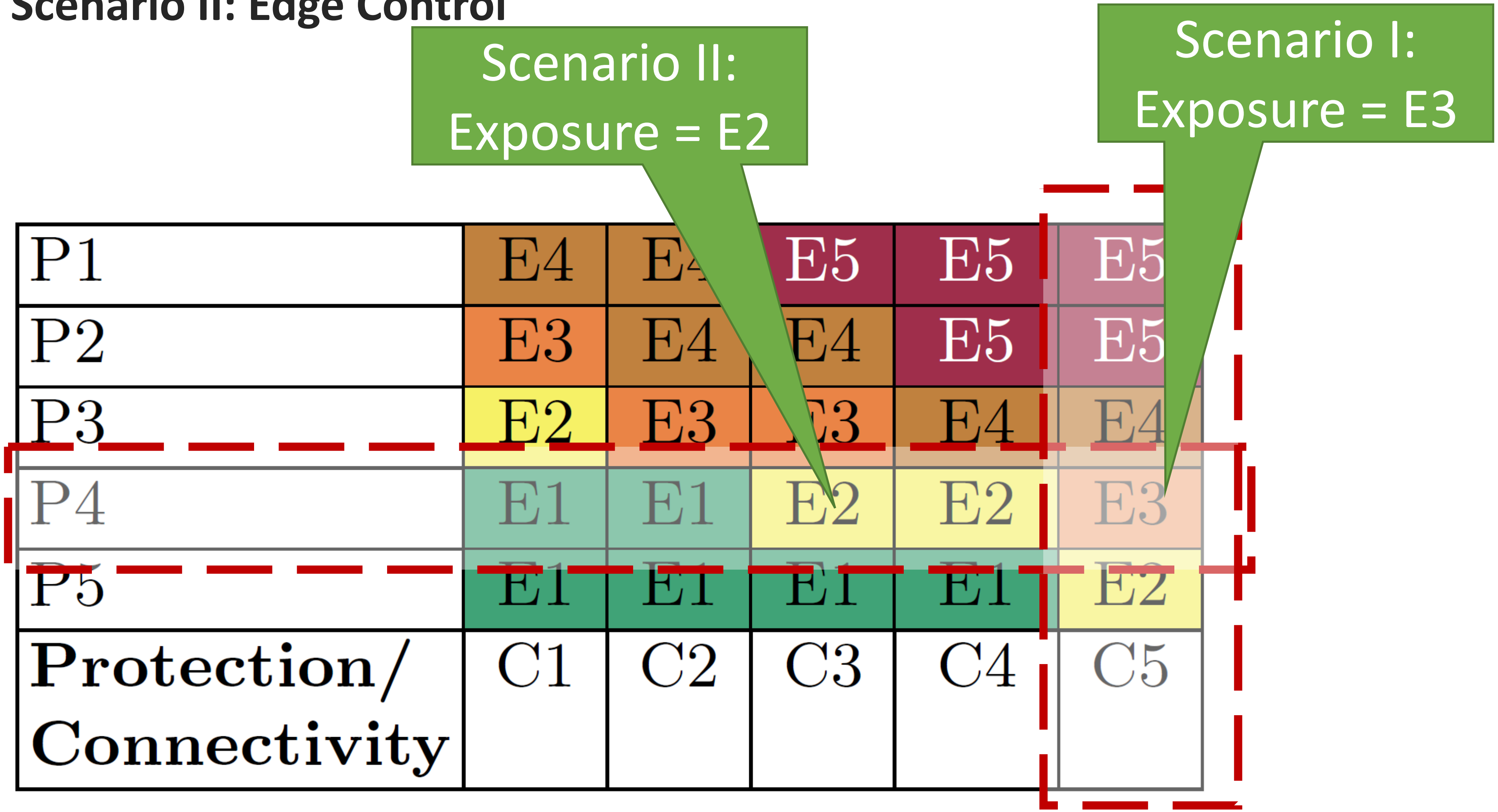
Catastrophic	A	C	E	F	F
Major	A	B	D	E	F
Moderate	A	B	C	E	E
Minor	A	A	B	D	D
Insignificant	A	A	A	C	C
Impact/ Exposure	E1	E2	E3	E4	E5

