UNIVERSITY OF OSLO

TEK5530 Measurable Security for the Internet of Things

L8 - Security Classification of Smart Home Energy Management Systems

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

[Courtesy: Manish Shrestha, UiO, 2019]

Josef Noll
Professor
Department of Technology Systems

UNIVERSITY
OF OSLO

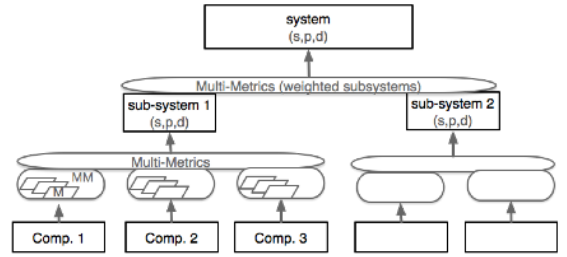
L9 - Expected Learning outcomes

Having followed the lecture, you can

- explain terminology for security and privacy
- provide examples of security classes
- provide examples of privacy data
- reason over relation between $System_{SPD}$ and security/privacy goals of applications

versus

$System_{SPD}$



system of systems

Acknowledgements

- This presentation was developed by

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

- as part of the PhD work
- see: https://its-wiki.no/wiki/Smart_ICT_2019

Smart ICT 2019 [edit]

Title	Smart ICT 2019
Place	Saidia@Morocco
Date, Time	2019/09/26, -28Sep2019
Contact Person	Josef.Noll
Participants	Manish Shrestha
related to Project	SenSecPhD
Keywords	

this page was created by Special:FormEdit/Meeting, and can be edited by Spe

Category:Meeting

https://link.springer.com/conference/smartict

Thumb	Title
	**Security Classification of Smart Home Energy Ma** *Click to Open* **Smart ICT 2019**

The presentation is linked to the paper Media:ICT_2019_paper_Manish.pdf

Applying Security Classification to Smart Home Energy Management

Background
- Problem Statement
- Security Classes

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

Implications
- Discussion and Conclusion
- Further work

[Courtesy: Manish Shrestha, UiO, 2019]

Standards & Certifications

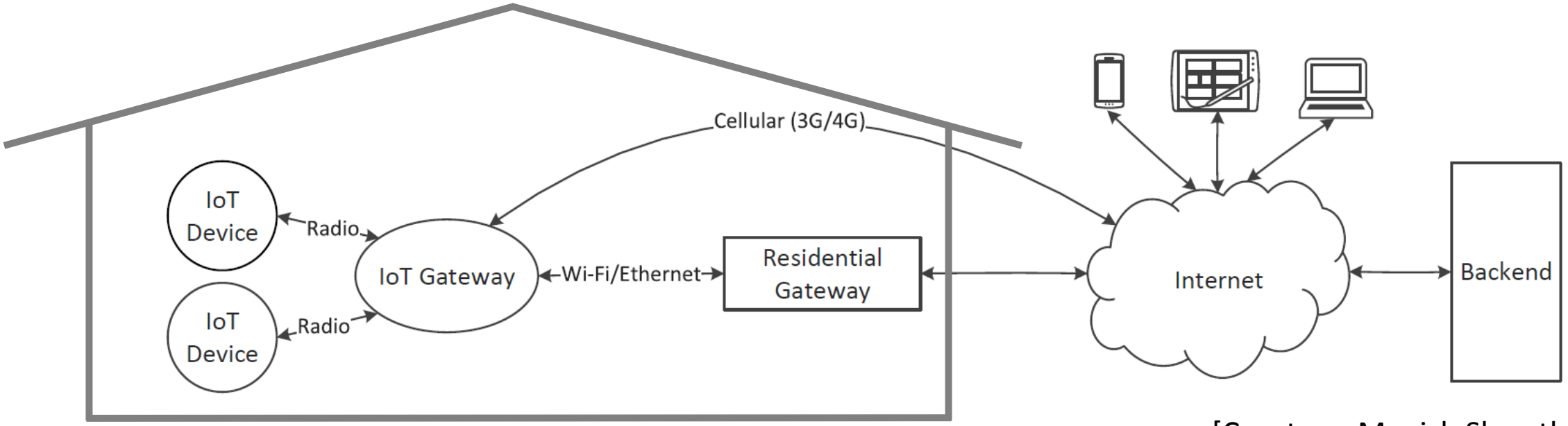
- Not adapted to IoT world
- Cost, complexity

Security Class

[Courtesy: Manish Shrestha, UiO, 2019]

Smart Home Energy Management (SHEMS)

- Adopted from e2U Systems
- Components:
  - IoT hub (IoT Gateway)
  - IoT Devices
  - Residential Gateway
  - Communication Channels
  - Backend System
  - Application and Network Data
- Sensor reading & Control Signals

