Safety-Security Convergence of Industrial Control Systems

« Attacks against SCADA made boring with formal methods »

Maxime PUYS

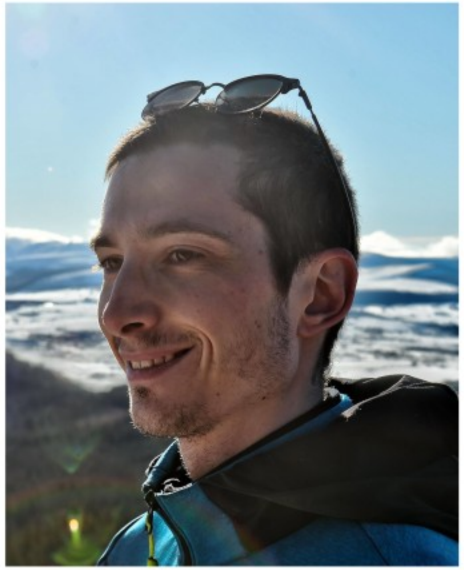
Dec. 13th, 2024

SoSySec Seminar

Slides shamelessly taken from Ph.D Defense of:

Mike Da Silva

Who am I?



- **Maxime Puys**
- Ph.D. in Computer Science Security in 2018 from Verimag, Univ. Grenoble Alpes
- 2018 – 2023: Research Engineer at CEA-LETI, Grenoble
- **Since 2023-10:** Associate Professor at IUT/LIMOS/SIC/RS
- **E-mail:** Maxime.Puys@uca.fr
- **Research interests:**
  - Cybersecurity of (I)IoT devices and networks
  - Cryptographic protocols

Two Types of IOT

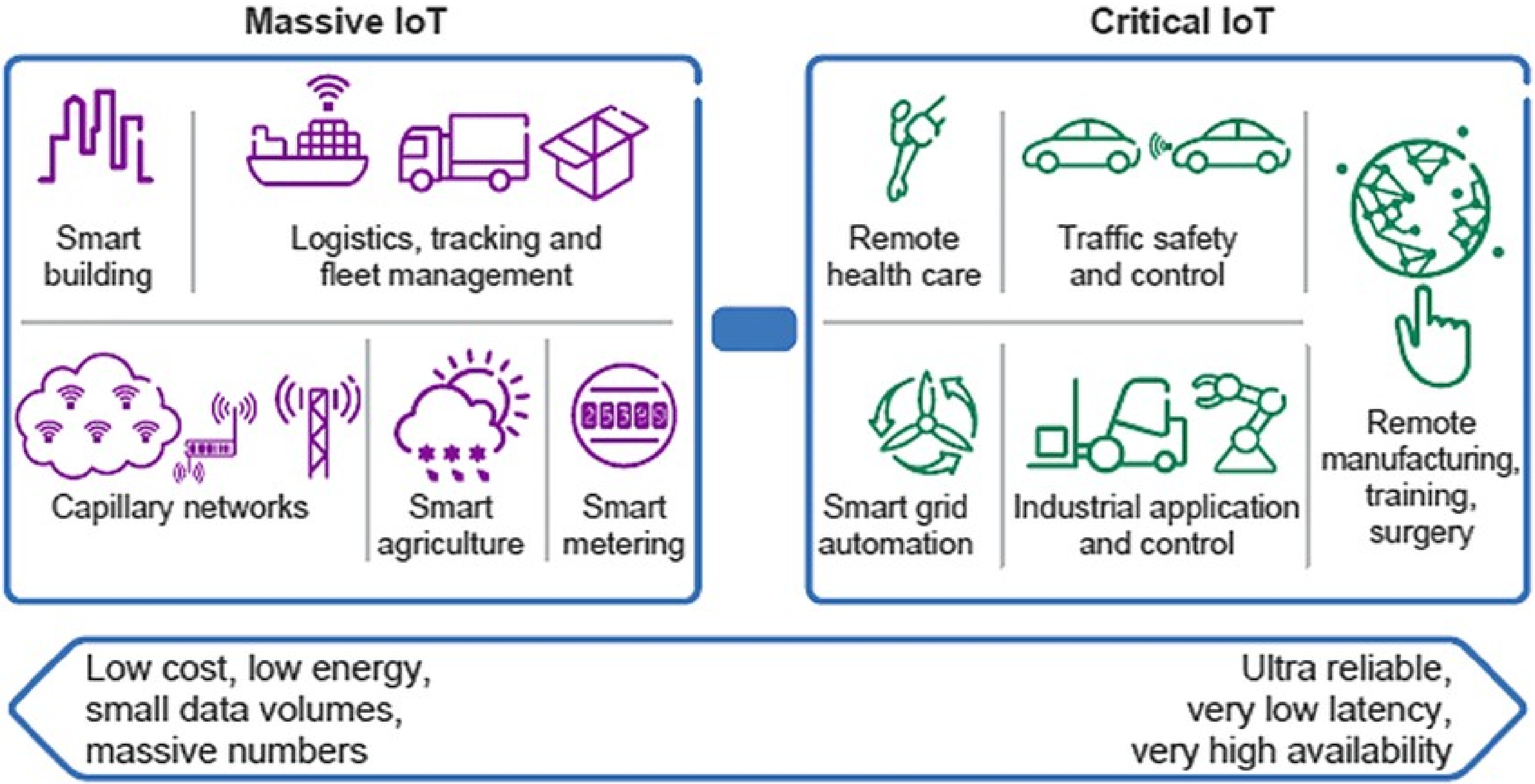

Massive IoT
Critical IoT
Smart building
Logistics, tracking and fleet management
Capillary networks
Smart agriculture
Smart metering
Remote health care
Traffic safety and control
Remote manufacturing, training, surgery
Smart grid automation
Industrial application and control
Low cost, low energy, small data volumes, massive numbers
Ultra reliable, very low latency, very high availability

Figure: [Alq19]

Two Types of IOT

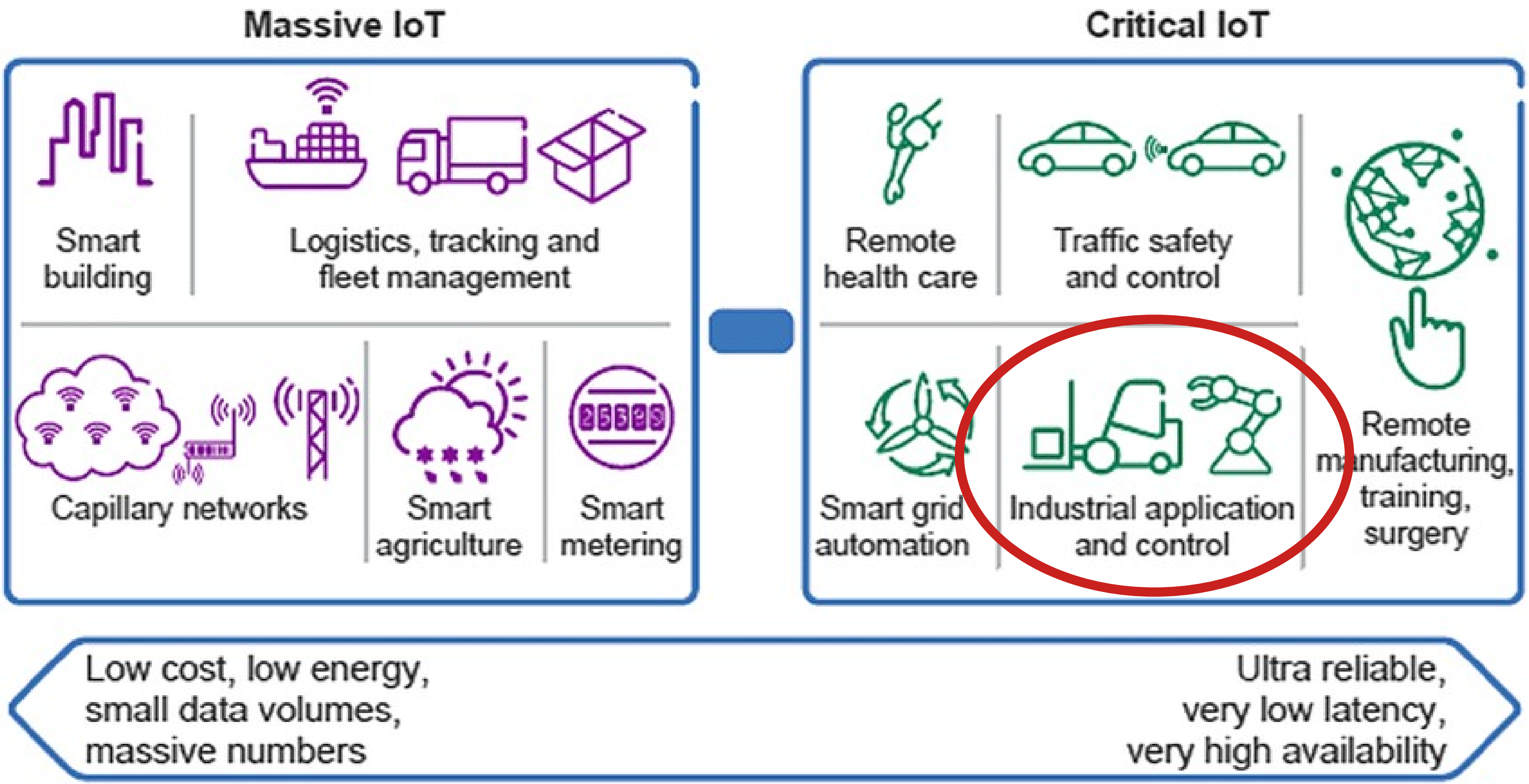
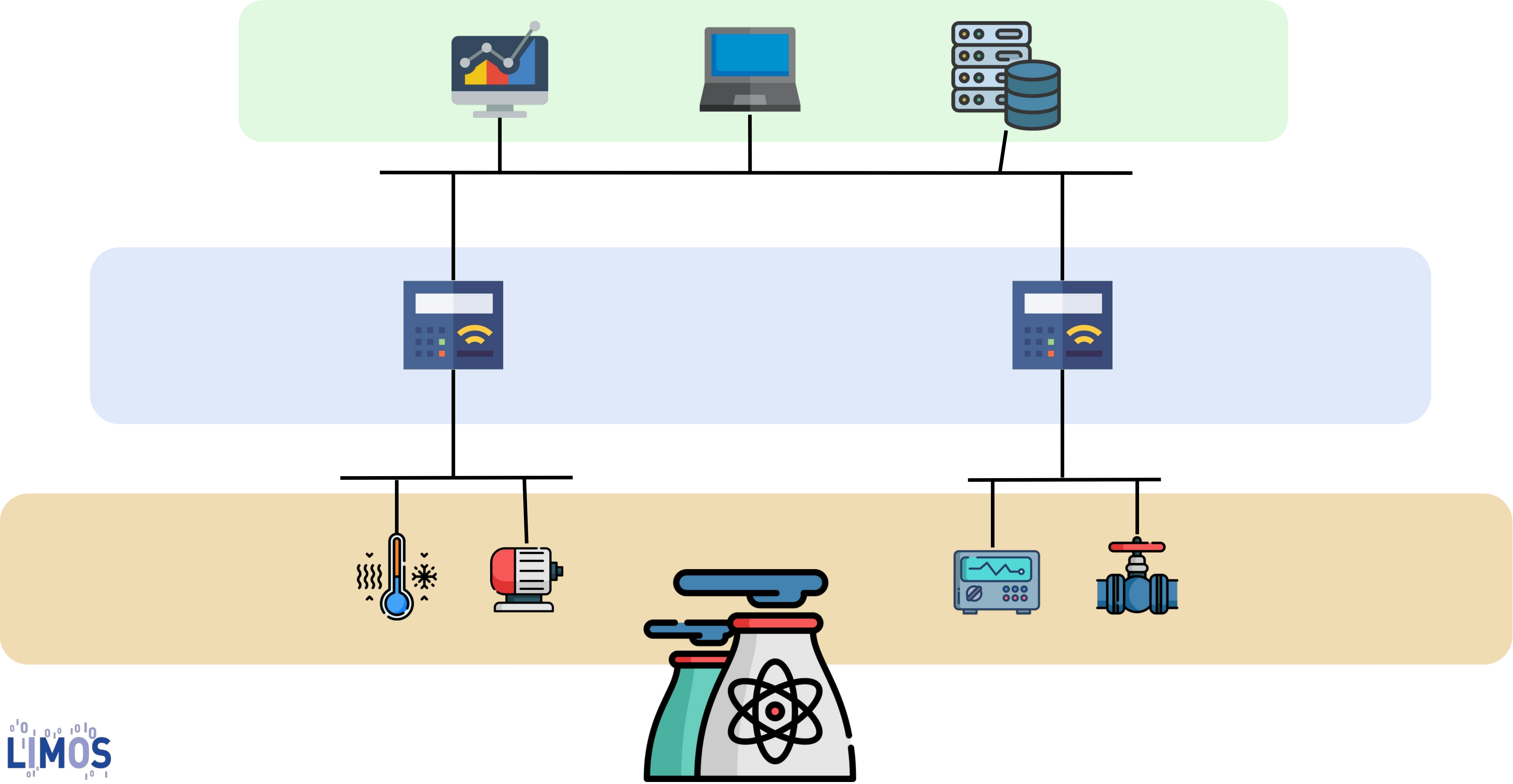
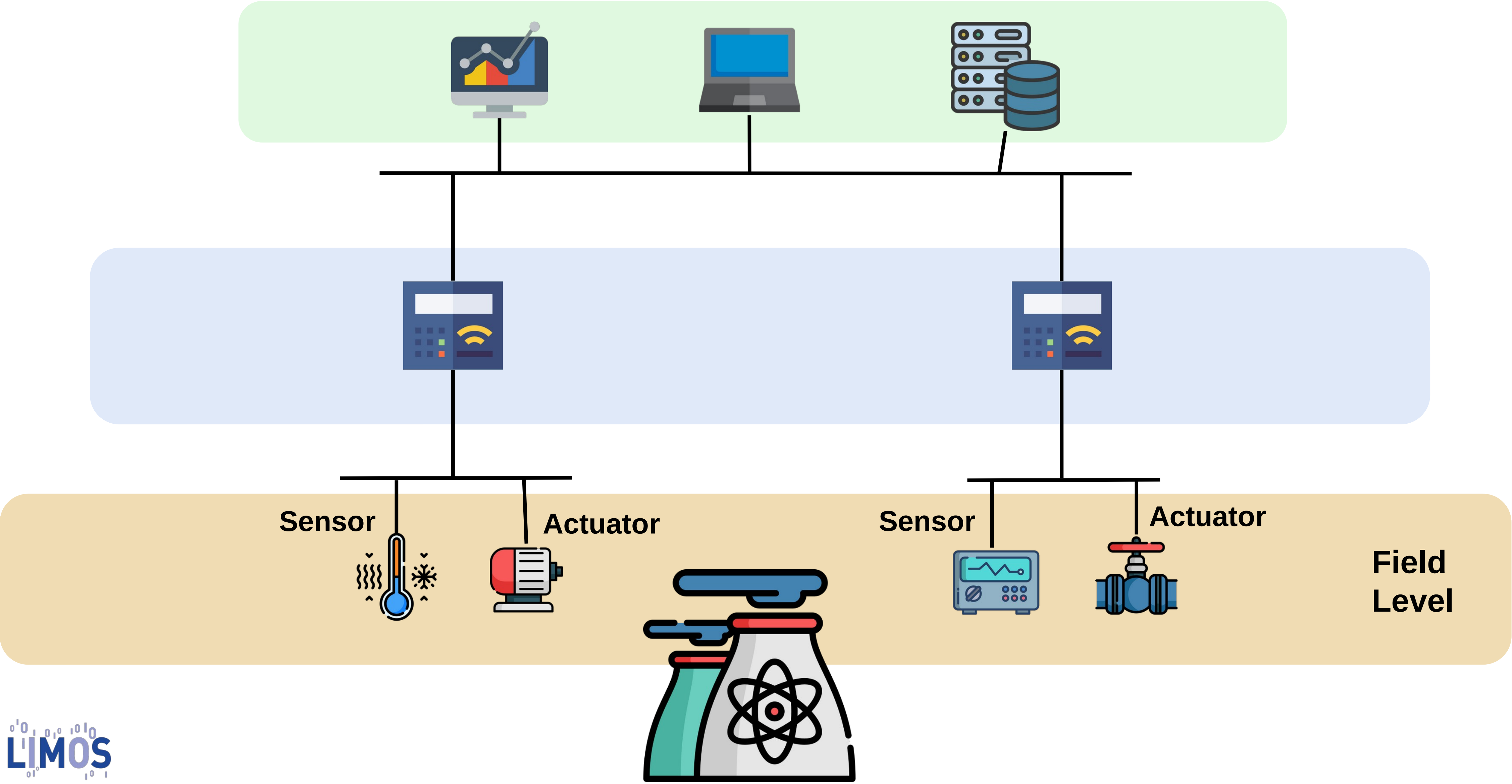

Massive IoT
Critical IoT
Smart building
Logistics, tracking and fleet management
Capillary networks
Smart agriculture
Smart metering
Remote health care
Traffic safety and control
Remote manufacturing, training, surgery
Smart grid automation
Industrial application and control
Low cost, low energy, small data volumes, massive numbers
Ultra reliable, very low latency, very high availability

Figure: [Alq19]