Class : D

Scenario II: Edge Control



Scenario II: Edge Control

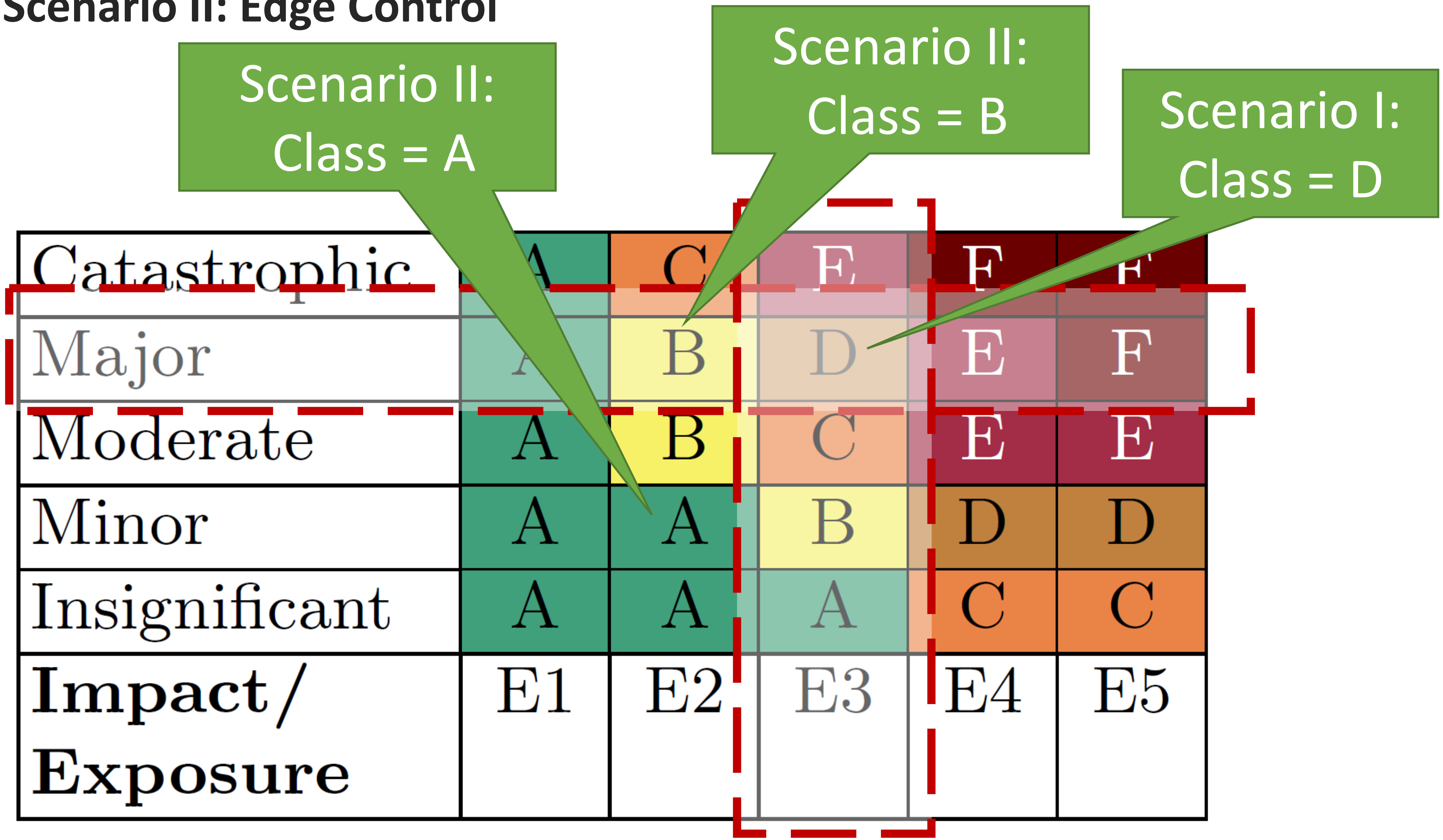


Scenario II:
Exposure = E2

Scenario I:
Exposure = E3

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

Scenario II: Edge Control



Scenario II: Class = A

Scenario II: Class = B

Scenario I: Class = D

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

Conclusion and Discussion

- **Security classification for Smart Home**
- **Appropriate security functionalities for**
  - Scenario I -> class D
  - Scenario II-> class B, single device leads to class A
- **Security Classification Method provides to end users**
  - transparency and
  - security awareness

- **Current Work**
  - Aggregation mechanism to calculate overall class for the system
  - Assurance mechanism to validate the expert judgement

Thank you for your attention

manish.shrestha@esmartsystems.com

Questions?

Compare other method or related work