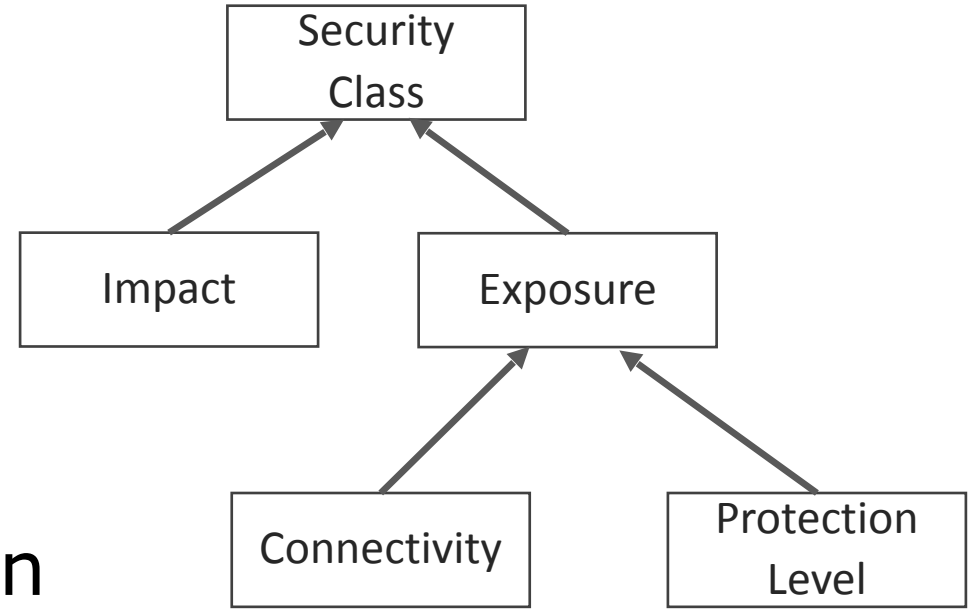


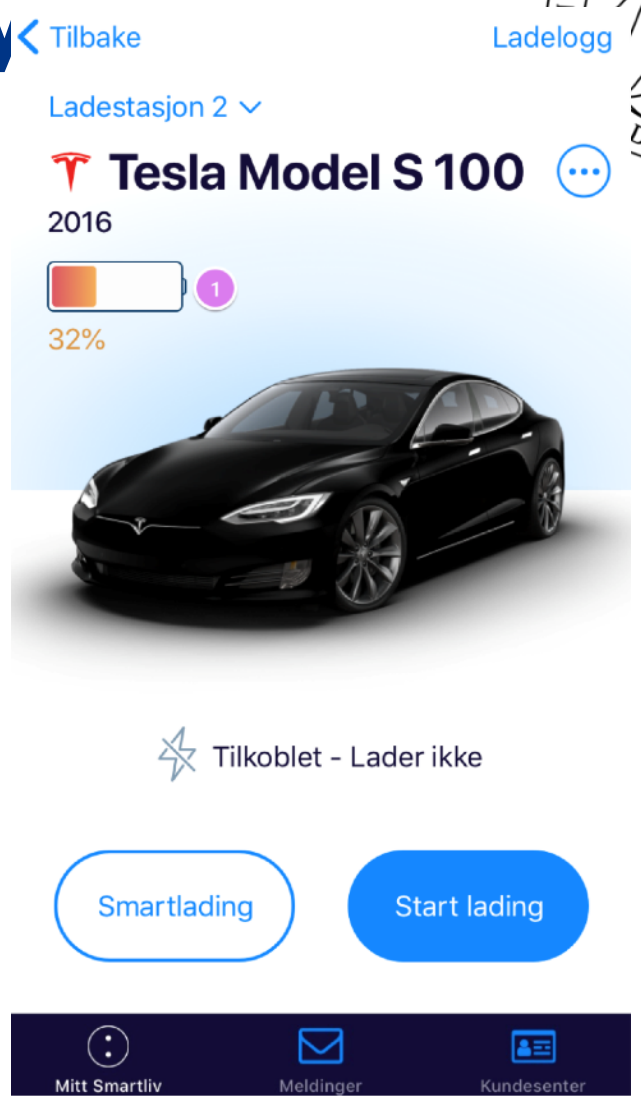
[1] Ghirardello, K., Maple, C., Ng, D., Kearney, P.: Cyber security of smart homes:Development of a reference architecture for attack surface analysis (2018)

[Courtesy: Manish Shrestha, UiO, 2019]

Security Classification Methodology

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





[Courtesy: Manish Shrestha, UiO, 2019]

Exposure

- Connectivity
- Protection Level

Lowest Protection

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

Highest Protection

Isolated

Wireless connectivity

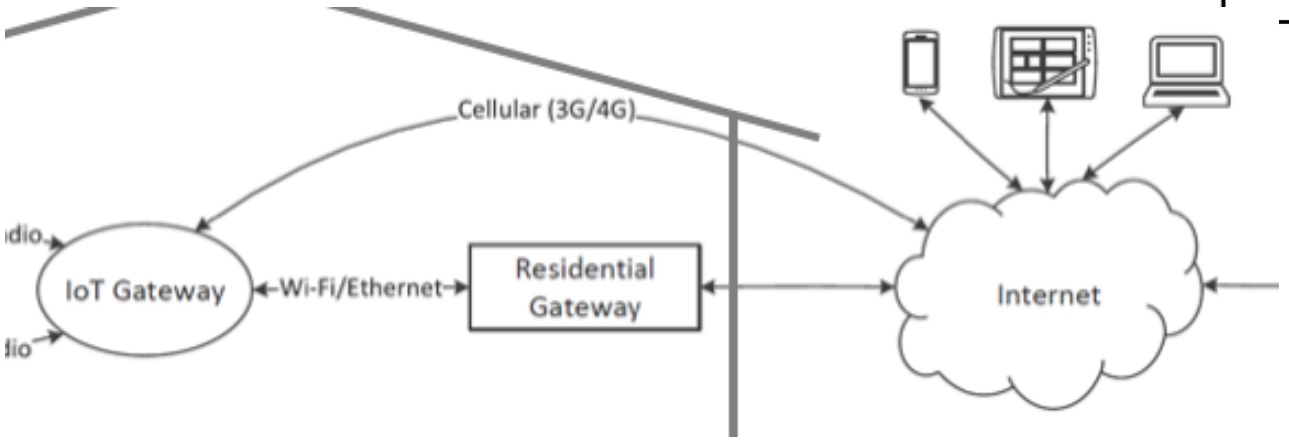
Internet

[Courtesy: Manish Shrestha, UiO, 2019]