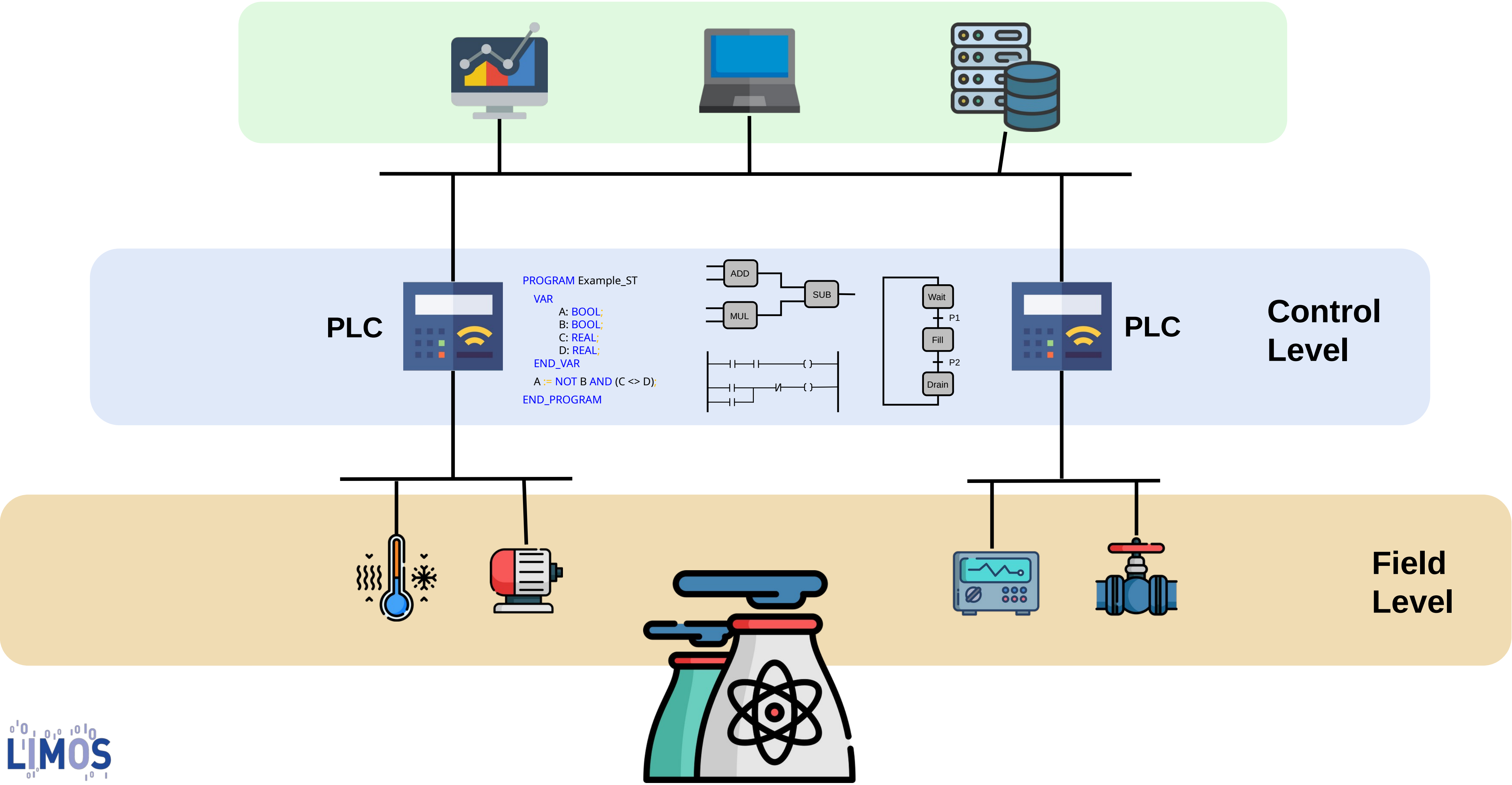
Context



Context



Context



PLC

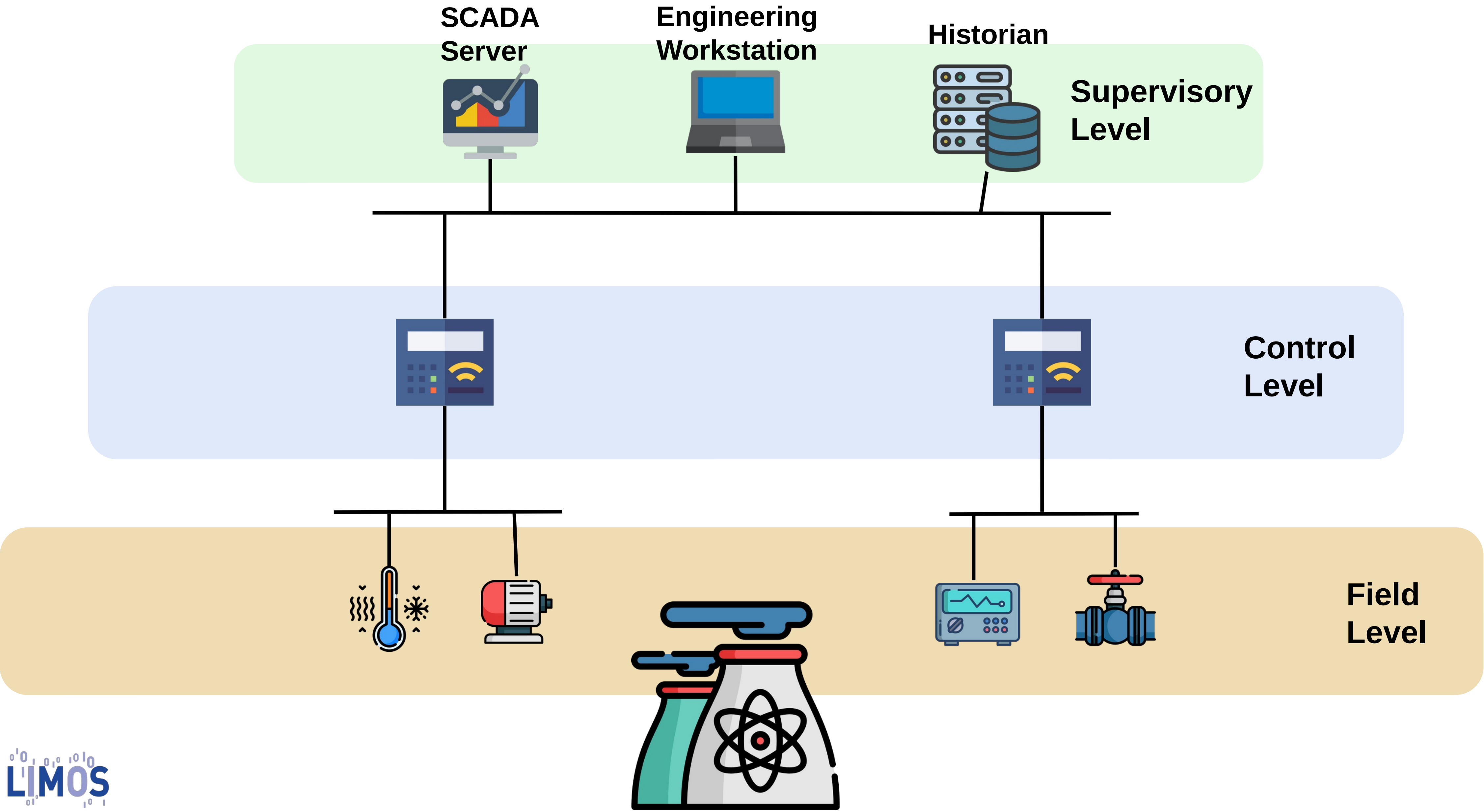
```
PROGRAM Example_ST
  VAR
      A: BOOL;
      B: BOOL;
      C: REAL;
      D: REAL;
  END_VAR
  A := NOT B AND (C <> D);
END_PROGRAM
```

PLC

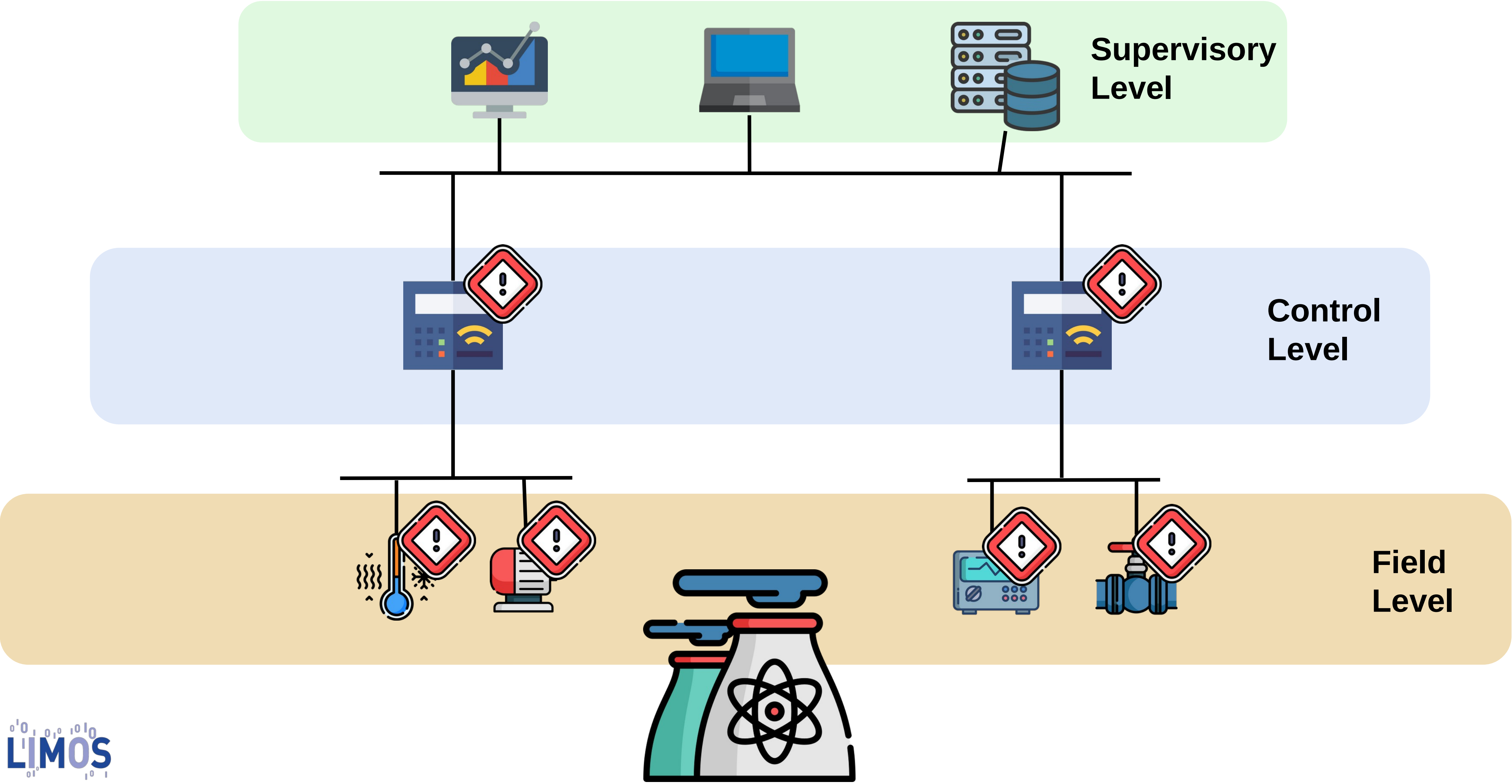
Control Level

Field Level

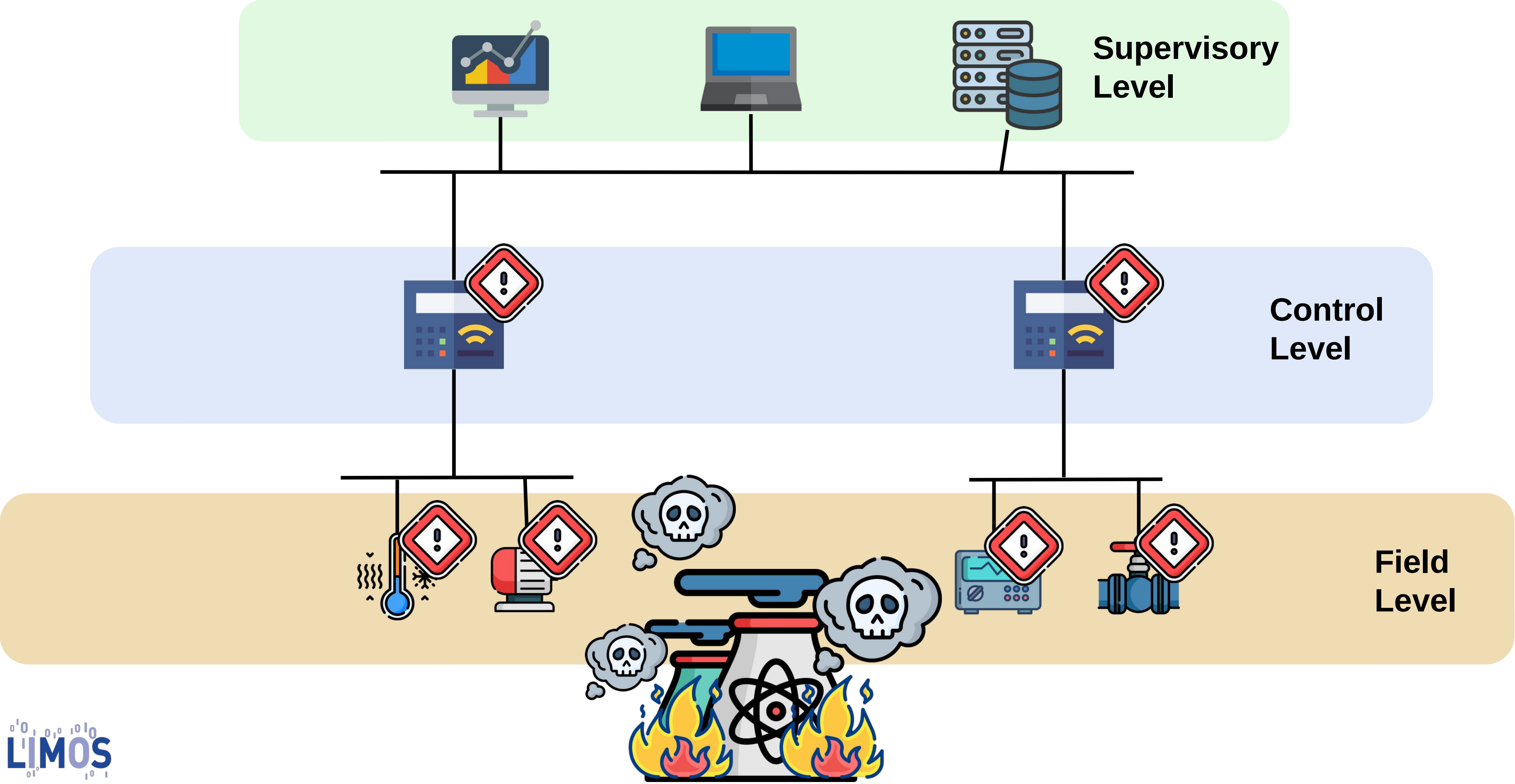
Context


SCADA Server
Engineering Workstation
Historian
Supervisory Level
Control Level
Field Level

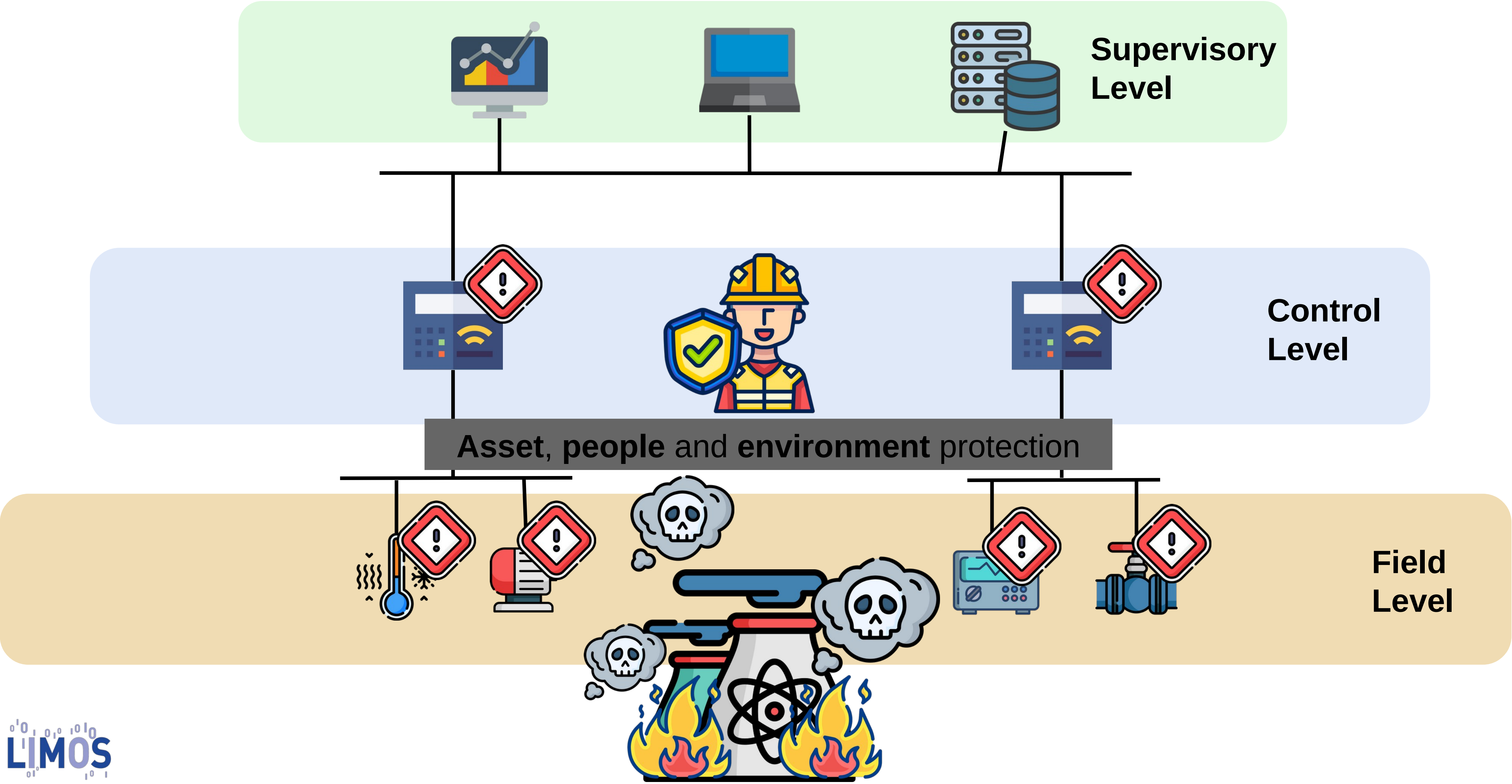
Context



Context



Context



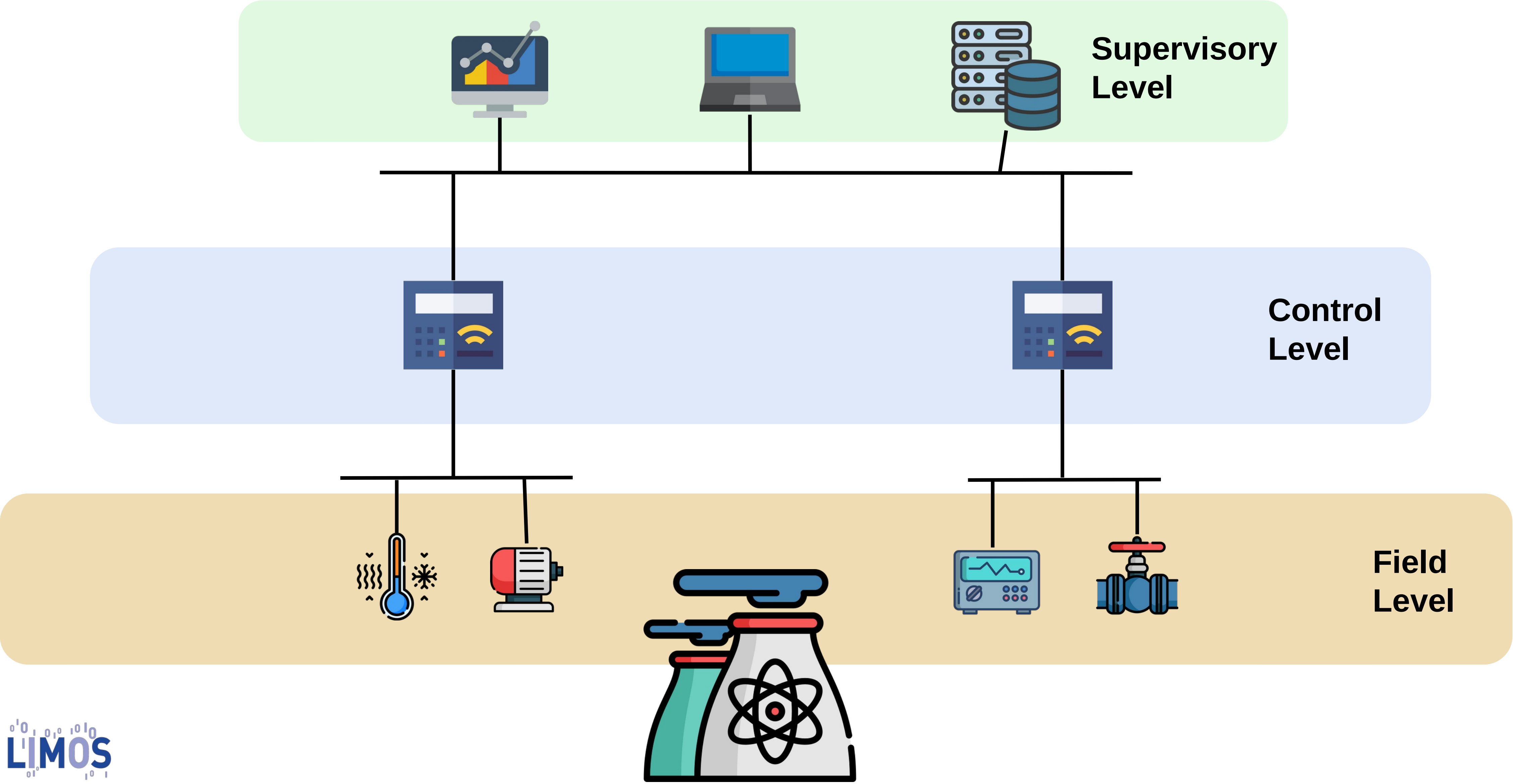
Supervisory Level

Control Level

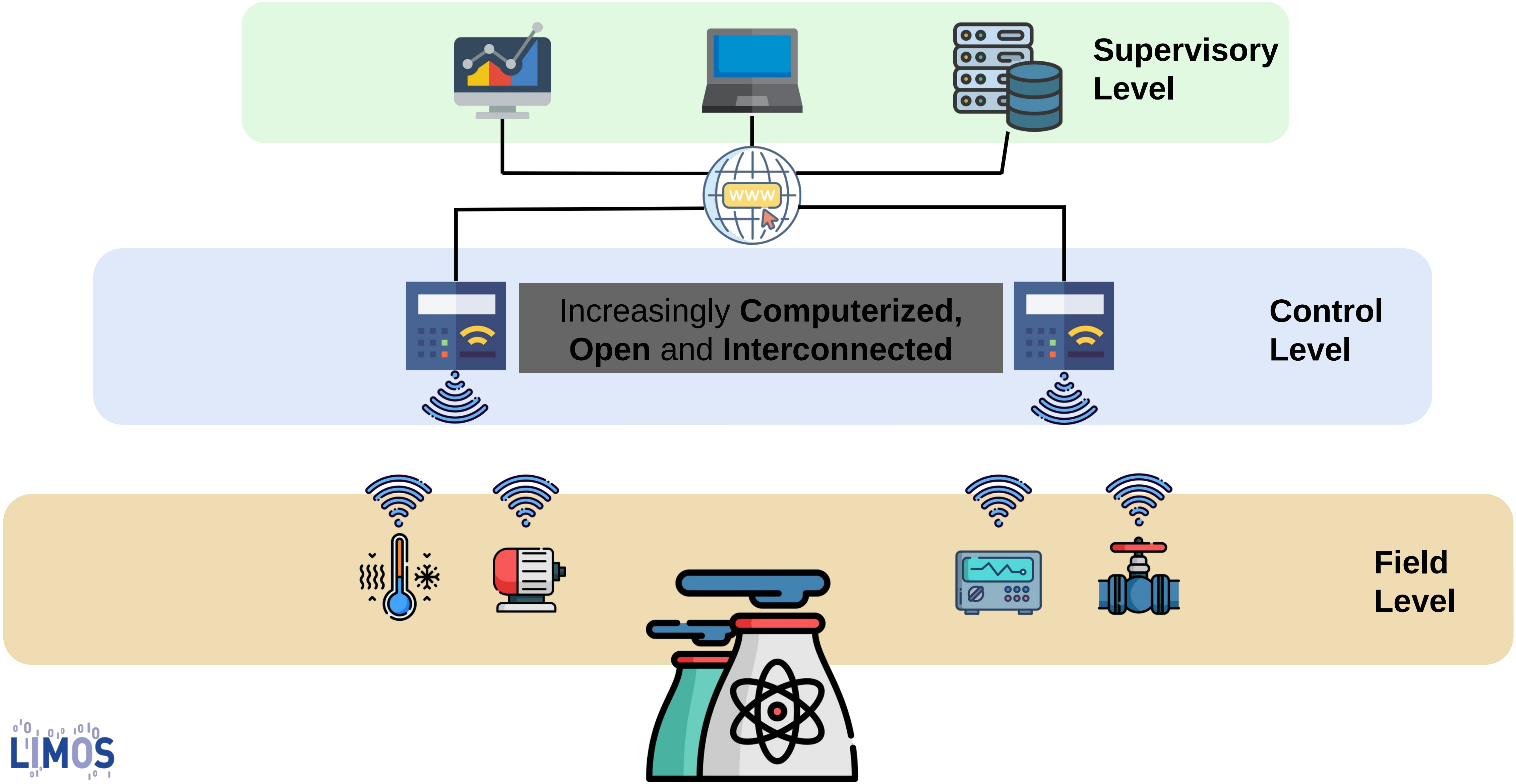
Asset, **people** and **environment** protection