Impact & Exposure gives Security Class

- Within the house
- External provider

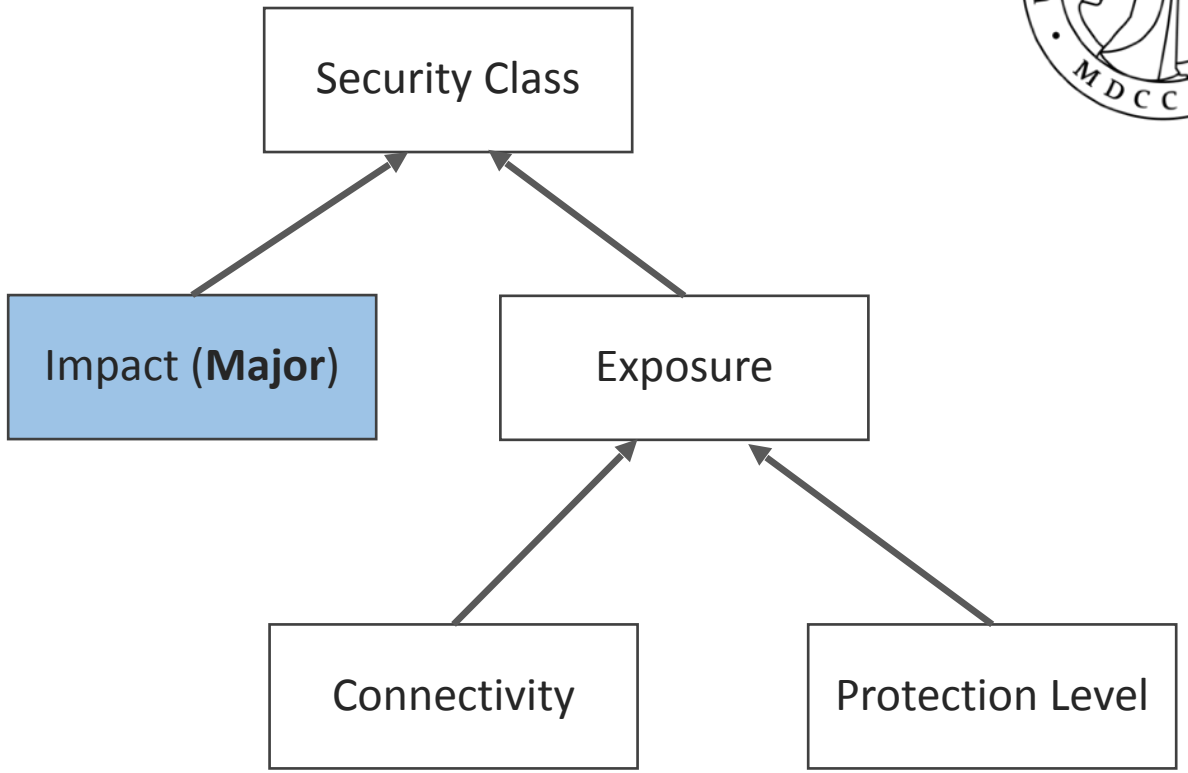
Catastrophic	A	C	E	F	F
Major	A	B	D	E	F
Moderate	A	B	C	E	E
Minor	A	A	B	D	D
Insignificant	A	A	A	C	C
Impact / Exposure	E1	E2	E3	E4	E5



[Courtesy: Manish Shrestha, UiO, 2019]

Impact

- Safety (grid failure)
- Grid stability [2]
- Agents for cyberattacks
- Increased electricity bills
- Privacy



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

[Courtesy: Manish Shrestha, UiO, 2019]

Available standards & Guidelines

- Adopted from standards

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

[Courtesy: Manish Shrestha, UiO, 2019]

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			

Protection levels

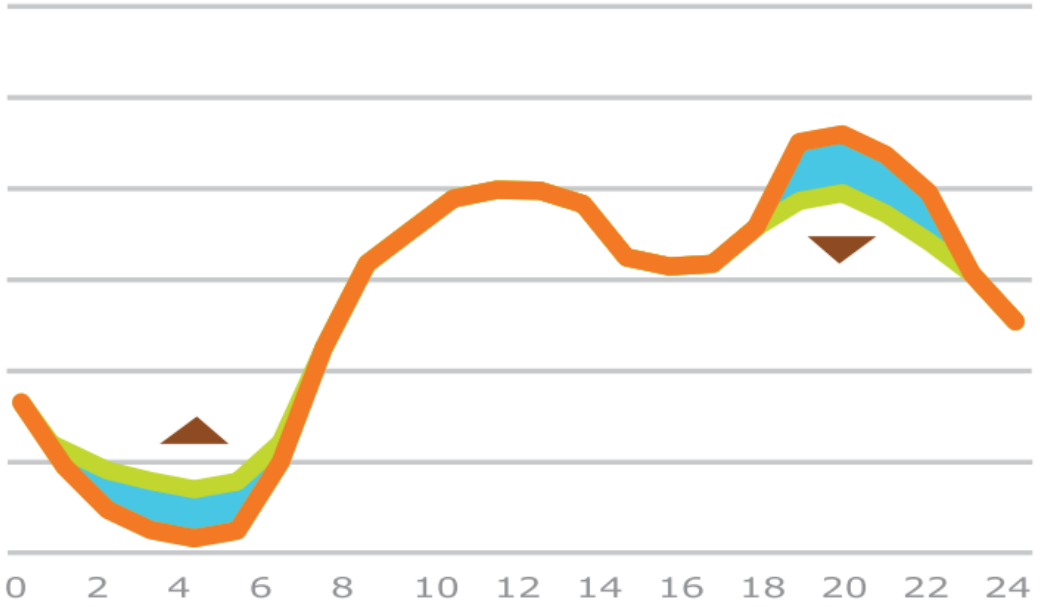
- P1-P5 from security functionality
- Encryption of data between components
- Strong encryption mechanism
- Credentials should not be exposed in the network
- End-to-end encryption
- Should not use cunsom encryption mechanism
- Stored data should be encrypted

IoTSF also propose checklist based approach in their compliance framework

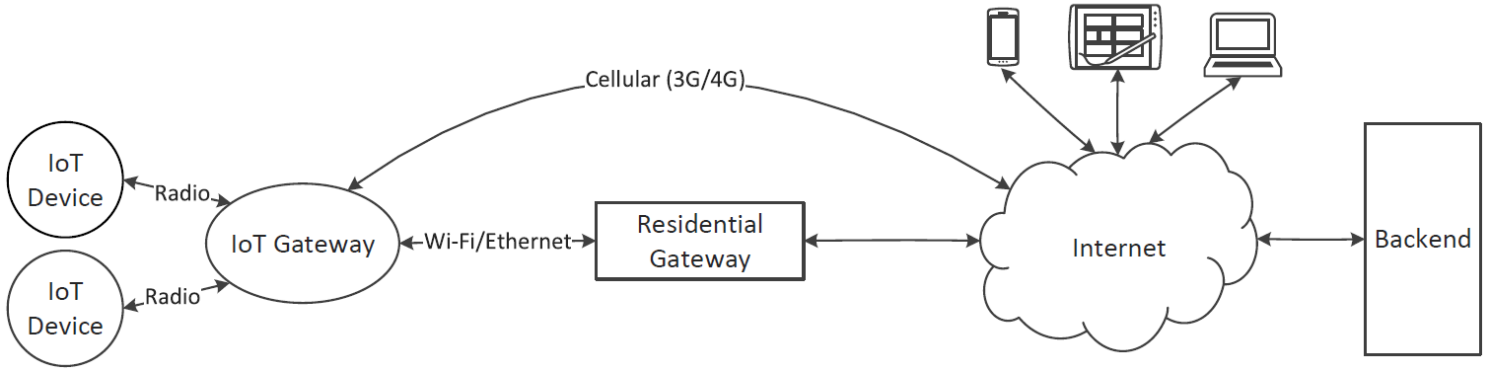
[Courtesy: Manish Shrestha, UiO, 2019]