Field Level

Context

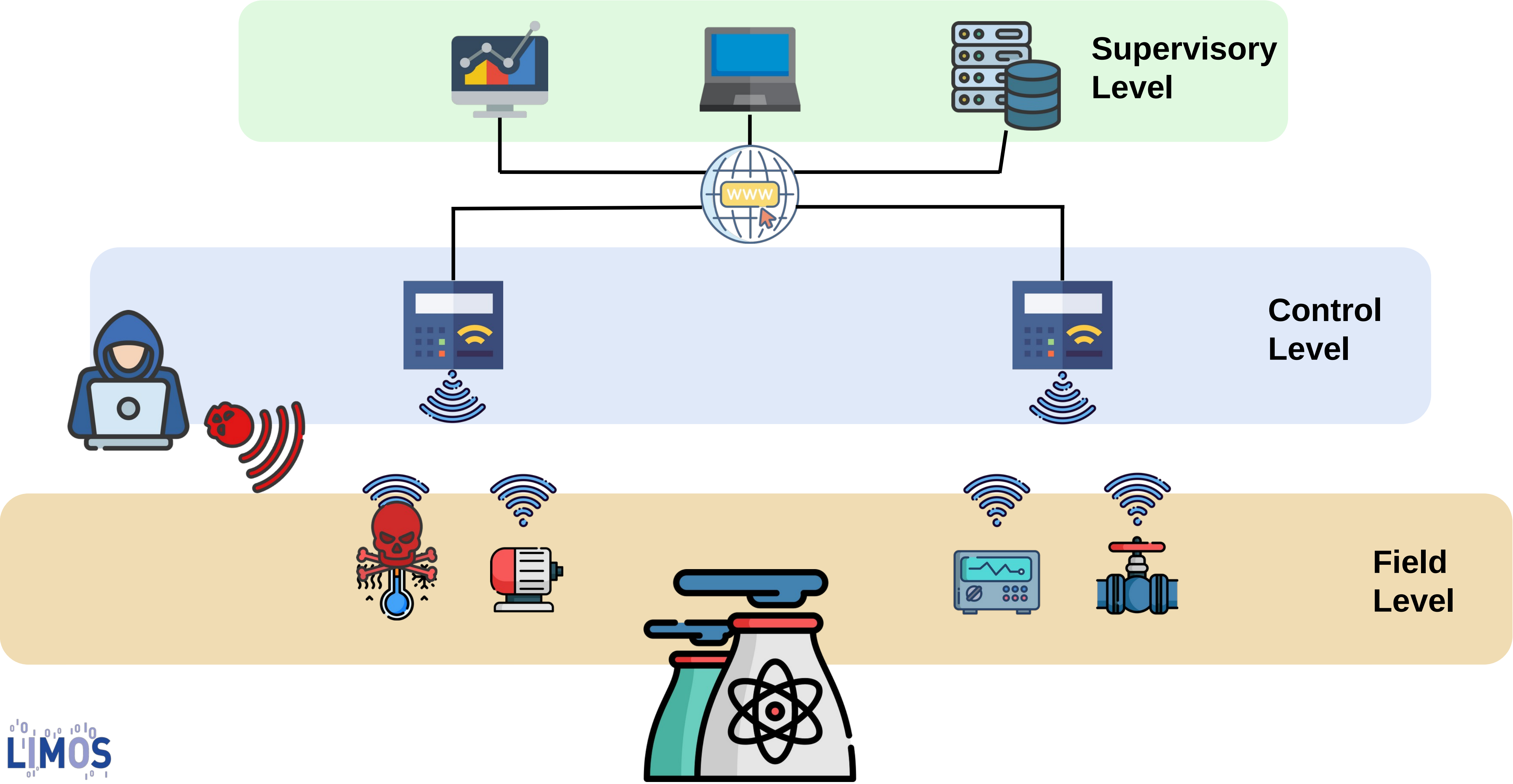


Context

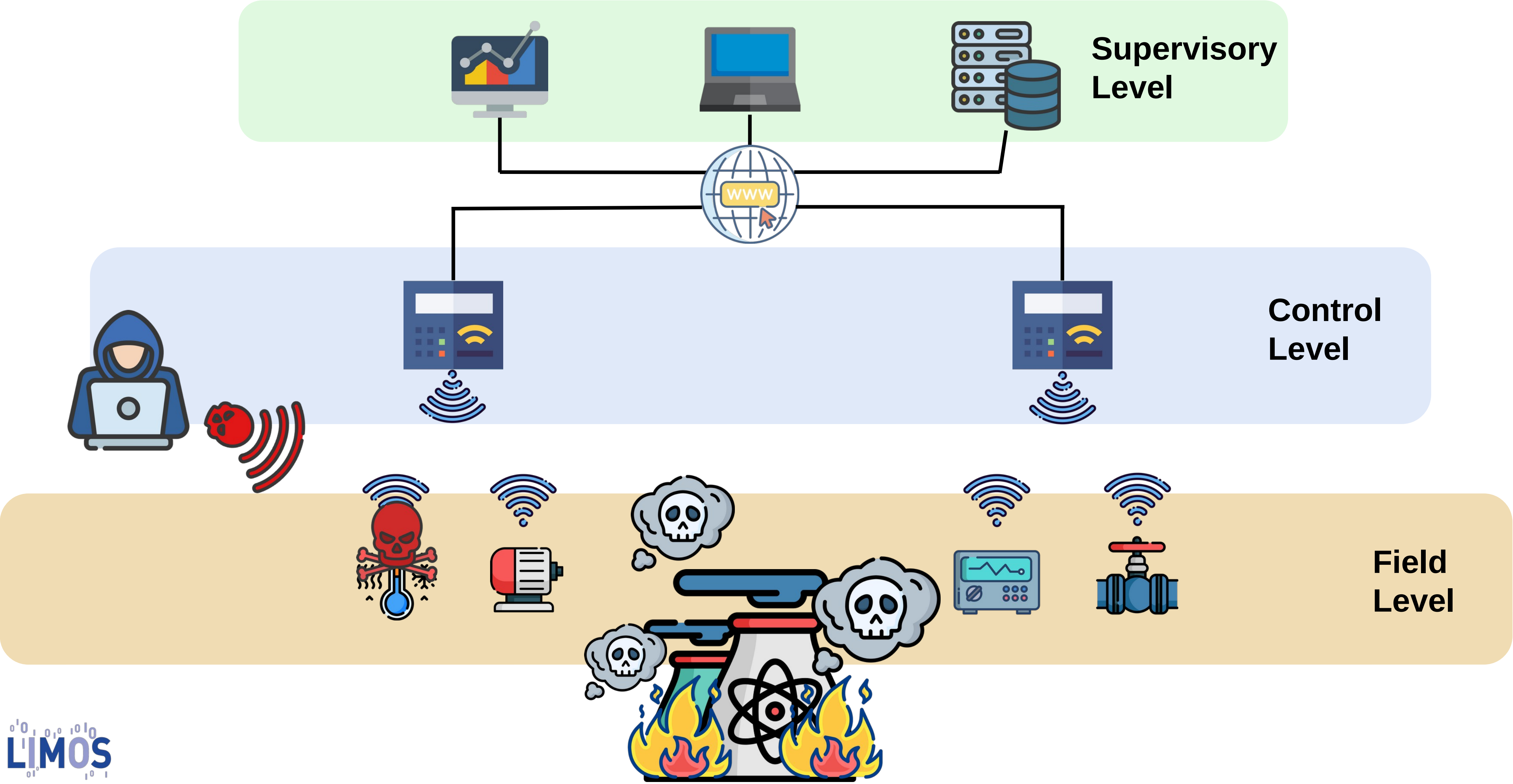


Increasingly **Computerized,**
Open and **Interconnected**

Context

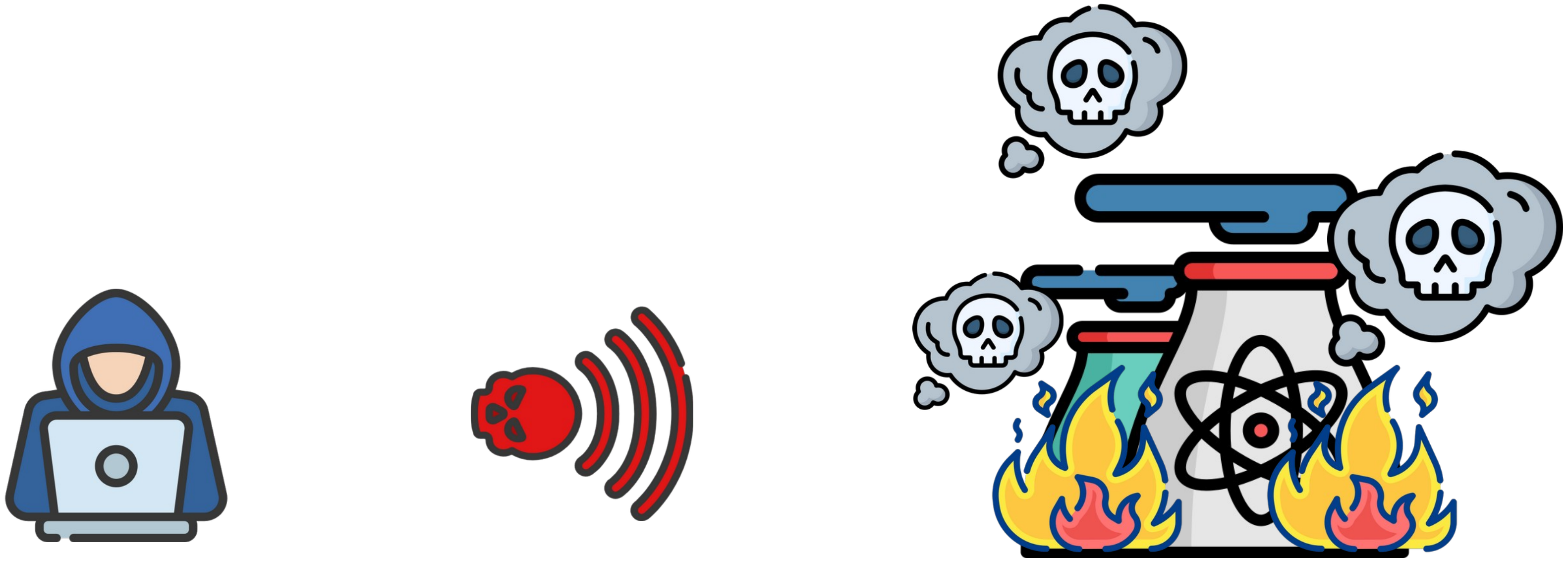


Context



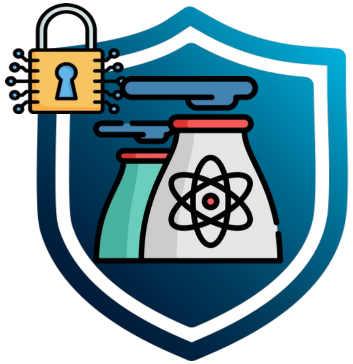
Goal

How to Identify Cyberattacks that Compromise System Safety



Goal

How to **Identify** **Cyberattacks** that Compromise System **Safety**



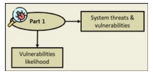
Protection against (cyber)**interference** with the proper and intended system **operation**[1]

Asset, **people** and **environment** protection against process **hazards**

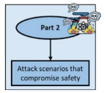
[1] IEC 62443-1-1. Industrial communication networks – Network and system security – Part 1-1 : Terminology, concepts and models.

Contents

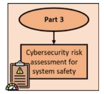
Cybersecurity Risk Assessment for System Safety



What an attacker can do



What an attacker might do



Is it serious ?

Literature Review & Classification

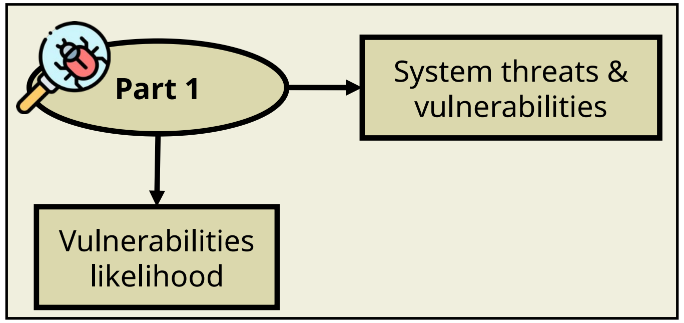
Identifying Cybersecurity Risk for System Safety

PLC-Logic Based Cybersecurity Risk Identification

Conclusion and perspectives

Cybersecurity risk assessment for system safety

What an attacker can do



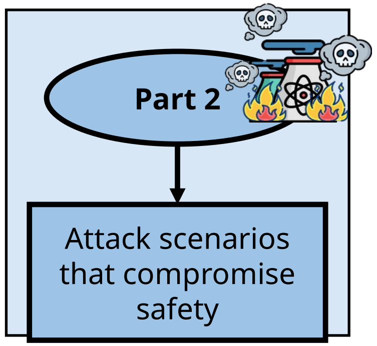
Part 1

System threats & vulnerabilities

Vulnerabilities likelihood

Threat modeling tool

What an attacker might do

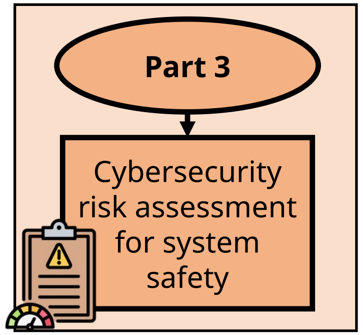


Part 2

Attack scenarios that compromise safety

Attack scenarios

Is it serious?



Part 3

Cybersecurity risk assessment for system safety

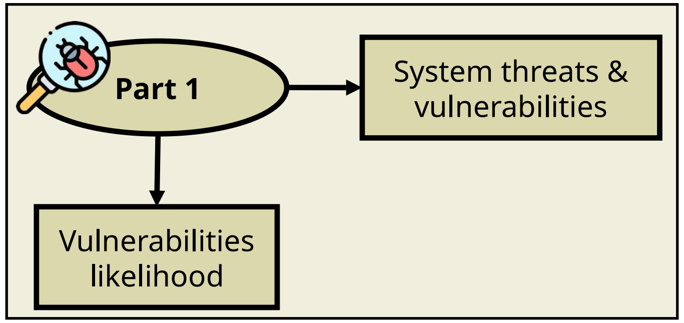
Risk matrix

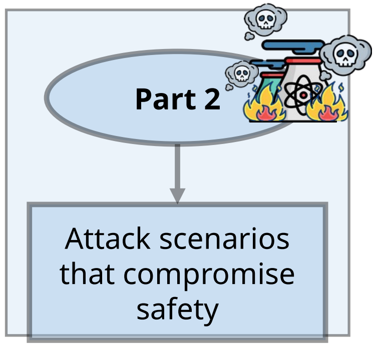
Cybersecurity risk assessment for system safety

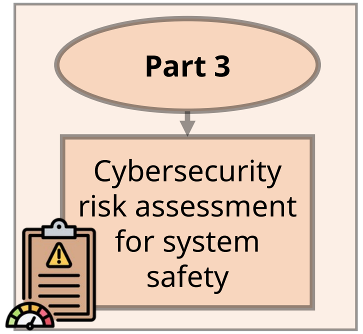
What an attacker can do

What an attacker must do

Is it serious?



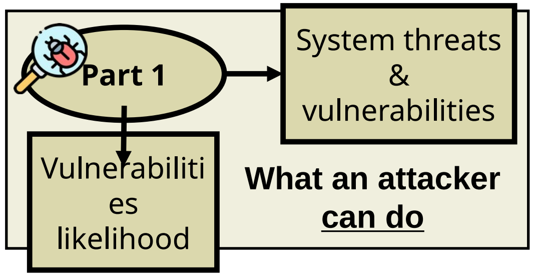




Threat modeling tool

Attack scenarios

Risk matrix



Part 1

System threats & vulnerabilities

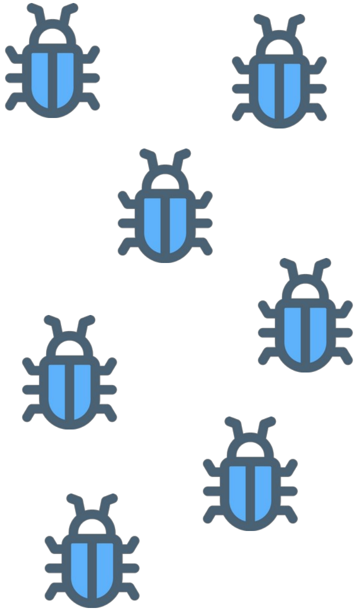
Vulnerabilities likelihood

What an attacker can do

Threat modeling

An attacker

Vulnerabilities



Threats

S

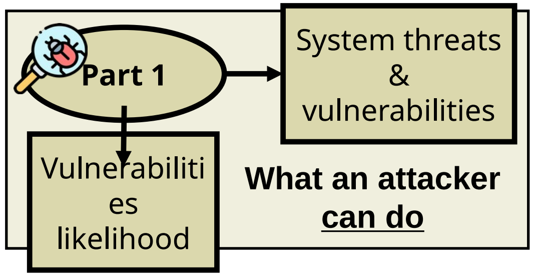
T

R

I

D

E



Part 1

System threats & vulnerabilities

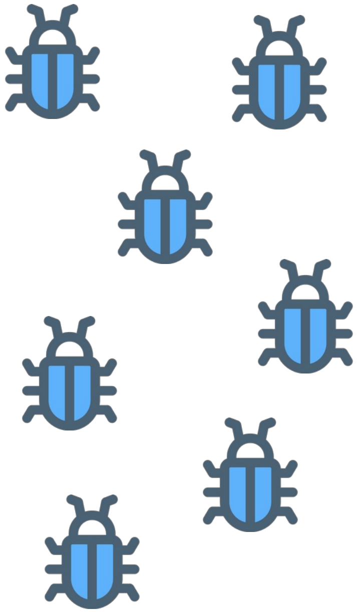
Vulnerabilities likelihood

What an attacker can do

Threat modeling

An attacker

Vulnerabilities



Threats

Spoofing

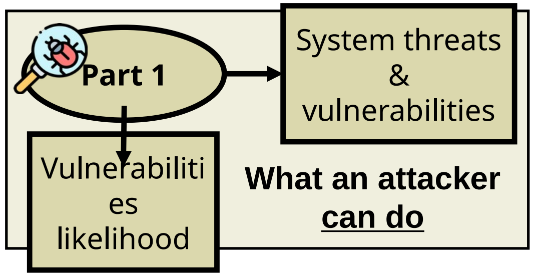
Tampering

Repudiation

Information disclosure

Denial of service

Elevation of privilege



What an attacker can do

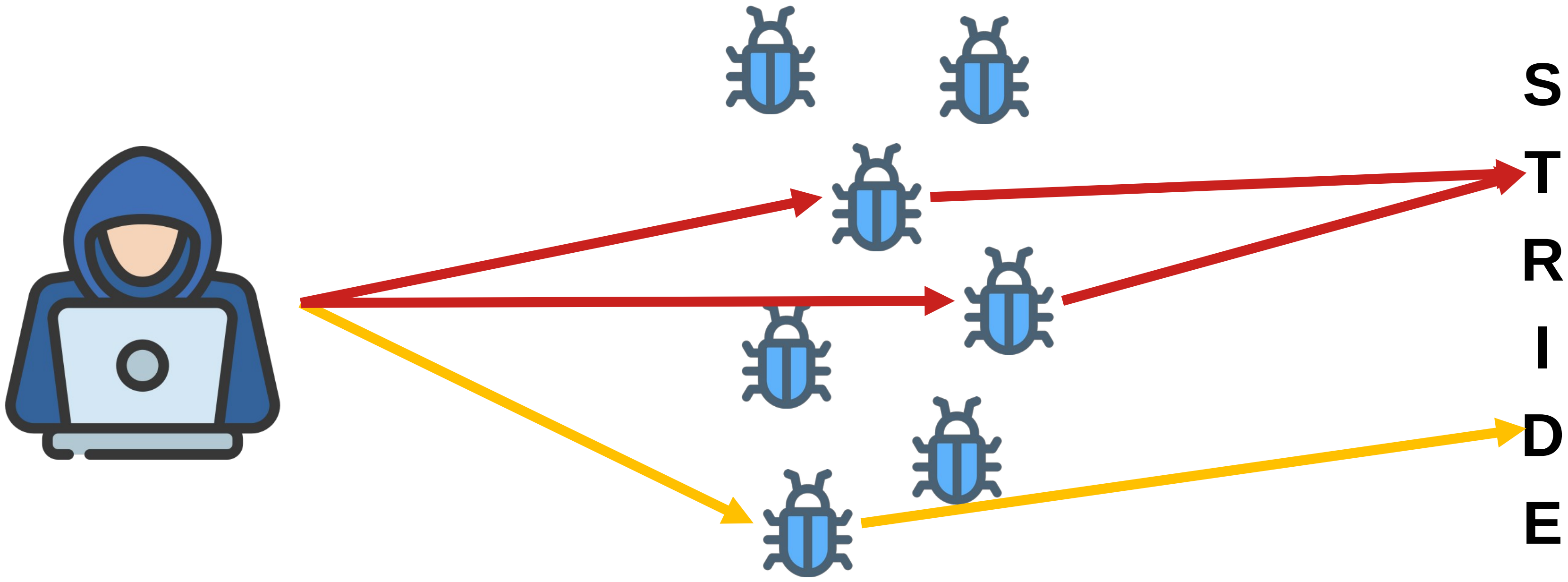
Threat modeling

Cyberattack

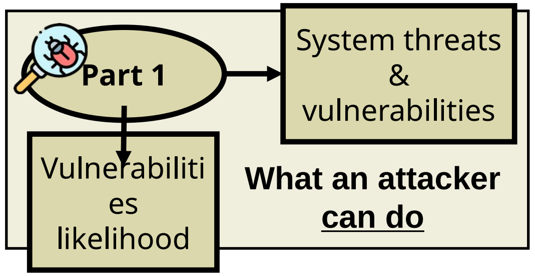
An attacker

Vulnerabilities

Threats



S
T
R
I
D
E



Part 1

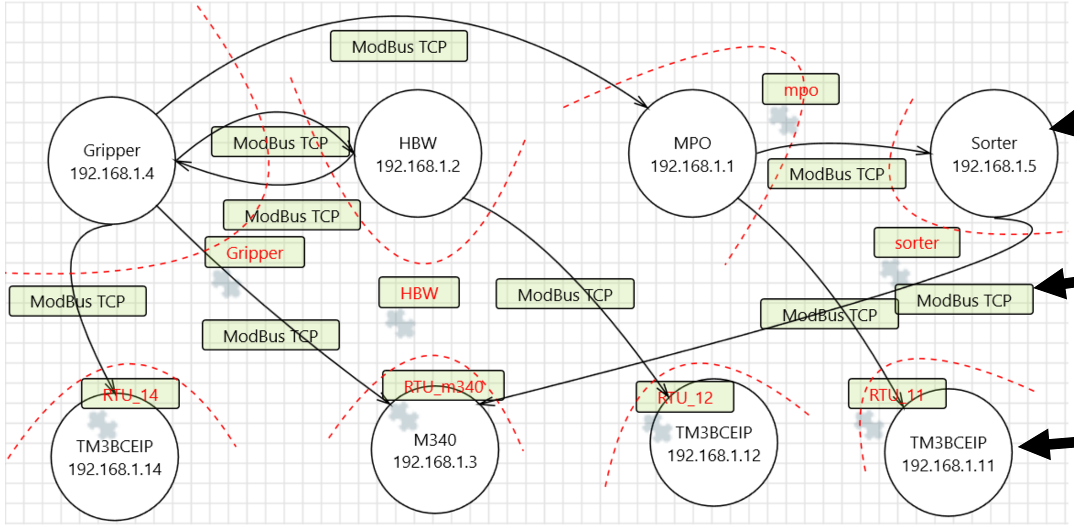
System threats & vulnerabilities

Vulnerabilities likelihood

What an attacker **can do**

Threat modeling

System model



Threats

?

?

?

S 🐞🐞🐞

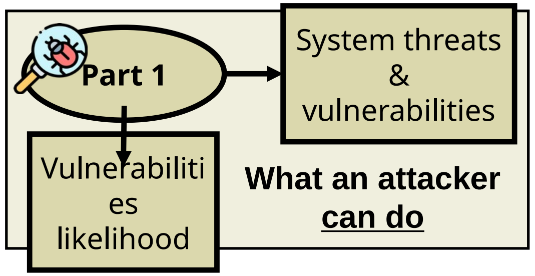
T 🐞🐞🐞🐞

R 🐞

I 🐞🐞🐞

D 🐞🐞

E 🐞🐞🐞🐞🐞



Part 1

System threats & vulnerabilities

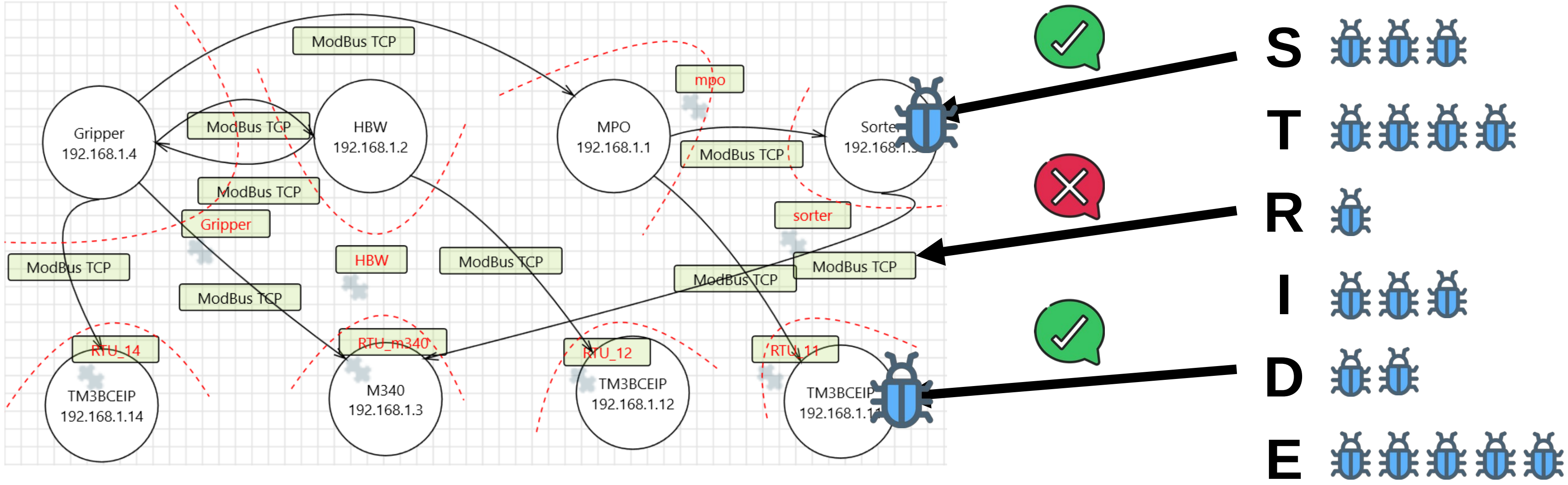
Vulnerabilities likelihood

What an attacker can do

Threat modeling

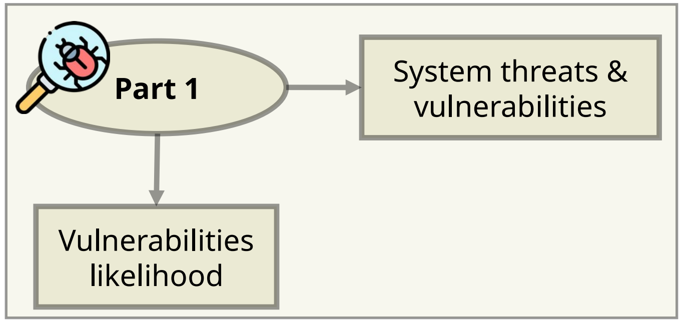
System model

Threats



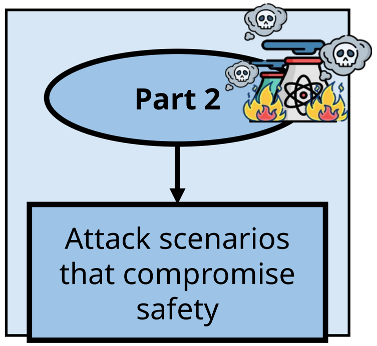
Cybersecurity risk assessment for system safety

What an attacker can do



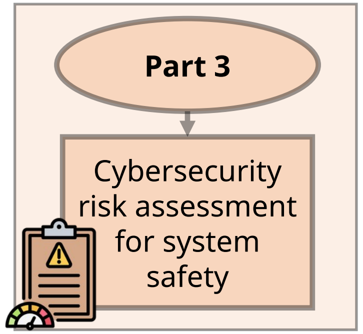
Threat modeling tool

What an attacker might do

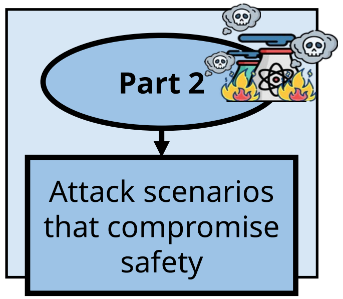


Attack scenarios

Is it serious?



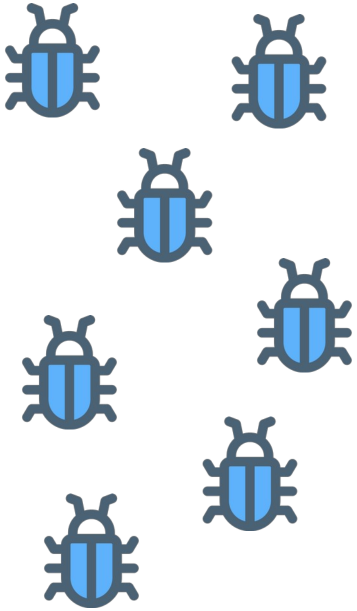
Risk matrix



Attack scenarios

An attacker

Vulnerabilities



Threats

S

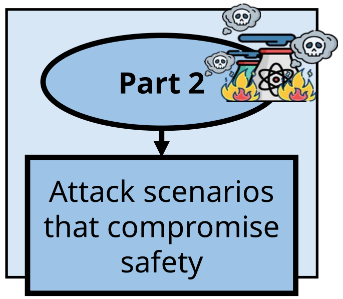
T

R

I

D

E



Part 2

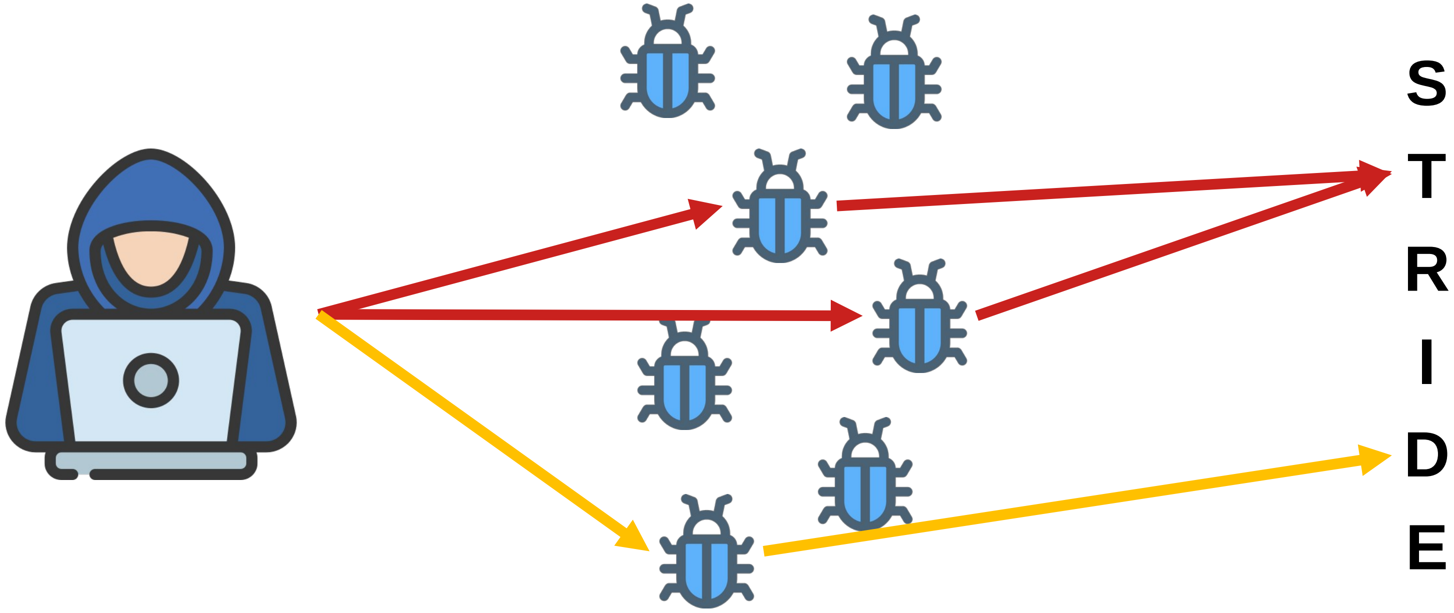
Attack scenarios that compromise safety

Attack scenarios

An attacker

Vulnerabilities

Threats



S

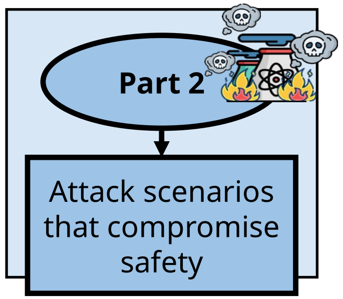
T

R

I

D

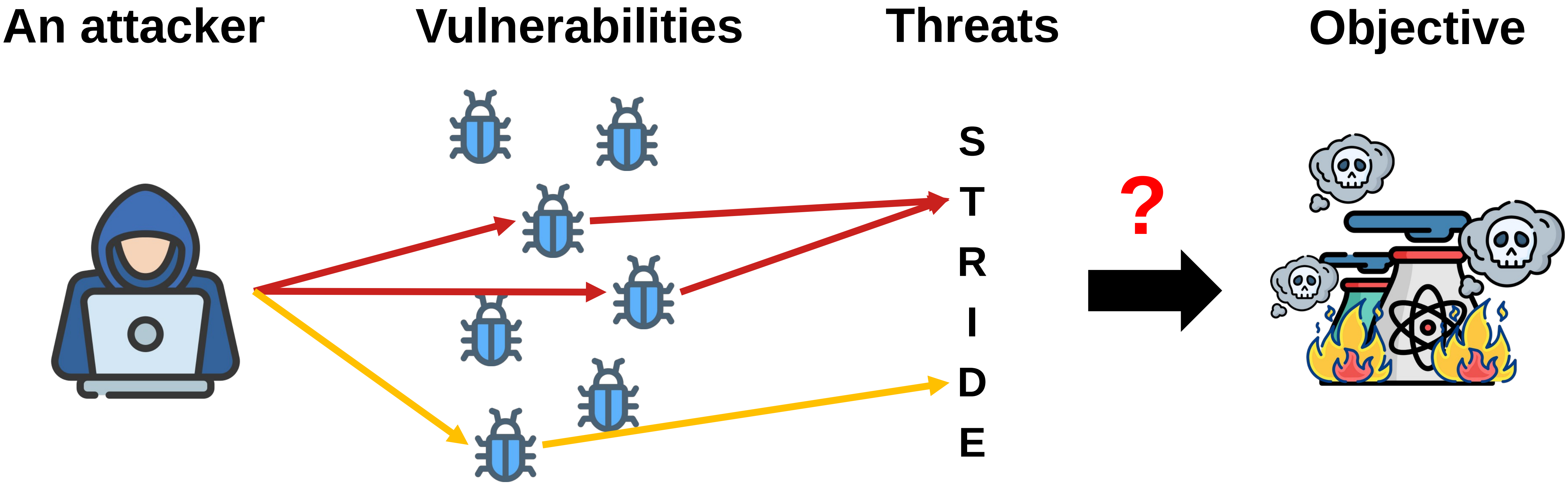
E



Part 2

Attack scenarios that compromise safety

Attack scenarios



An attacker

Vulnerabilities

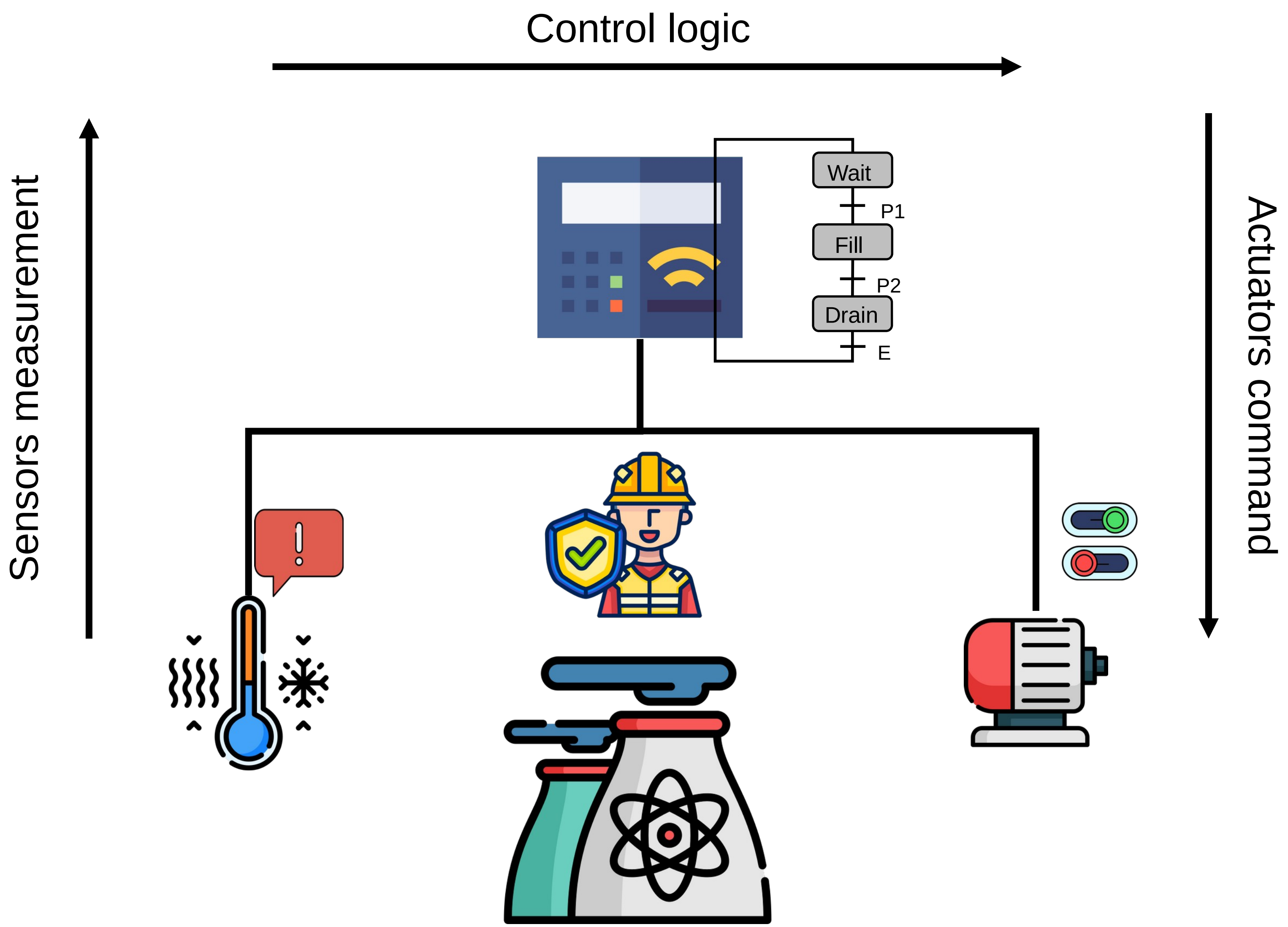
Threats

Objective

S
T
R
I
D
E

?