Evaluation of security class

- Focus: Control Signal components
  - car charging
  - hot water/heat pump
  - ventilation



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



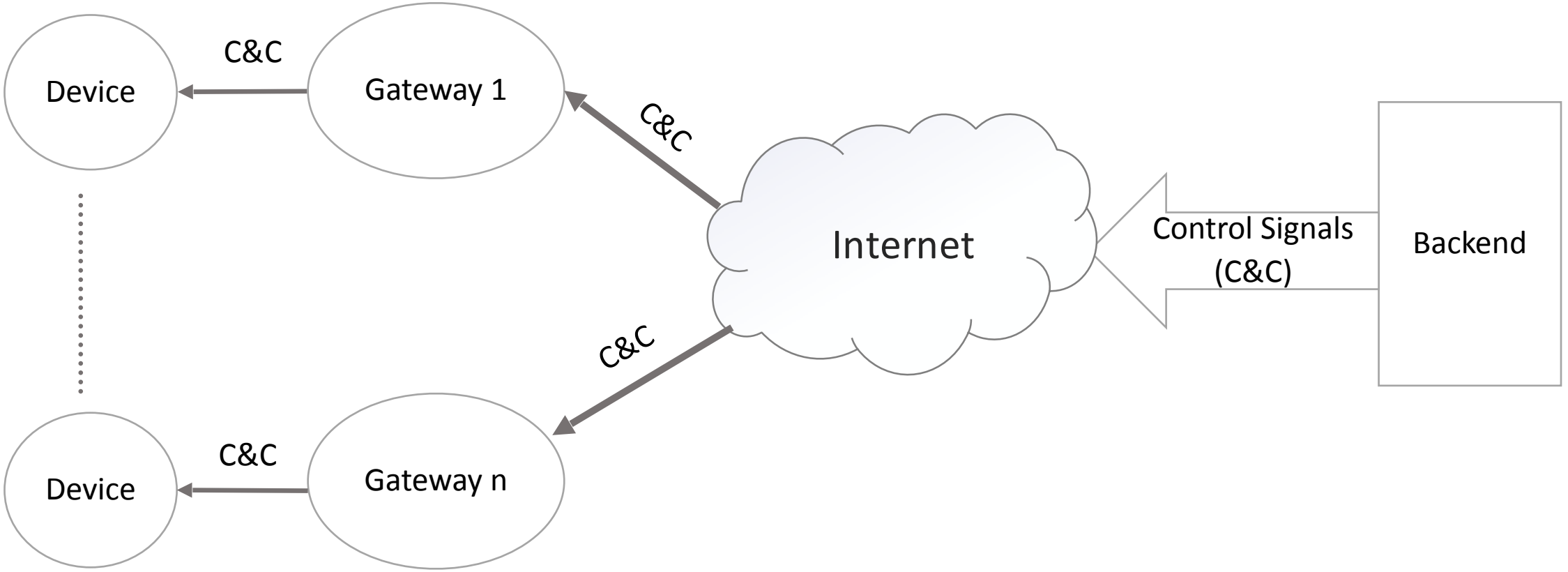
[Courtesy: Manish Shrestha, UiO, 2019]

Scenarios

- SC1: Centralised Control
- SC2: Edge Control

[Courtesy: Manish Shrestha, UiO, 2019]

SC1: Centralised Control



[Courtesy: Manish Shrestha, UiO, 2019]

SC1: Exposure calculation

- Assessment: Exposure E3
  - full Internet access (C5)
  - high protection (P4)

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

[Courtesy: Manish Shrestha, UiO, 2019]

SC1: Centralised Control

- Relevant protection criteria to achieve P4:
  - Data encryption
  - communication and connectivity protection
  - access control and
  - monitoring and analysis

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

[Courtesy: Manish Shrestha, UiO, 2019]

SC1: Relevant Protection Criteria

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 authorised devices can join the network
- The APIs calls should be authenticated and authorised
- Default and weak passwords should not be used

[Courtesy: Manish Shrestha, UiO, 2019]