Control loop



Control logic

Sensors measurement

Actuators command

Wait

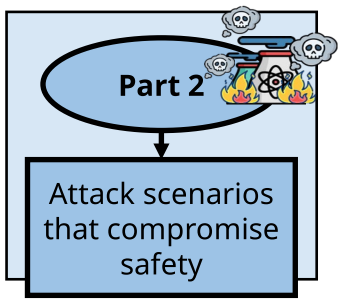
P1

Fill

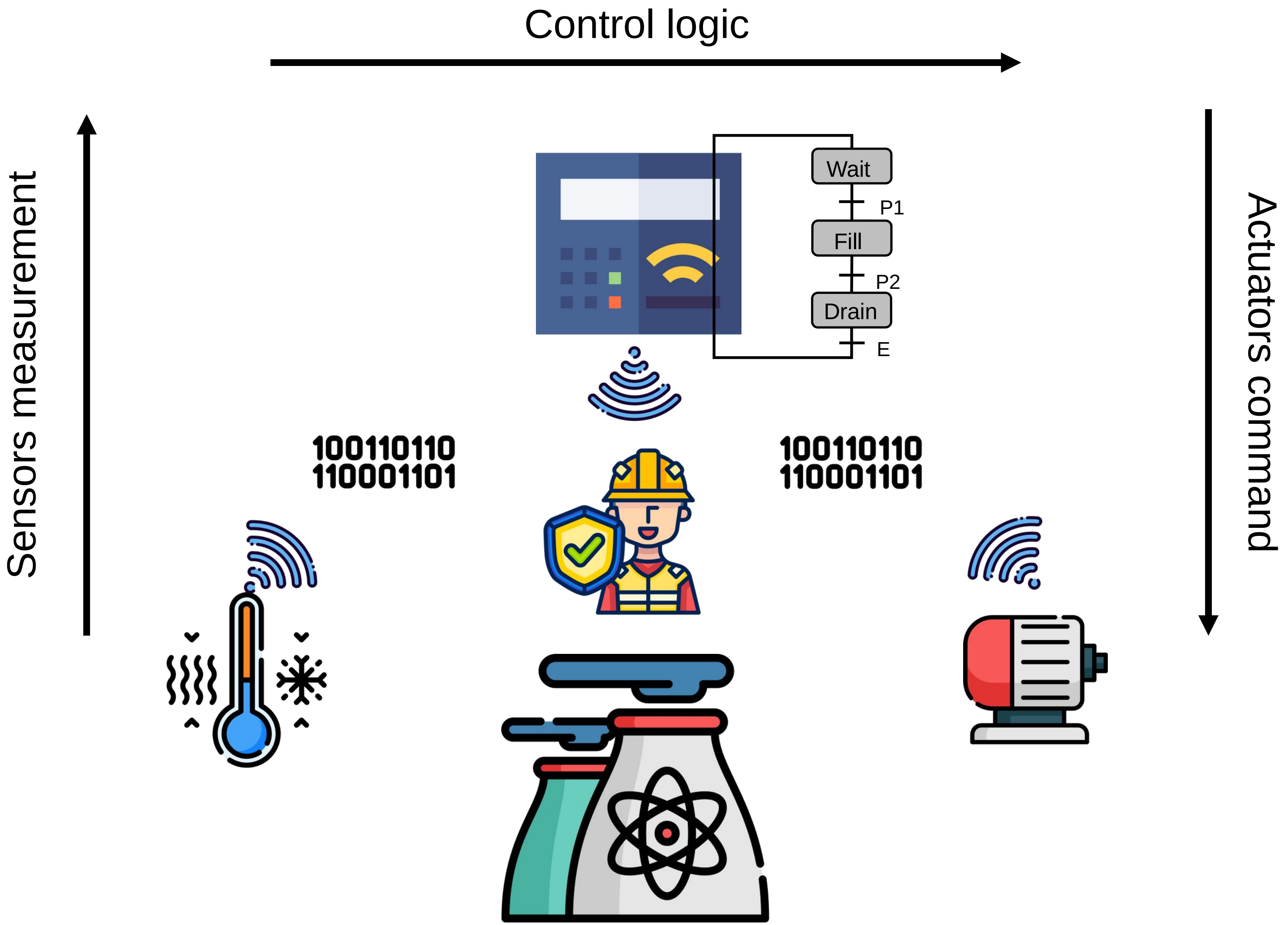
P2

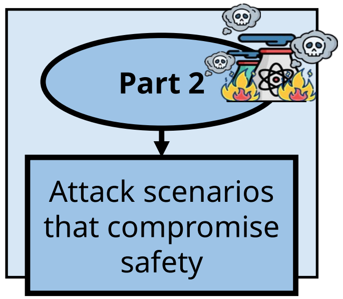
Drain

E

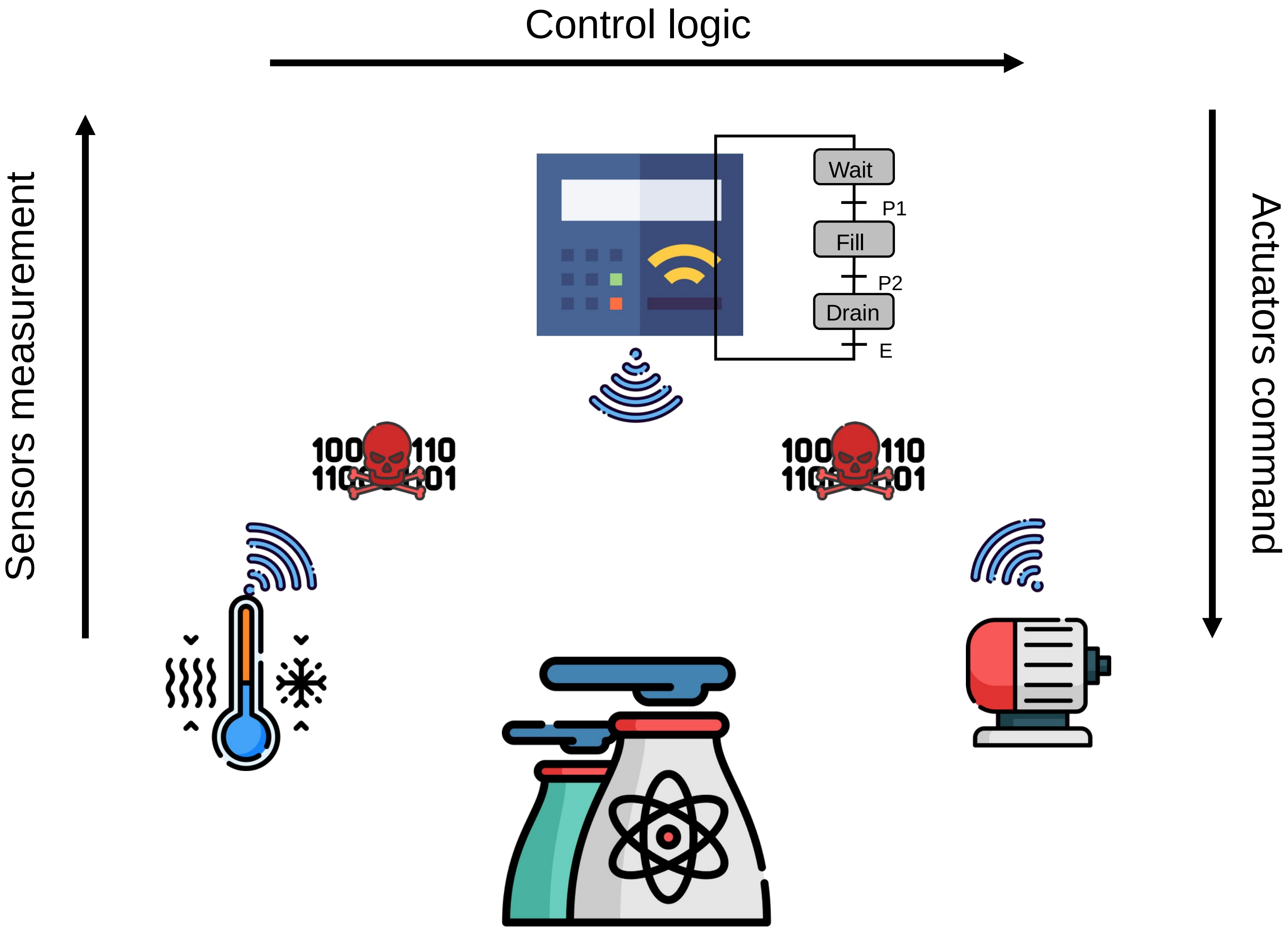


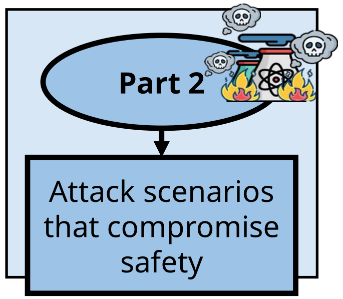
Attack scenarios



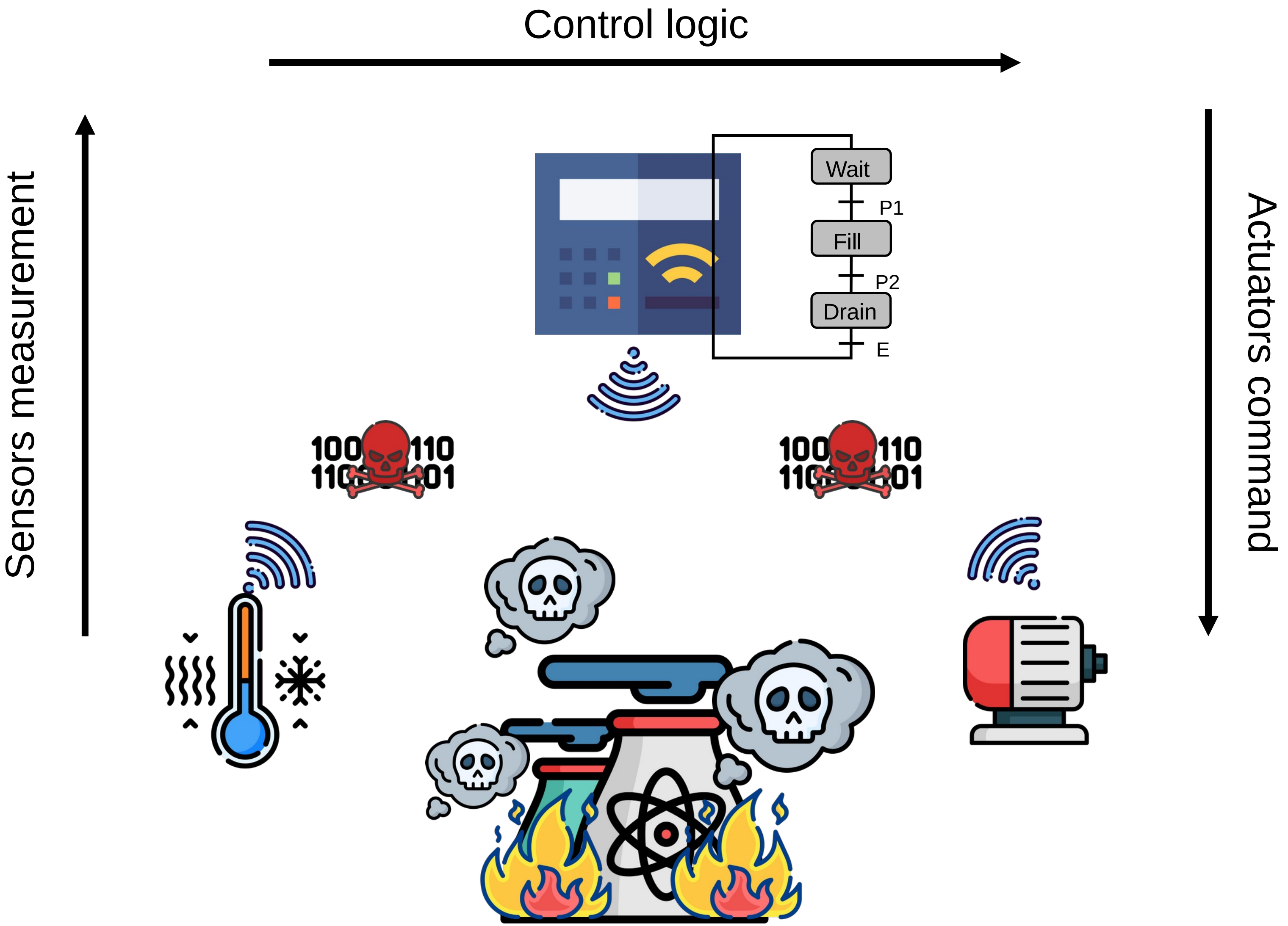


Attack scenarios





Attack scenarios

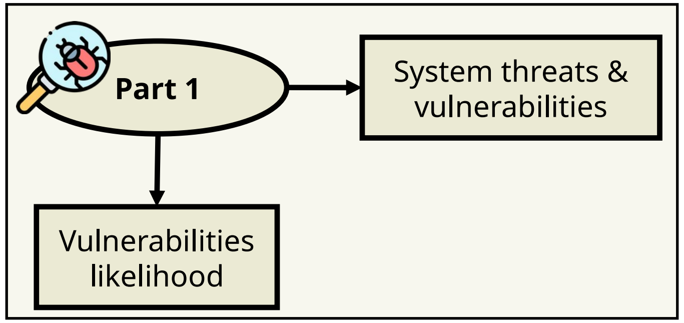


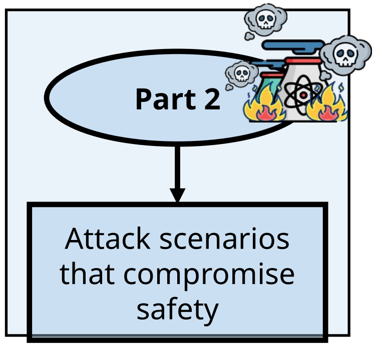
Cybersecurity risk assessment for system safety

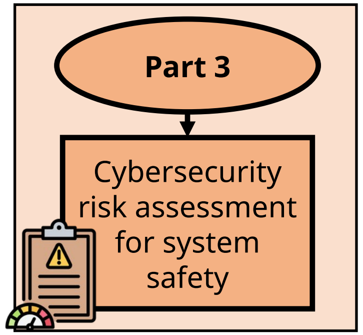
What an attacker can do

What an attacker might do

Is it serious?







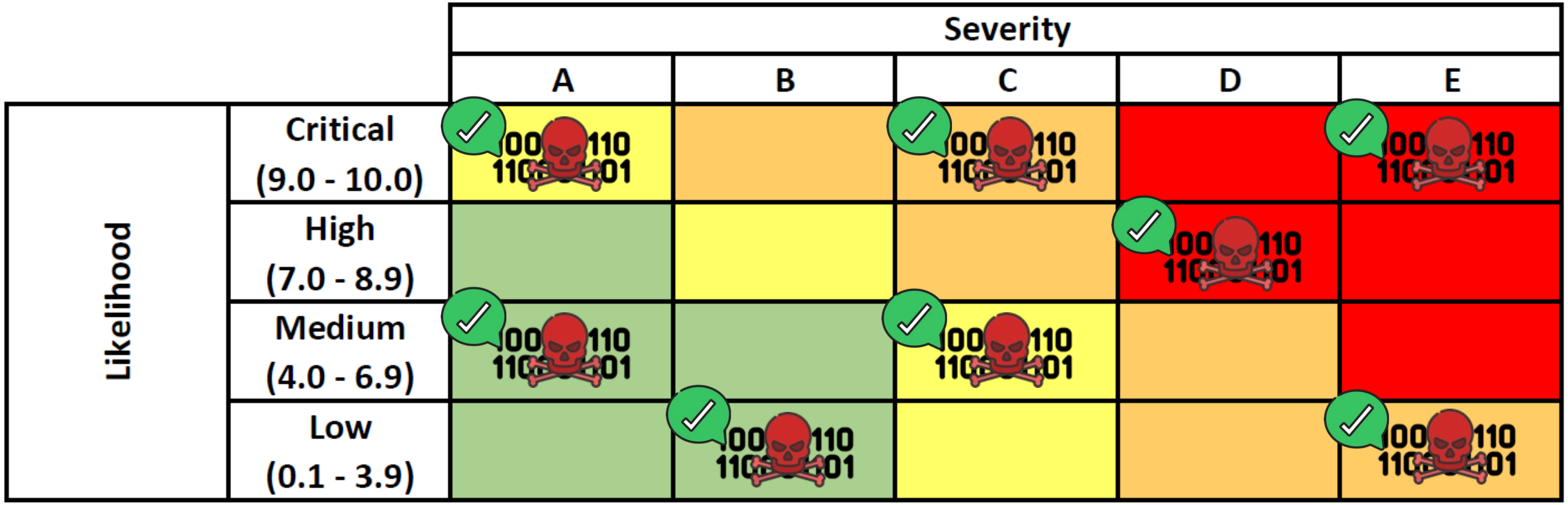
Threat modeling tool

Attack scenarios

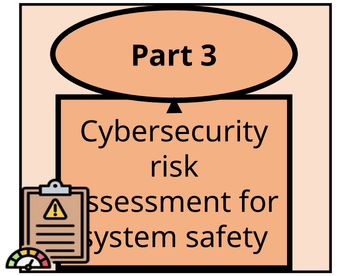
Risk matrix

Risk matrix

Standard **IEC 62443-3-2/ISO 31010 risk matrix**

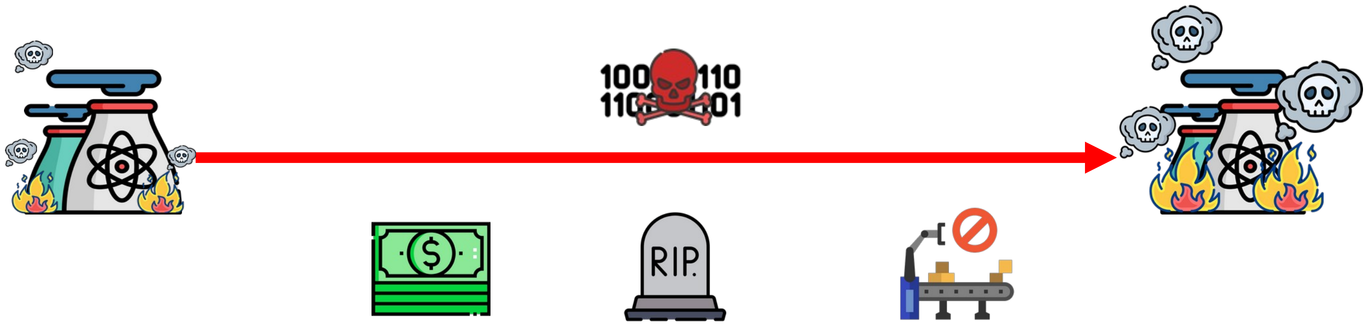


		Severity				
		A	B	C	D	E
Likelihood	Critical (9.0 - 10.0)	🟨 ✓ ☠	🟧	🟧 ✓ ☠	🟥	🟥 ✓ ☠
	High (7.0 - 8.9)	🟩	🟨	🟧	🟥 ✓ ☠	🟥
	Medium (4.0 - 6.9)	🟩 ✓ ☠	🟩	🟨 ✓ ☠	🟧	🟥
	Low (0.1 - 3.9)	🟩	🟩 ✓ ☠	🟨	🟧	🟧 ✓ ☠



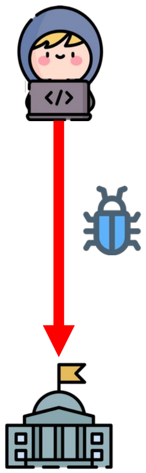
Risk matrix

Safety expert



Exploitability score (CVSS 3.1)

Easy

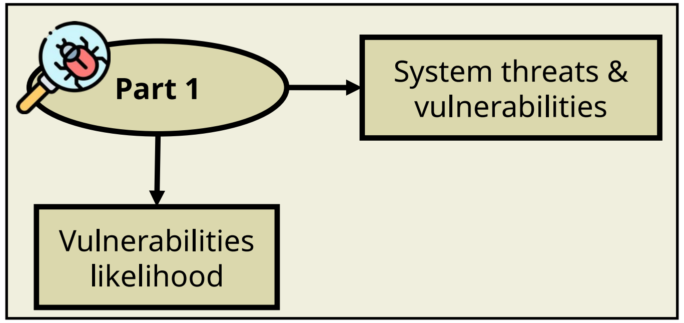


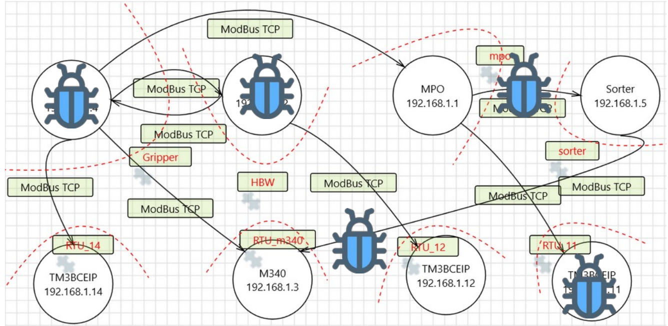
Hard

		Severity				
		A	B	C	D	E
Likelihood	Critical (9.0 - 10.0)	🟨 ✓	🟧	🟧 ✓	🟥	🟥 ✓
	High (7.0 - 8.9)	🟩	🟨	🟧	🟥 ✓	🟥
	Medium (4.0 - 6.9)	🟩 ✓	🟩	🟨 ✓	🟧	🟥
	Low (0.1 - 3.9)	🟩	🟩 ✓	🟨	🟧	🟧 ✓

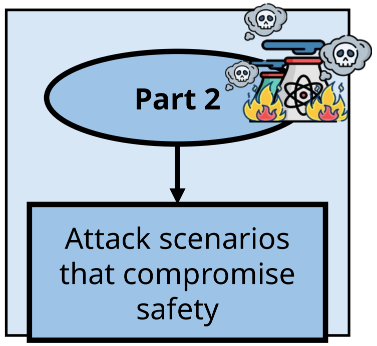
Cybersecurity risk assessment for system safety

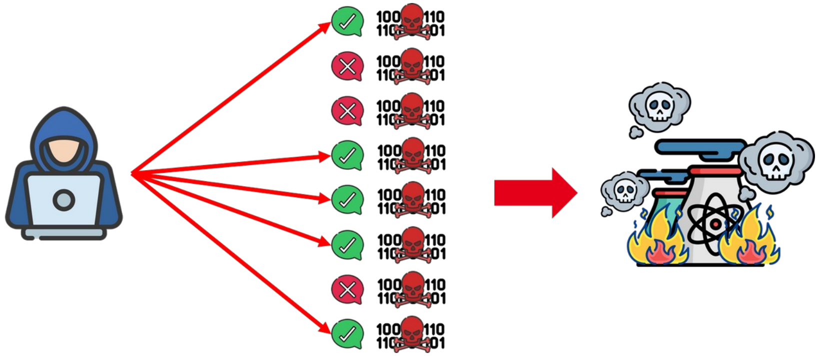
What an attacker can do



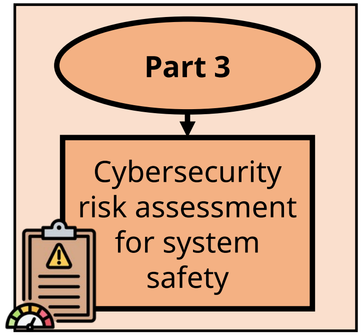


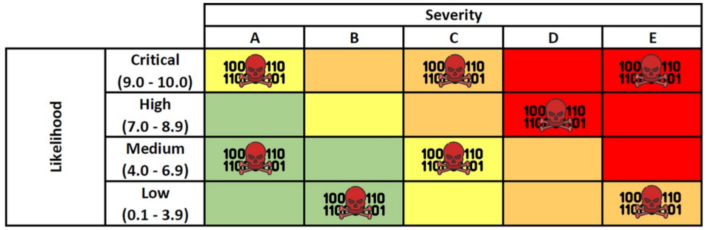
What an attacker might do





Is it serious?

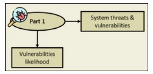




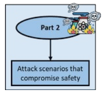
Likelihood		Severity				
		A	B	C	D	E
Likelihood	Critical (9.0 - 10.0)	🟨 100 110 110 01	🟧	🟧 100 110 110 01	🟥	🟥 100 110 110 01
	High (7.0 - 8.9)	🟩	🟨	🟧	🟥 100 110 110 01	🟥
	Medium (4.0 - 6.9)	🟩 100 110 110 01	🟩	🟧 100 110 110 01	🟧	🟥
	Low (0.1 - 3.9)	🟩	🟩 100 110 110 01	🟨	🟧	🟧 100 110 110 01

Contents

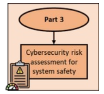
Cybersecurity Risk Assessment for System Safety



What an attacker can do



What an attacker might do



Is it serious ?

Literature Review & Classification

Identifying Cybersecurity Risk for System Safety

PLC-Logic Based Cybersecurity Risk Identification

Conclusion and perspectives

Literature Review & Classification

Unified

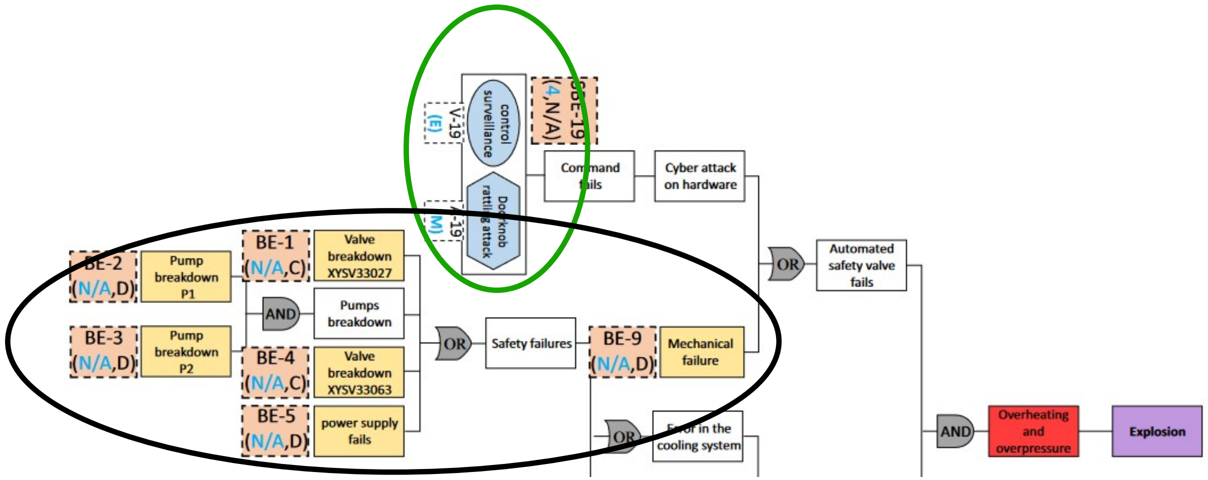
Integrated

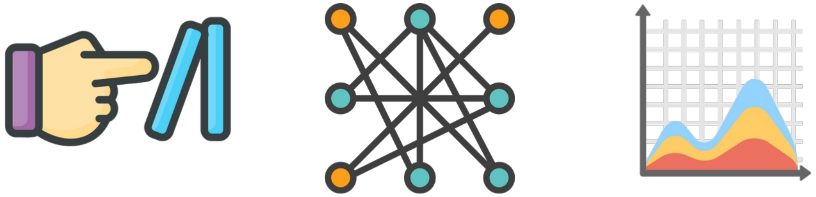
Literature Review & Classification

Unified

Integrated

→ Single method

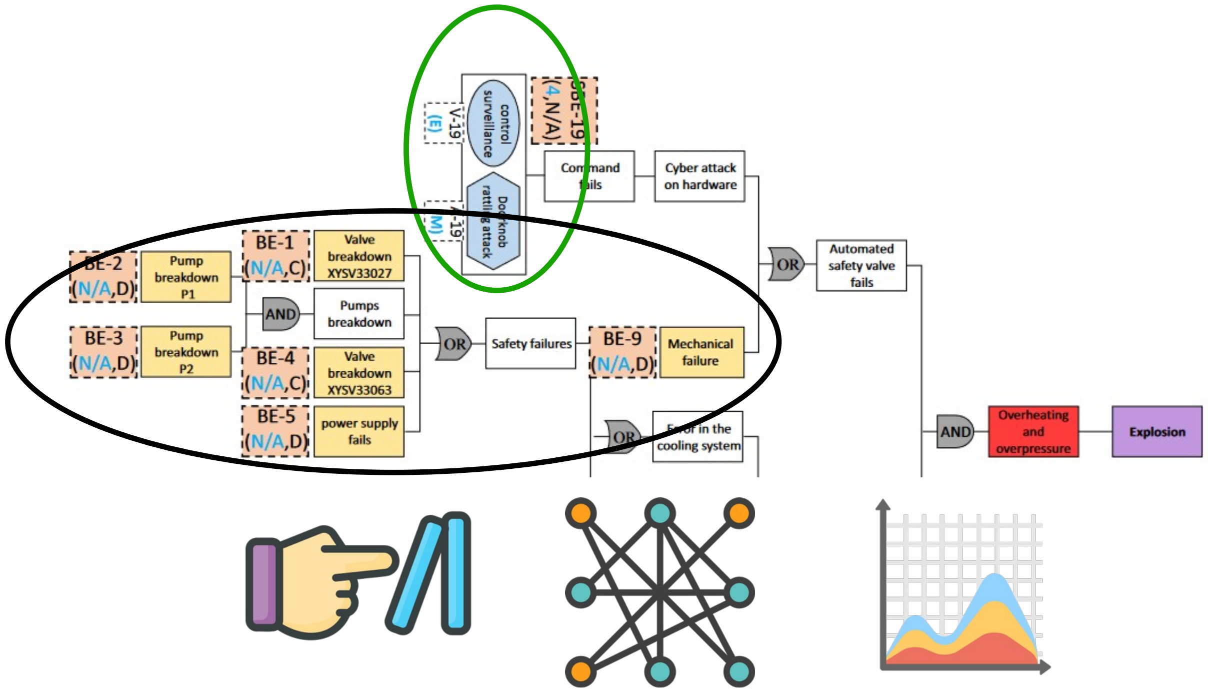




Literature Review & Classification

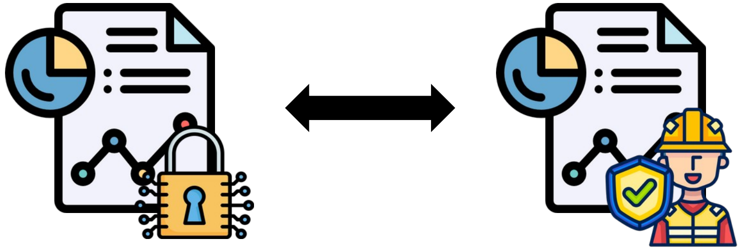
Unified

→ Single method



Integrated

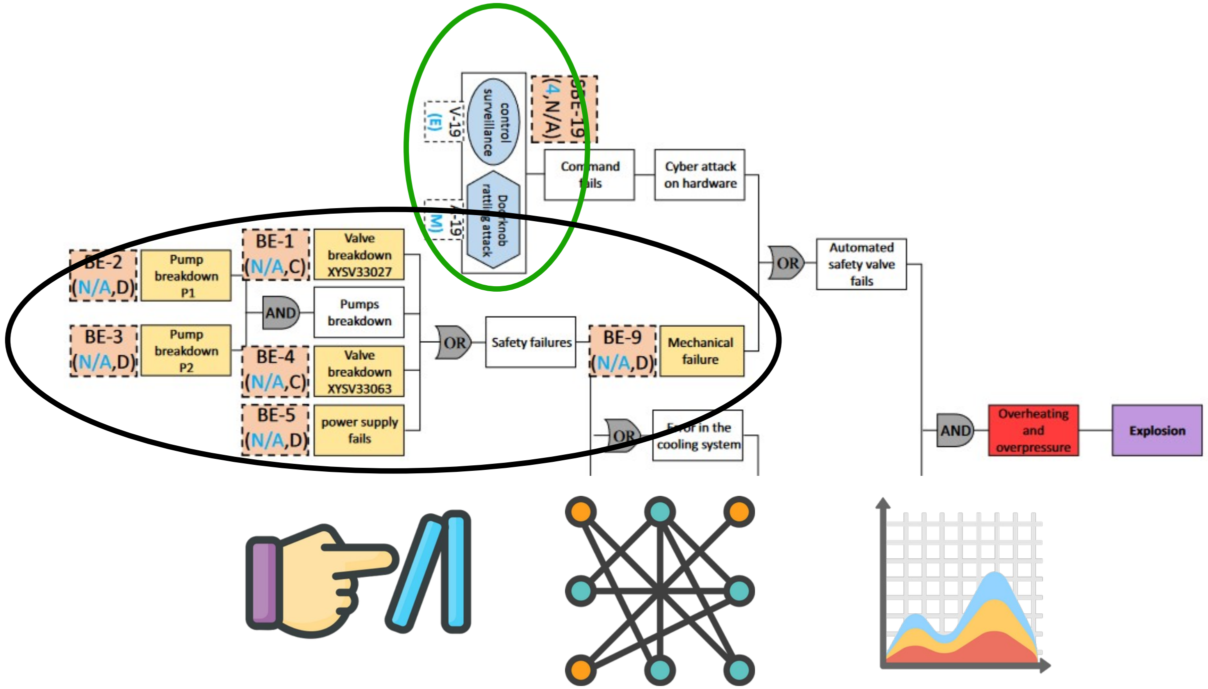
→ Separate method



Literature Review & Classification

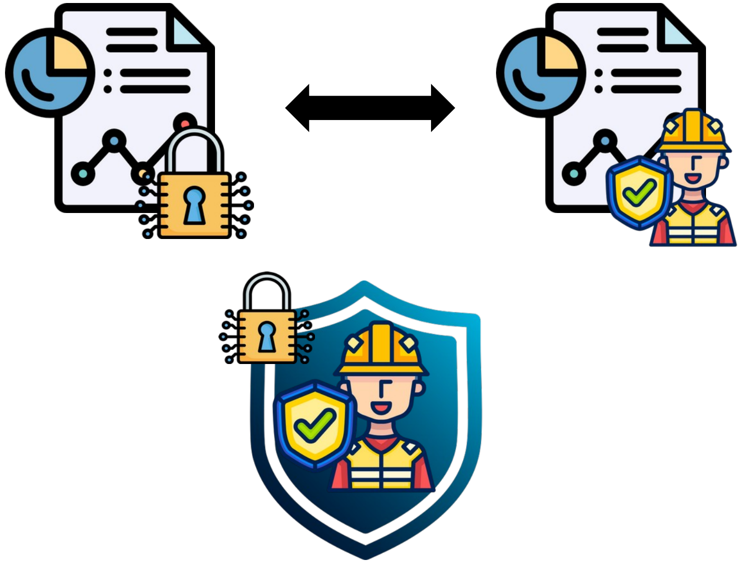
Unified

→ Single method



Integrated

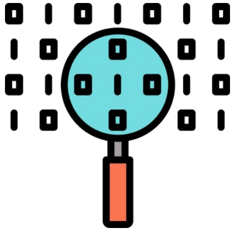
→ Separate method



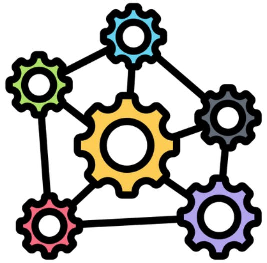
Literature Review & Classification

Integrated

Fine granularity



System size



+20 sensors & actuators

Literature Review & Classification

Integrated

Fine granularity

System size

+20 sensors & actuators

Literature Review & Classification

Methods	Integrated	System Size
Winther et al. (2001)	✓	Small
Cárdenas et al. (2011)	✓	Small
Song et al. (2012)	✓	Small
Young et Leveson (2013)	✓	Small
Kriaa (2015)	✘	Small
Sabaliauskaite et al. (2015)	✘	Small
Mesli-kesraoui et al. (2016)	✓	Small
Subramanian et Zalewski (2016)	✘	Small
Rocchetto et Tippenhauer (2017)	✓	Large
Friedberg et al (2017)	✘	Small
Abdo et al. (2018)	✘	Small
Cheh et al. (2018)	✓	Small
Subramanian et Zalewski (2018)	✘	Small
Puys et al. (2018)	✓	Small
Zhu et al. (2018)	✓	Small
Papakonstantinou et al. (2019)	✘	Small
Khaled et al. (2020)	✓	Small
Kumar et al. (2020)	✘	Small
Hosseini et al. (2021)	✘	Small
Oueidat et al. (2021)	✘	Small
Bhosale et al. (2023)	✓	Small
Eckhart et al. (2022)	✓	Small
Földvári et al. (2023)	✘	Small
Son et al. (2023)	✓	Small
This work	✓	Large

Literature Review & Classification

Integrated

Attack complexity

Rocchetto et Tippenhauer
1000 lines of ASLan++ code to model system behavior

System complexity

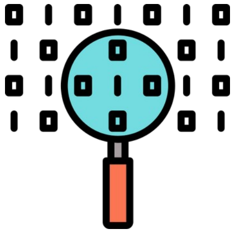
+20 sensors & actuators

M. Rocchetto et N. O. Tippenhauer, « Towards Formal Security Analysis of Industrial Control Systems », in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, Abu Dhabi United Arab Emirates: ACM, avr. 2017, p. 114-126. doi: 10.1145/3052973.3053024.

Literature Review & Classification

Integrated

Attack complexity

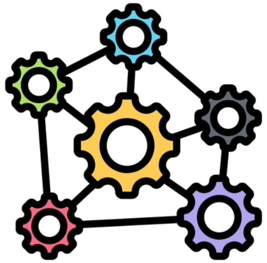


Rocchetto et Tippenhauer
1000 lines of ASLan++ code to model system behavior

→ **Model checking (stop at first occurrence)**
→ **System behavior description**

→ **Decomposition to control complexity**
→ **Lower complex attacker**
→ **Method automation from PLC-logic**

System complexity

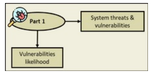


+20 sensors & actuators

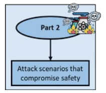
M. Rocchetto et N. O. Tippenhauer, « Towards Formal Security Analysis of Industrial Control Systems », in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, Abu Dhabi United Arab Emirates: ACM, avr. 2017, p. 114-126. doi: 10.1145/3052973.3053024.