SC1: Centralised Control

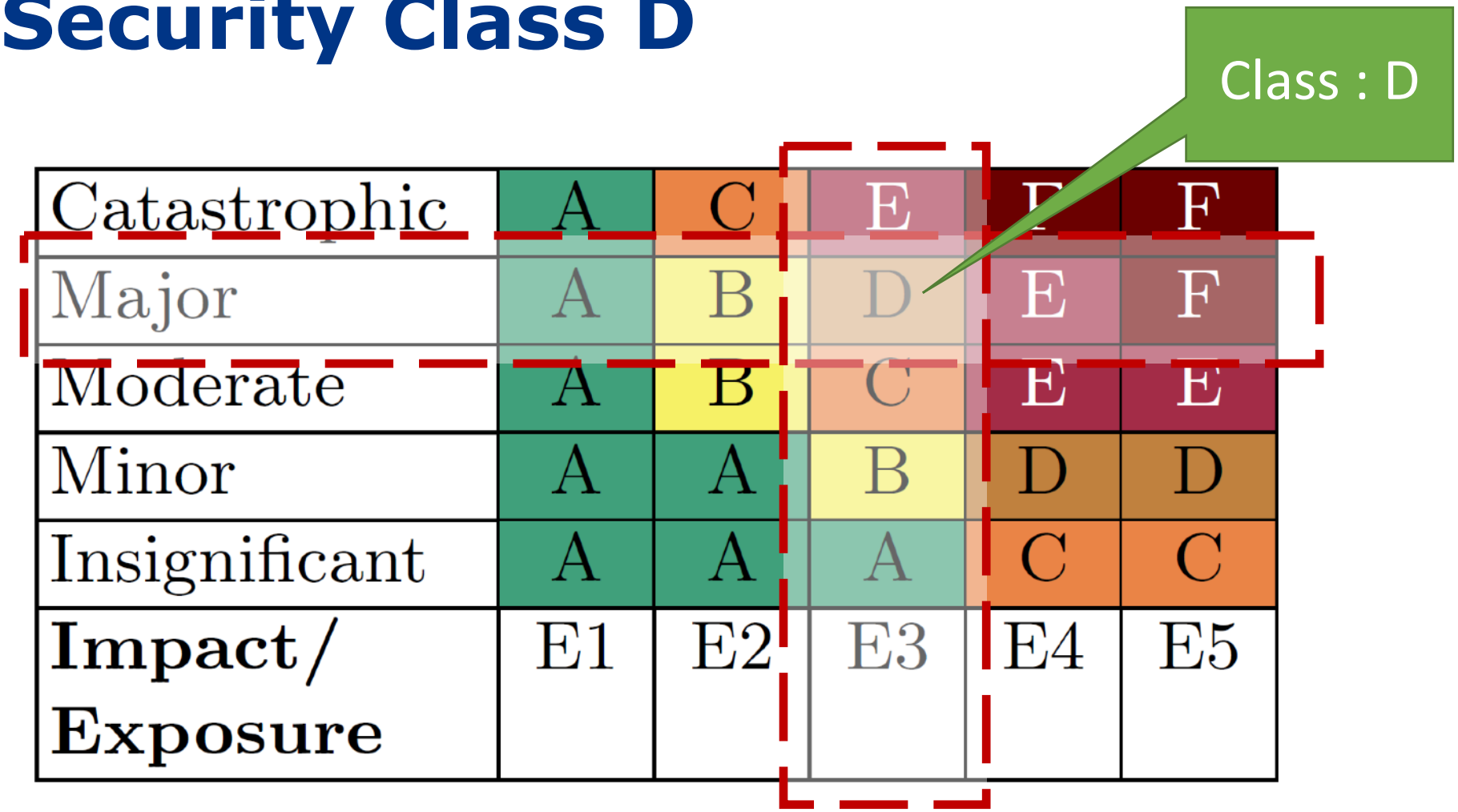
Exposure = E3

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

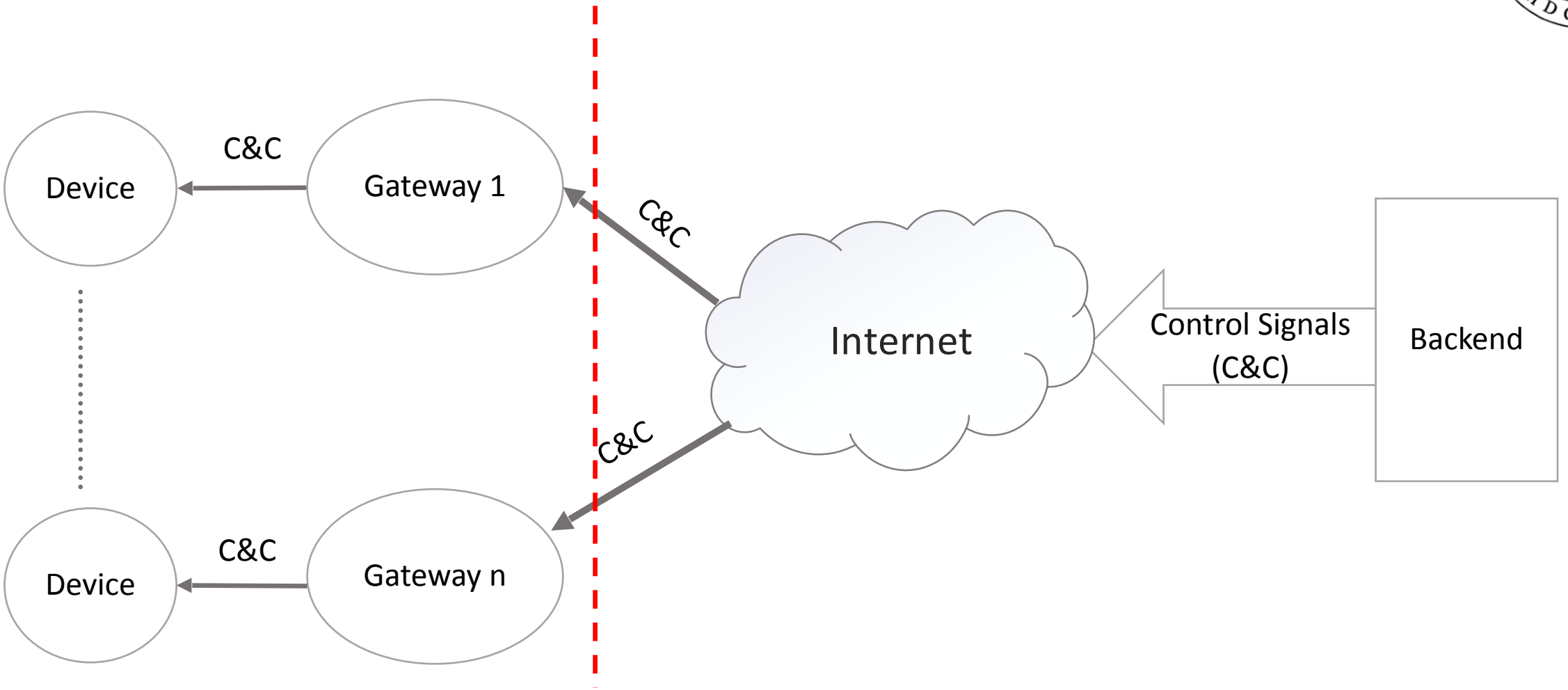
[Courtesy: Manish Shrestha, UiO, 2019]

SC1: Security Class D



[Courtesy: Manish Shrestha, UiO, 2019]

SC2: Edge Control



[Courtesy: Manish Shrestha, UiO, 2019]

SC2: Assessme

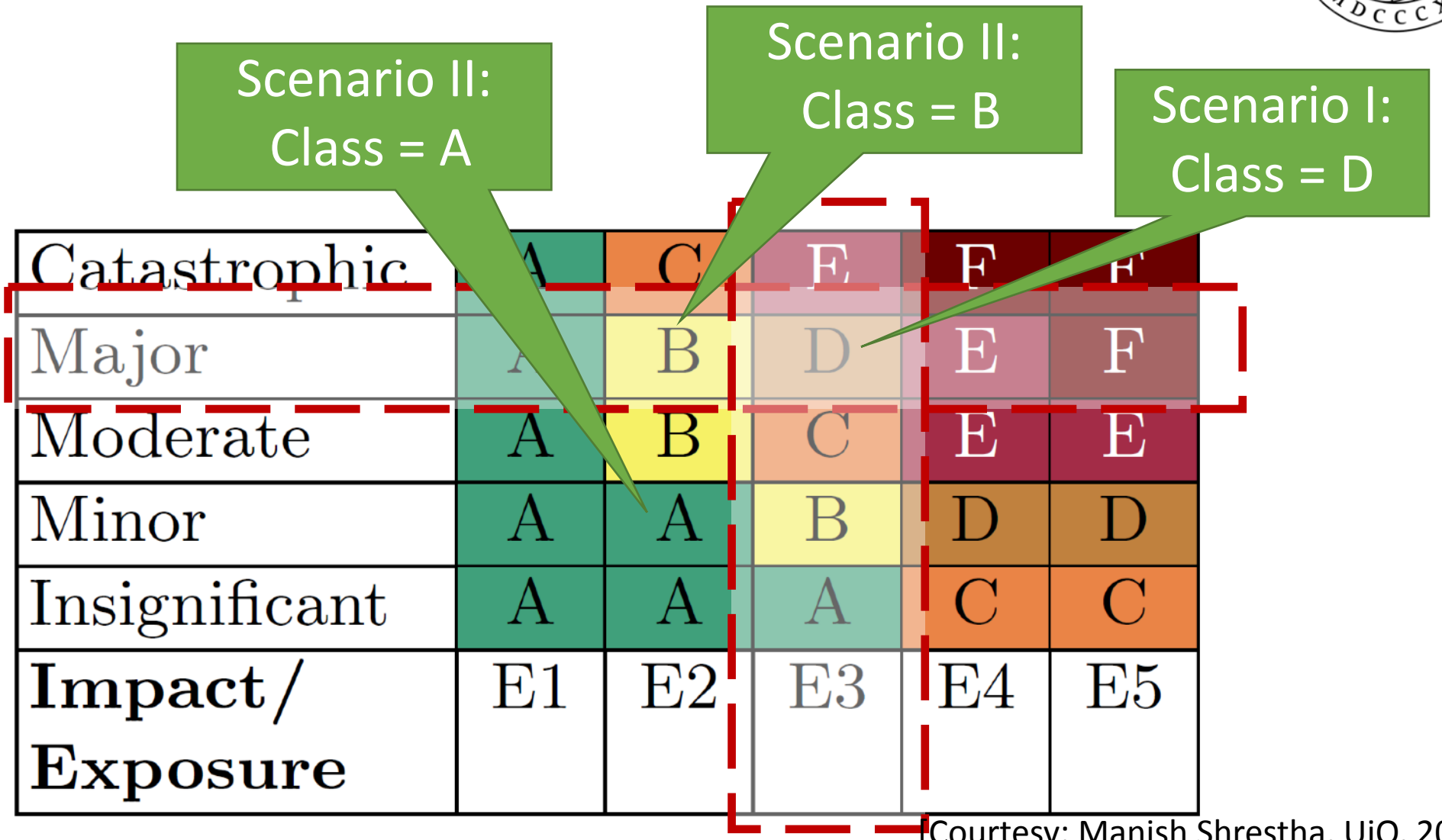
Scenario II: Exposure = E2

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

[Courtesy: Manish Shrestha, UiO, 2019]

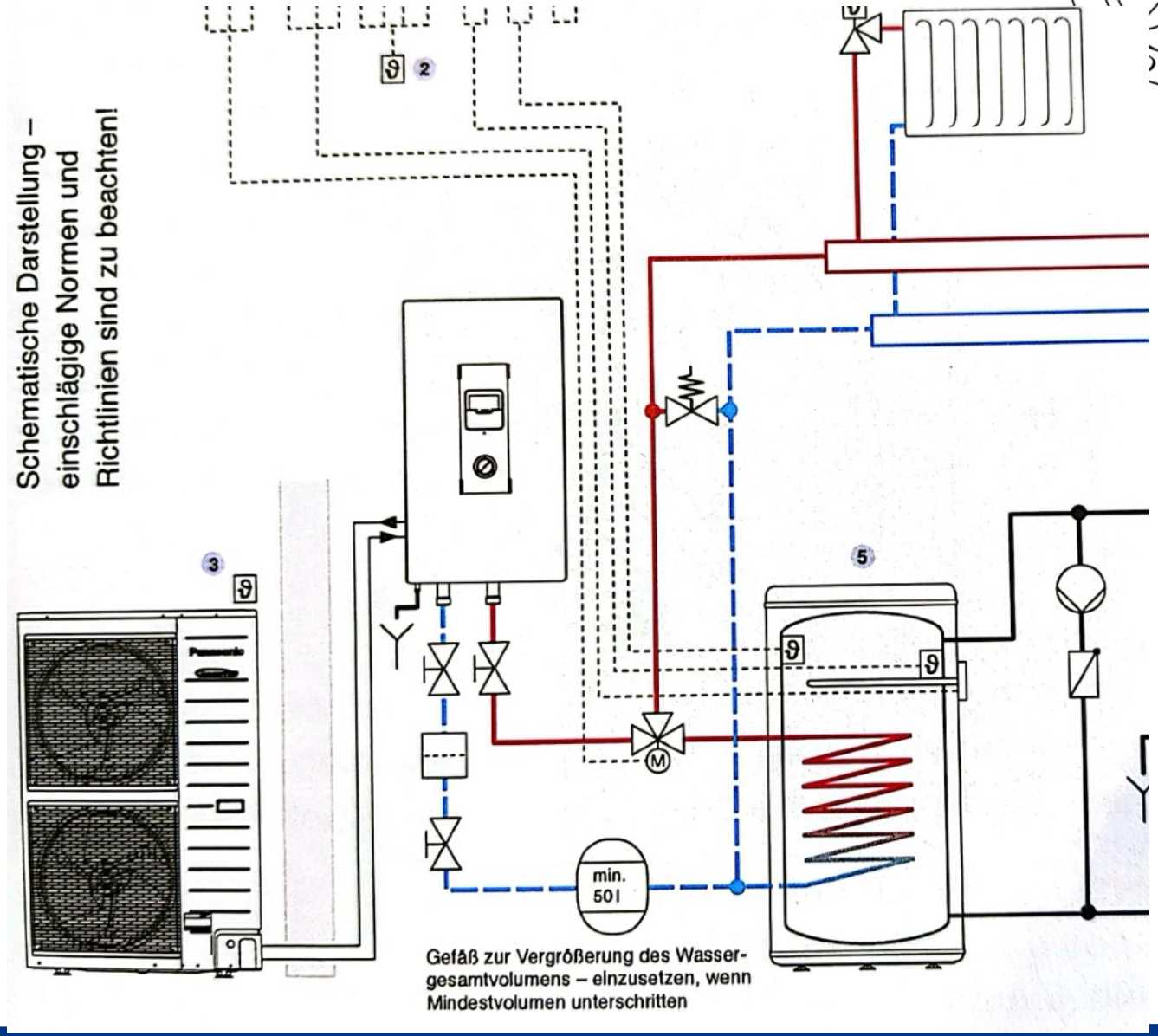
SC2: Edge Control - Security Class A / B