Contents

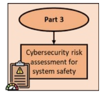
Cybersecurity Risk Assessment for System Safety



What an attacker can do



What an attacker might do



Is it serious ?

Literature Review & Classification

Identifying Cybersecurity Risk for System Safety

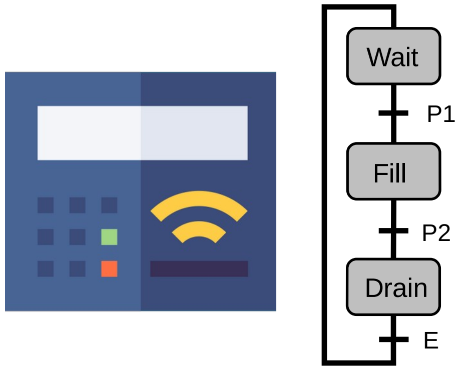
PLC-Logic Based Cybersecurity Risk Identification

Conclusion and perspectives

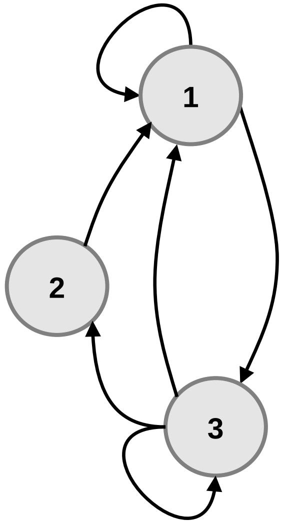
UNIVERSITÉ
Clermont
Auvergne

LIMOS

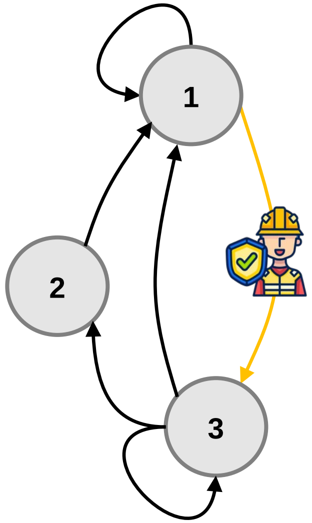
PLC-Logic Based Cybersecurity Risk Identification



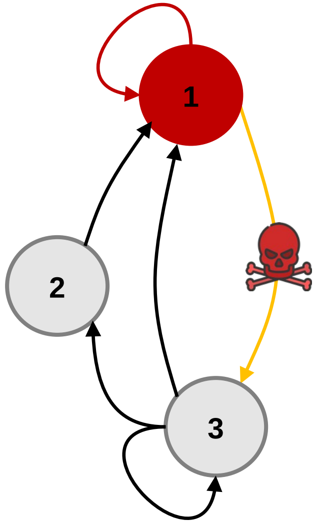
PLC logic



System model

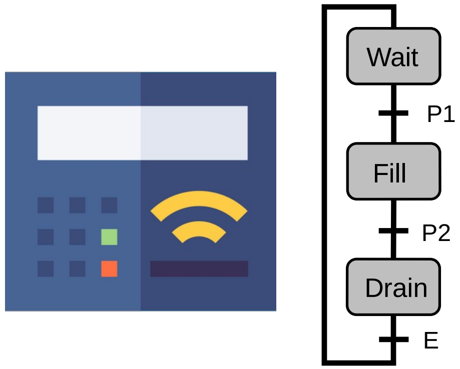


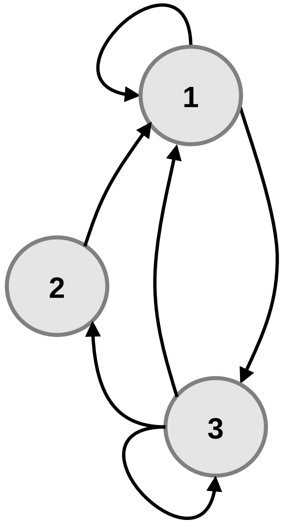
Safety

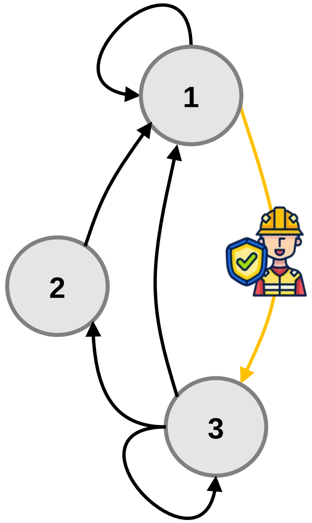


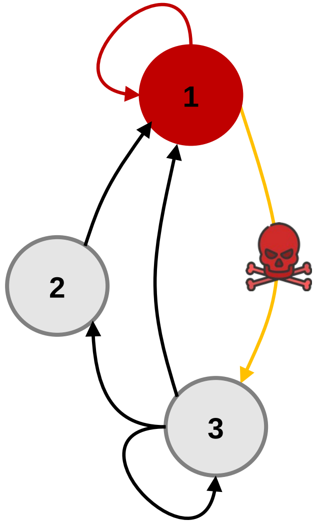
Attack scenarios

PLC-Logic Based Cybersecurity Risk Identification









PLC logic

System model

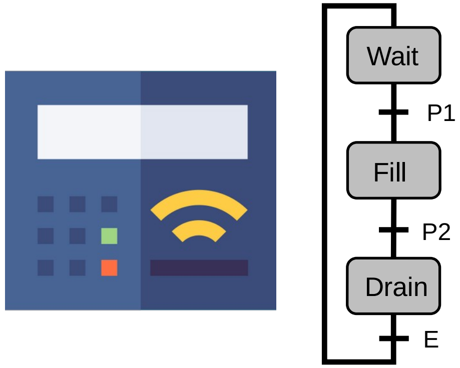
Safety

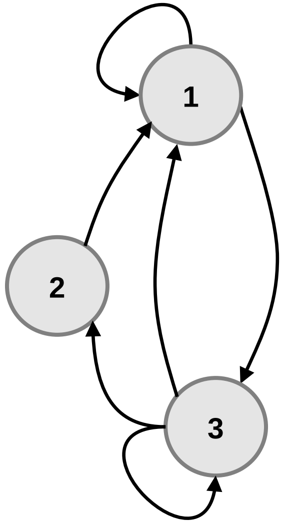
Attack scenarios

Model building

Threat model application

Model Building





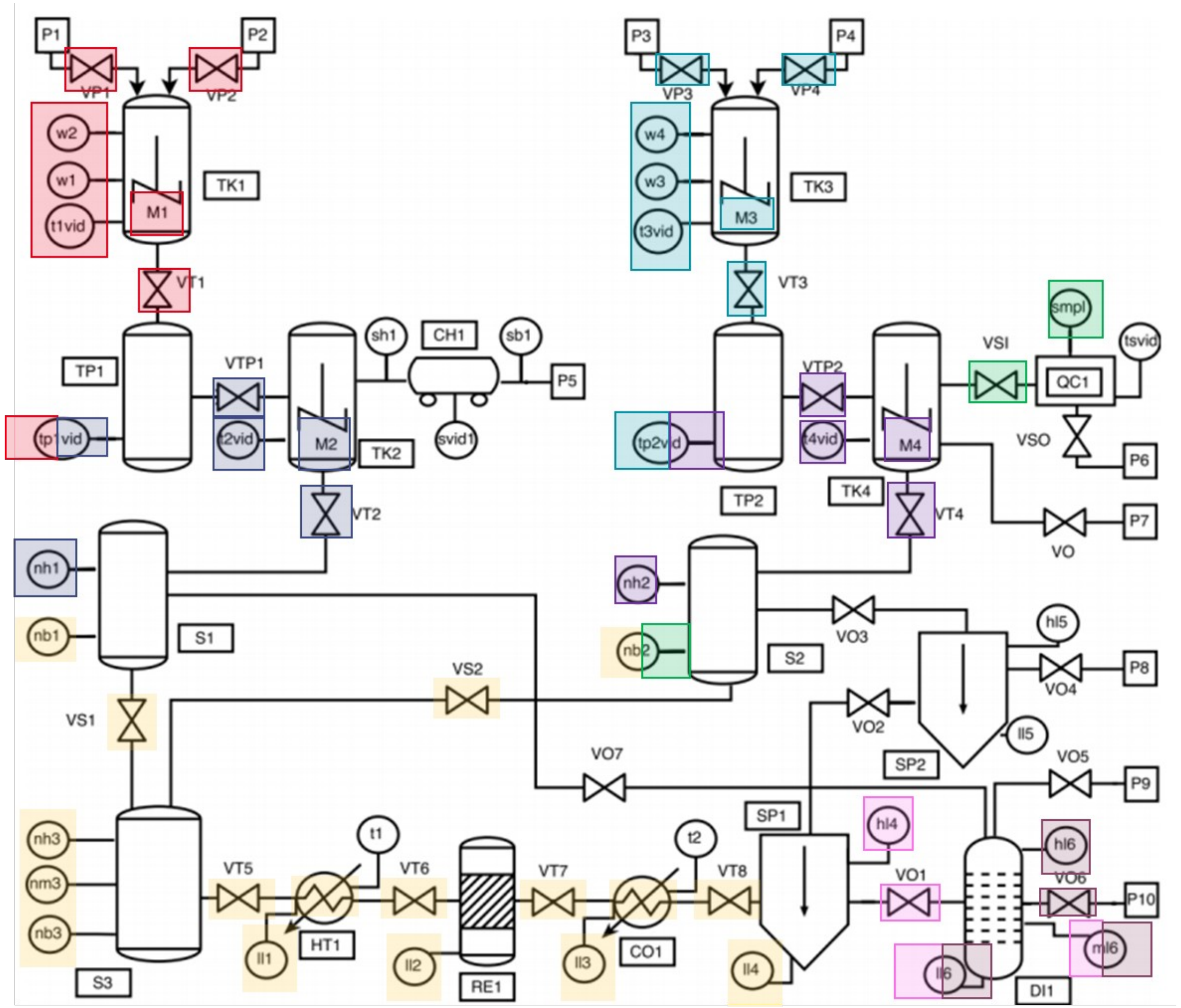
PLC logic

System model

Model building

Objective

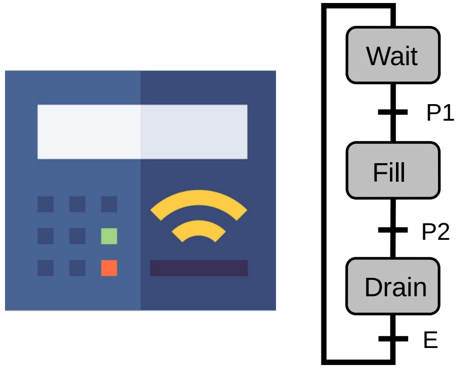
Tennessee Eastman Physical Process



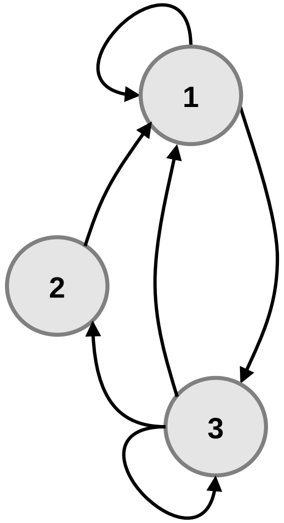
26 sensors
24 actuators

McAvoy, T. J., & Ye, N. (1994). Base control for the Tennessee Eastman problem. Computers & Chemical Engineering, 18(5), 383-413.

Model Building

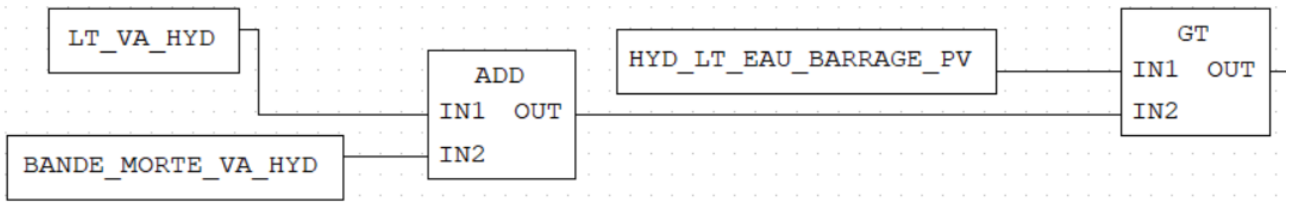


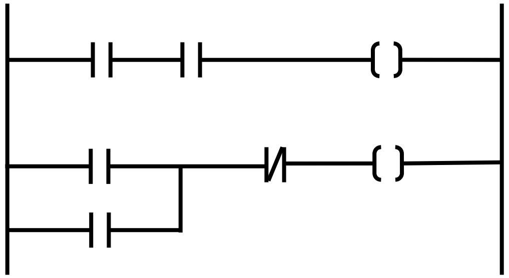
PLC logic

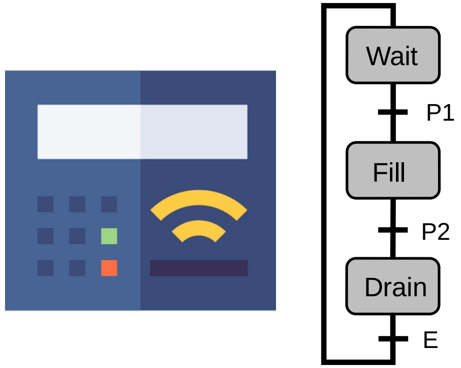


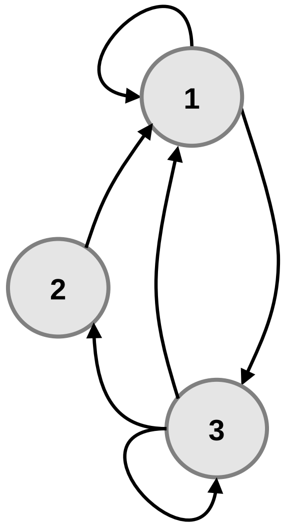
System model

Model Building







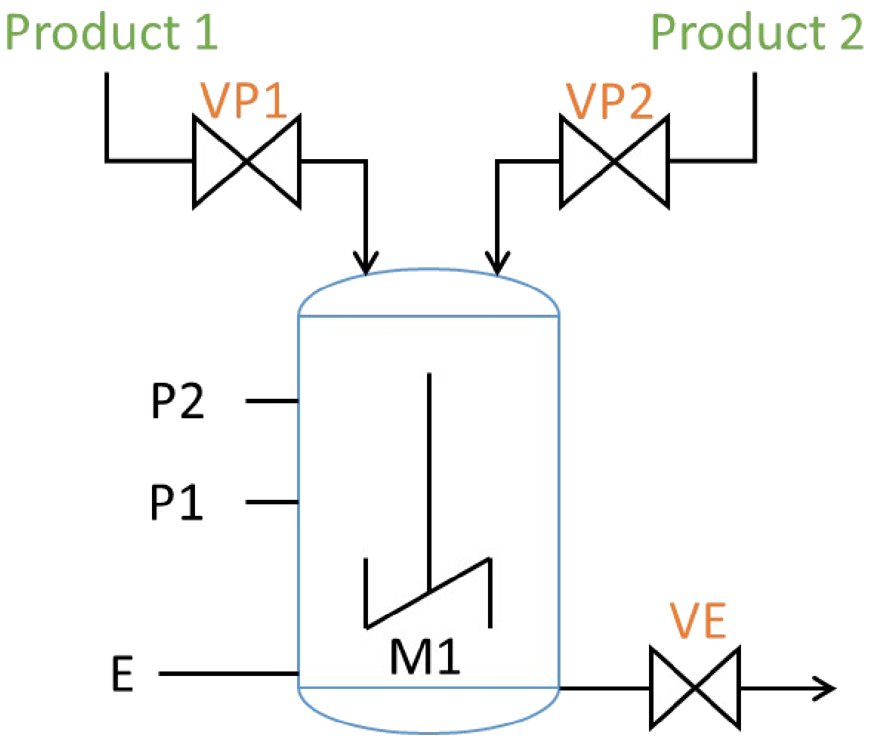


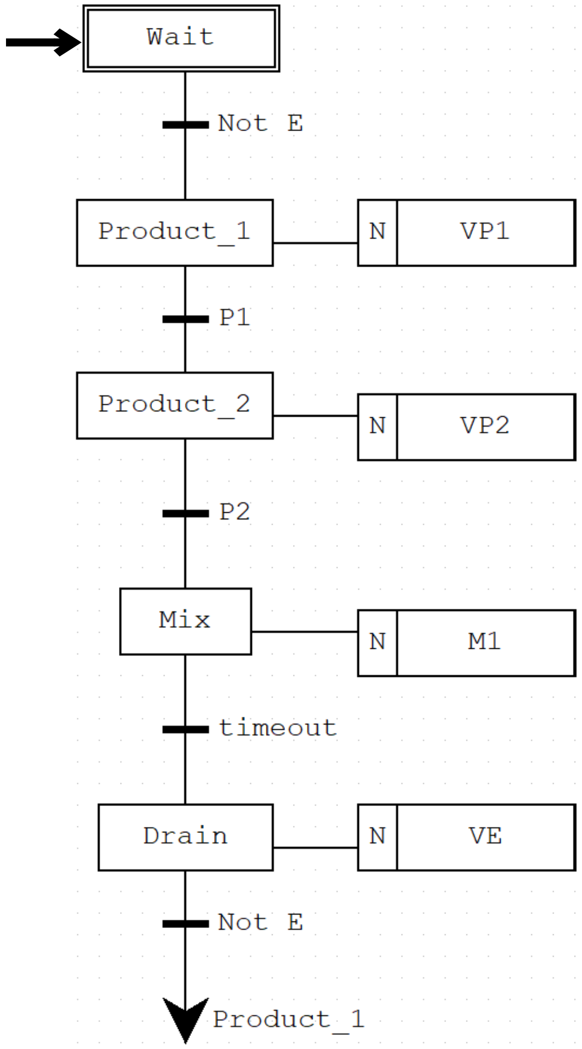
```
PROGRAM Example_ST
   VAR
         A: BOOL;
         B: BOOL;
         C: REAL;
         D: REAL;
   END_VAR
   A := NOT B AND (C <> D);
END_PROGRAM
```

Sequential Function Chart (SFC)