[Courtesy: Manish Shrestha, UiO, 2019]

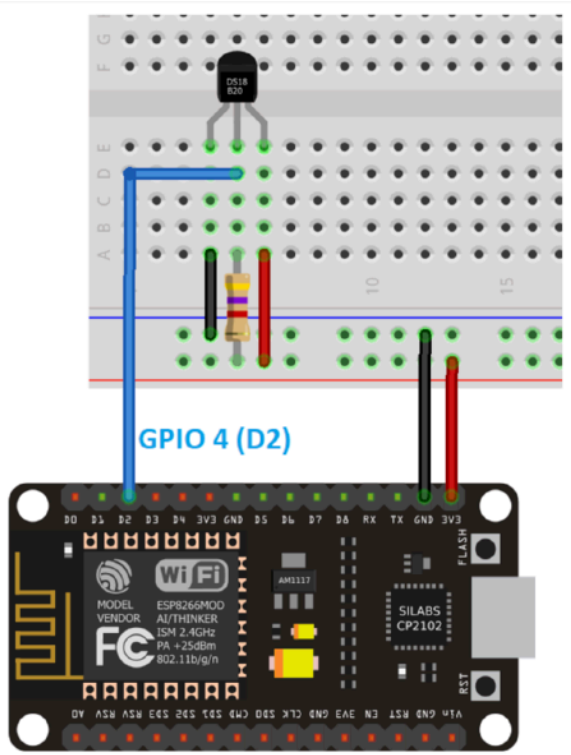
Real world assessment
Heat pump control

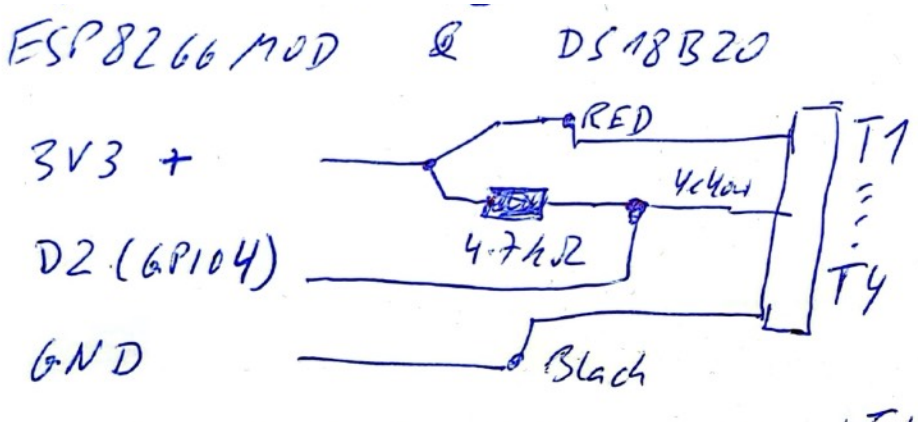
- Heat pump drives tank
  - Top: 240 l hot water
  - Bottom: 120 l floor heating
- Goal:
  - set temperature of water
  - price, convenience,

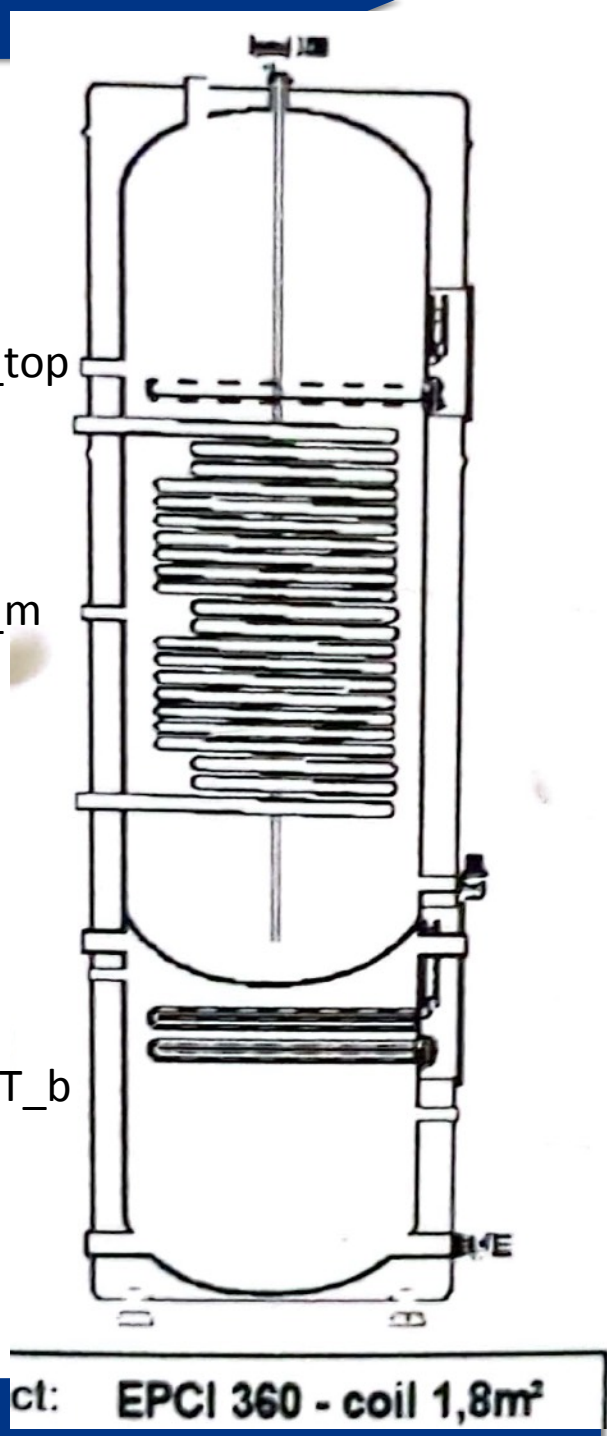


Temperature control

- ESP8266Mod
  - Tank top
  - Tank middle
  - Tank bottom
- connected to Raspberry Pi with Home Assistant

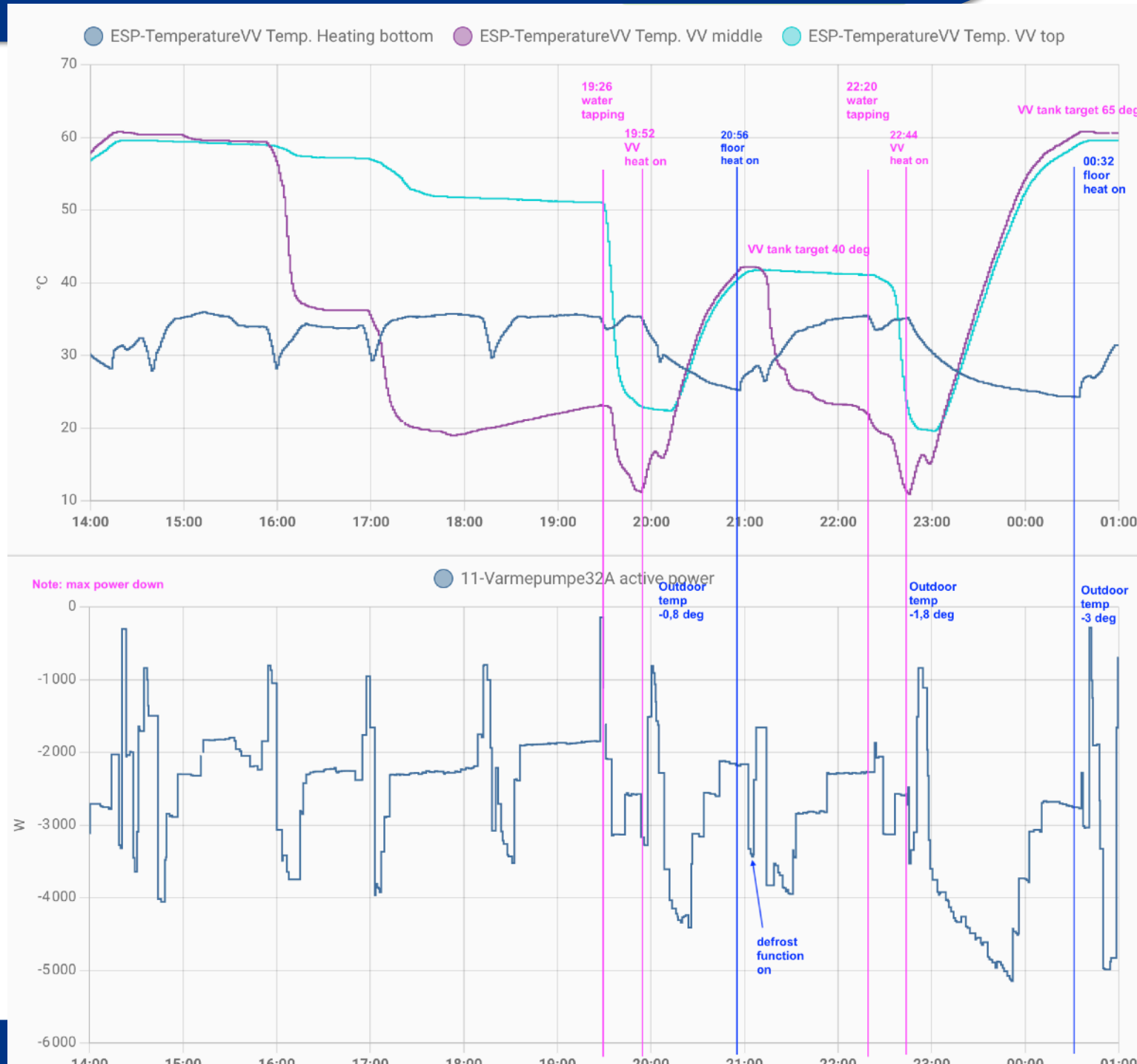






Tank simulation

- Switch heat pump off
  - set water temperature
- (Invers) power profiel



Heat pump

Assessment Detail

Name

Heat pump control

Component Type

Iot Device

Description

Heat pump measure and switch on/off

Select Connectivity

C3

Select Impacts

Major

Connectivity

Connectivity represents the surface of a system exposed to attacks. We have considered five levels of connectivity (C):

1. **C1** Includes completely closed/isolated systems
2. **C2** Includes the system with wired Local Area Network and does not permit operations from outside the network
3. **C3** Includes all C2 systems that also use wireless technologies.
4. **C4** Includes the system with private or leased infrastructure, which may permit remote operations (e.g., VPN, private APN, etc). An example could be allowing to access the corporate network only via VPN. Another example could be the operators being able to connect to their field devices system through their mobile device using a private Access Point Name (APN)
5. **C5** Includes distributed systems with public infrastructure, i.e., like the C4 category except that the communication infrastructure is public. Example: Web applications and services accessible using Internet.

Protection Assessment

Security Criterion	Yes	No	N/A
Data Encryption	◉	○	○

Security Functionality	Yes	No	N/A
Encryption of data between system components	◉	○	○
Strong encryption mechanism	○	◉	○
Credentials should not be exposed in the network	◉	○	○
End-to-end encryption	◉	○	○
Should not use custom encryption algorithms	◉	○	○
Sensitive stored data should be encrypted	◉	○	○

Security Criterion	Yes	No
Software/Firmware Security	◉	○

Security Functionality	Yes	No
Updatability of device firmware	◉	○
Updatability of the operating system	◉	○
Automatic updates available	○	◉
Encryption of update files	○	◉
Signing update files before installing	○	◉

ESP8266 for heat pump control

You obtained **Class <E, 100.00, 0.00 >**

Details

Connectivity	C3
Protection Level (?)	P2
Impact	Major
Exposure (?)	E4
Security Class	**E**

Table: Exposure Lookup

Protection Level \ Connectivity	C1	C2	C3	C4	C5
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

Table: Class Lookup

Class \ Exposure	E1	E2	E3	E4	E5
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

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

[Courtesy: Manish Shrestha, UiO, 2019]