System model

Model Building





Wait

Not E

Product_1 — N VP1

P1

Product_2 — N VP2

P2

Mix — N M1

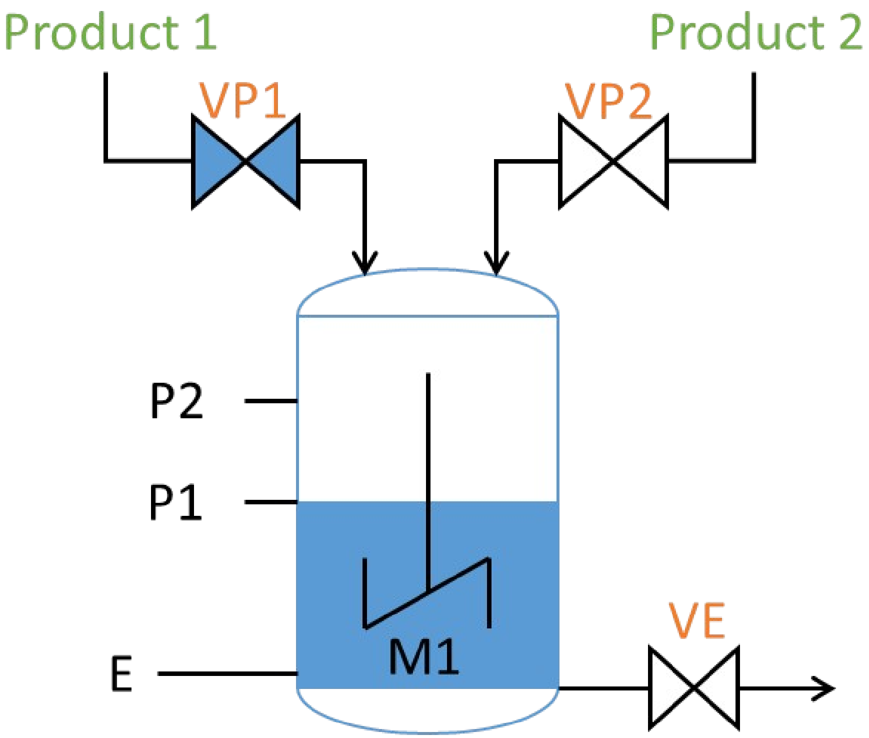
timeout

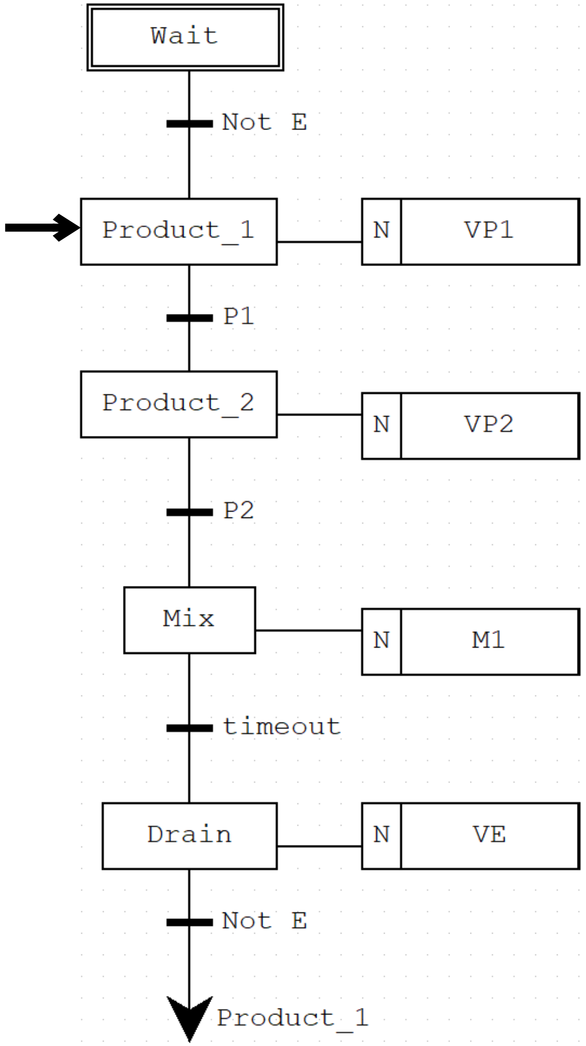
Drain — N VE

Not E

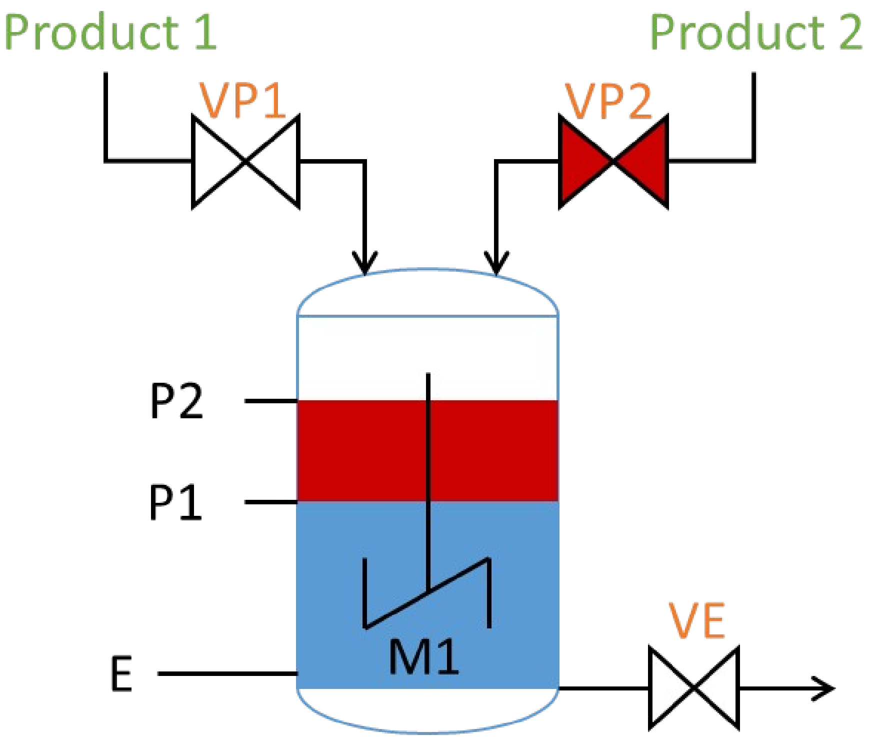
Product_1

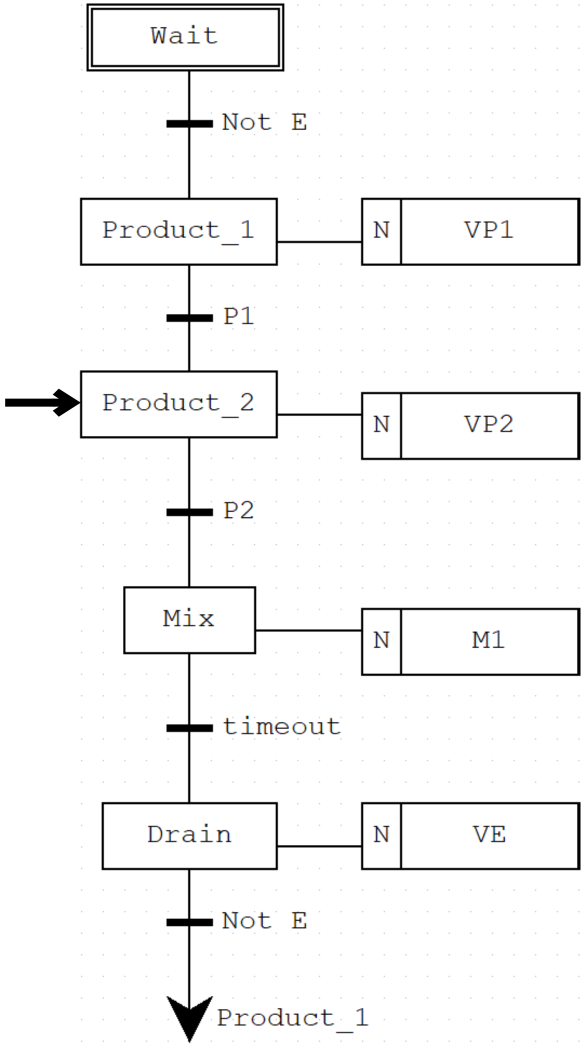
Model Building



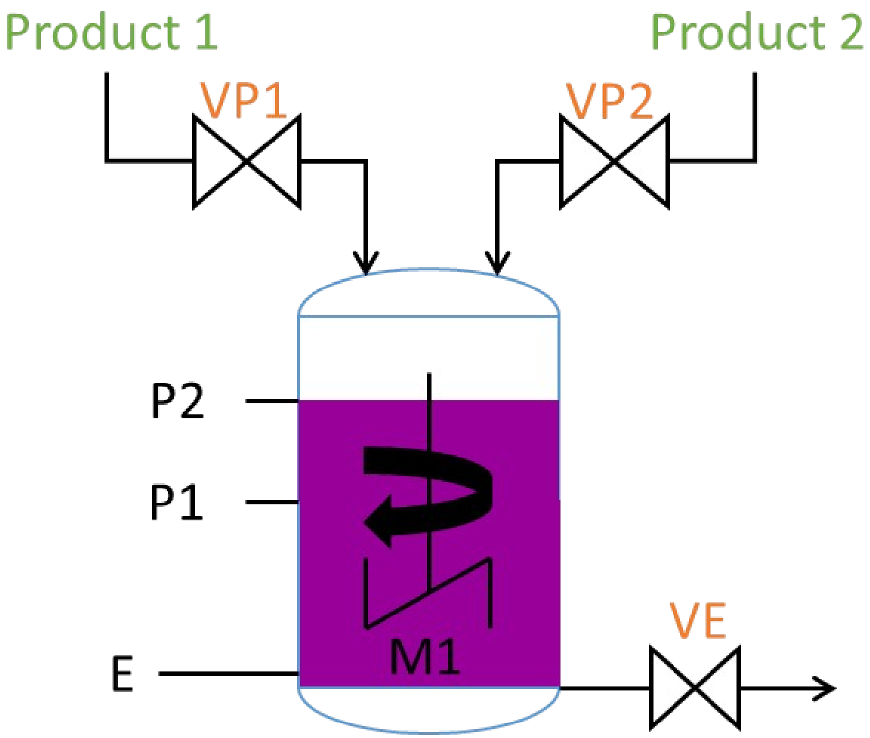


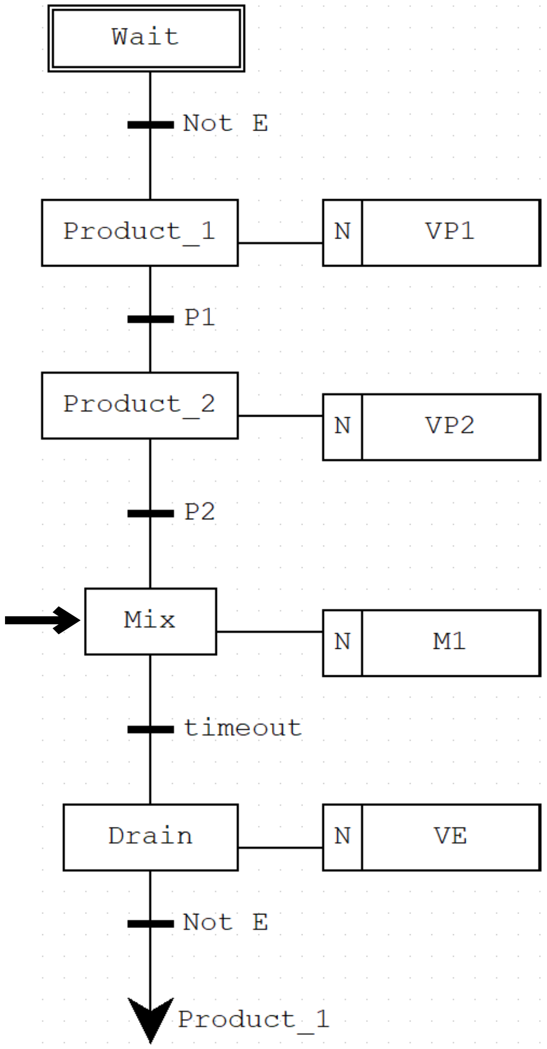
Model Building





Model Building





Wait

Not E

Product_1 — N VP1

P1

Product_2 — N VP2

P2

Mix — N M1

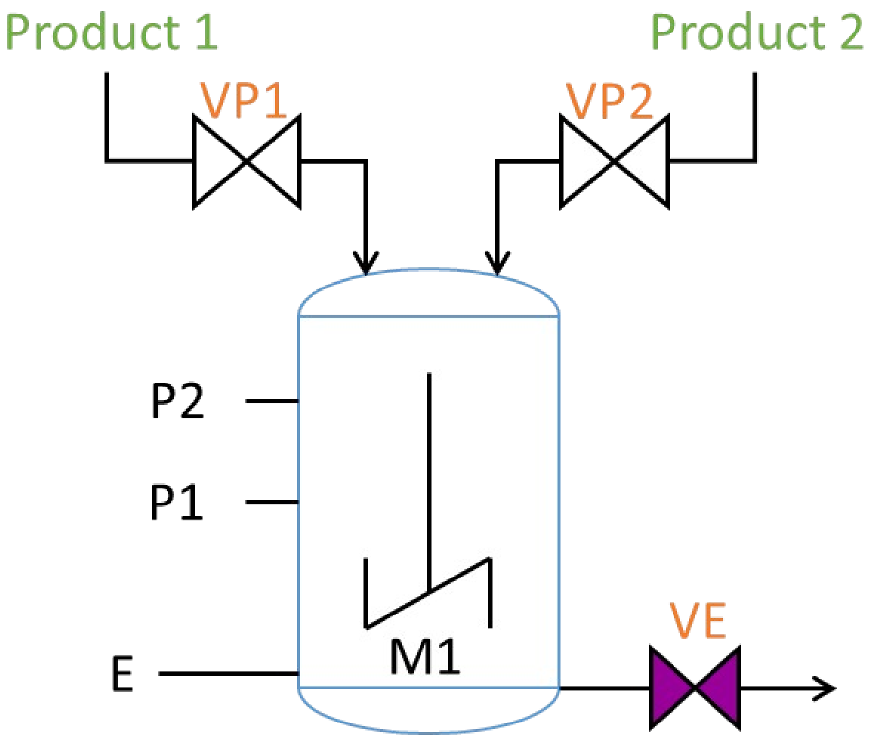
timeout

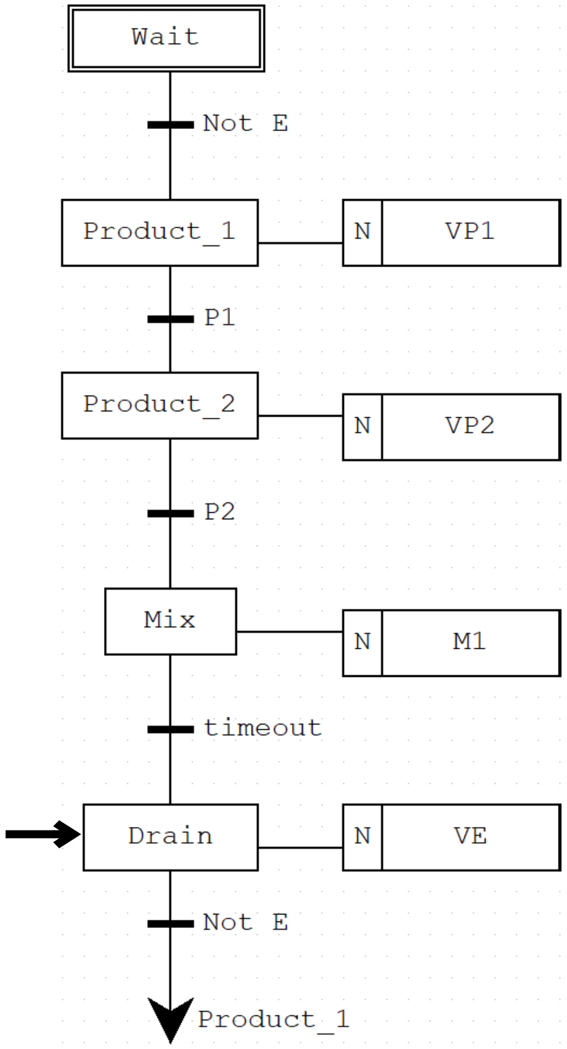
Drain — N VE

Not E

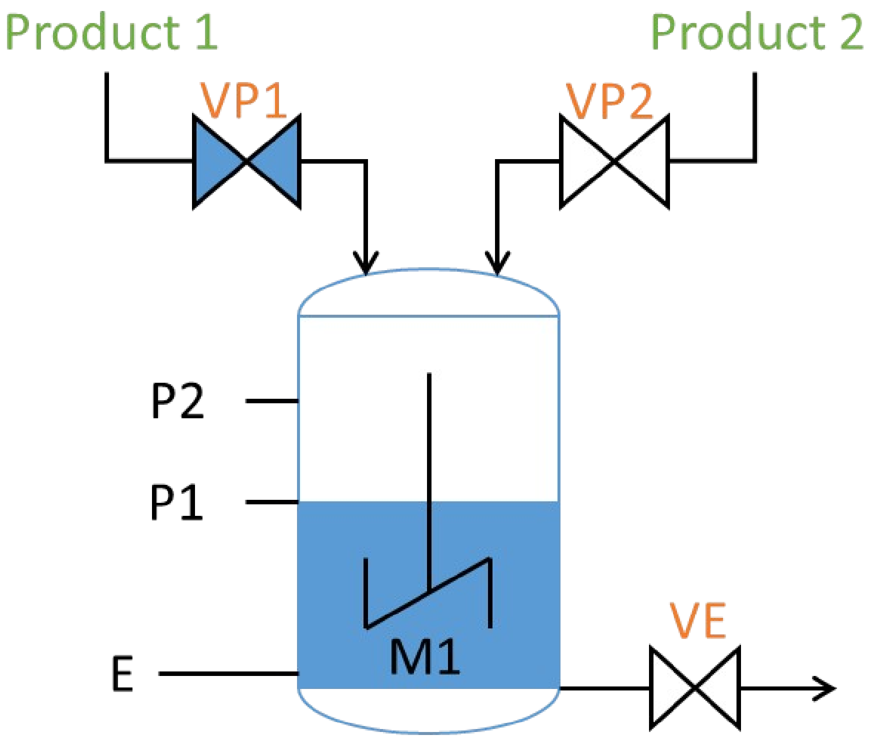
Product_1

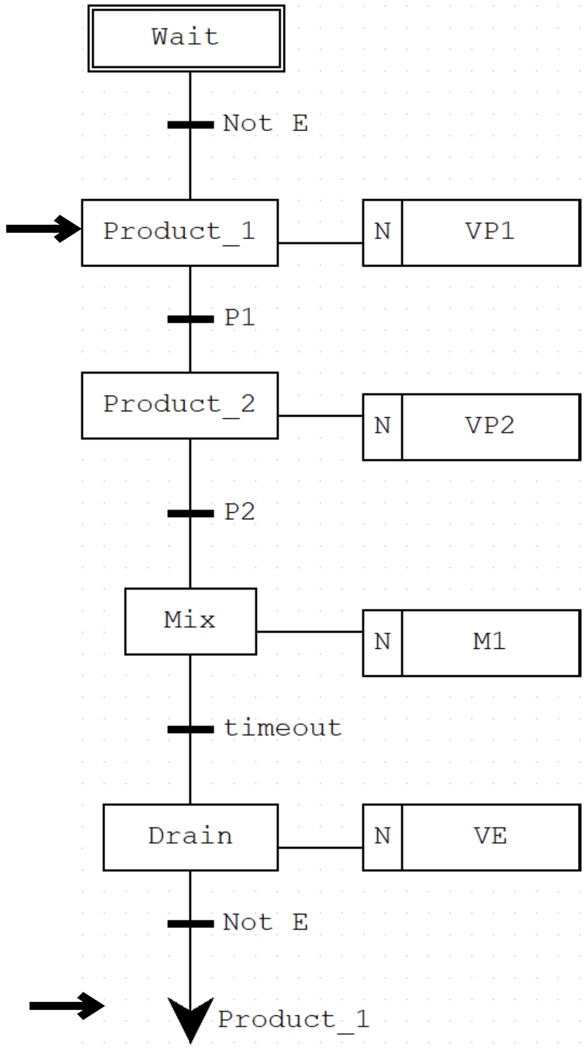
Model Building



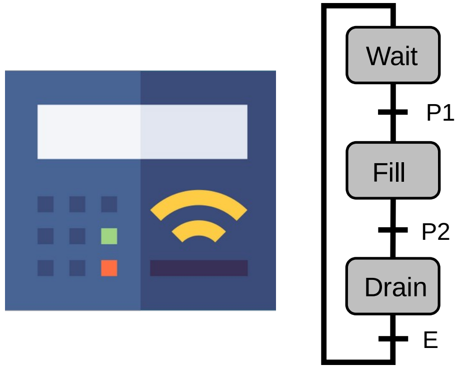


Model Building

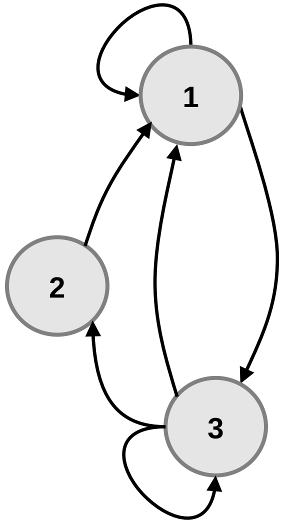




Model Building

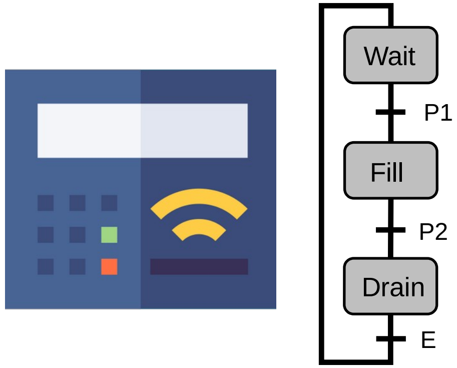


SFC

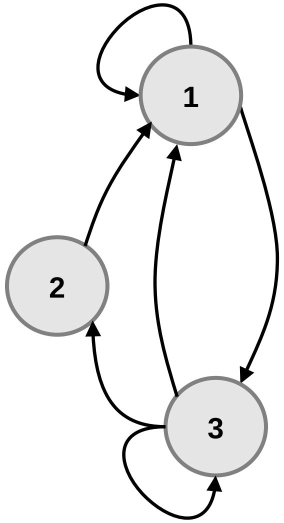


System model

Model Building

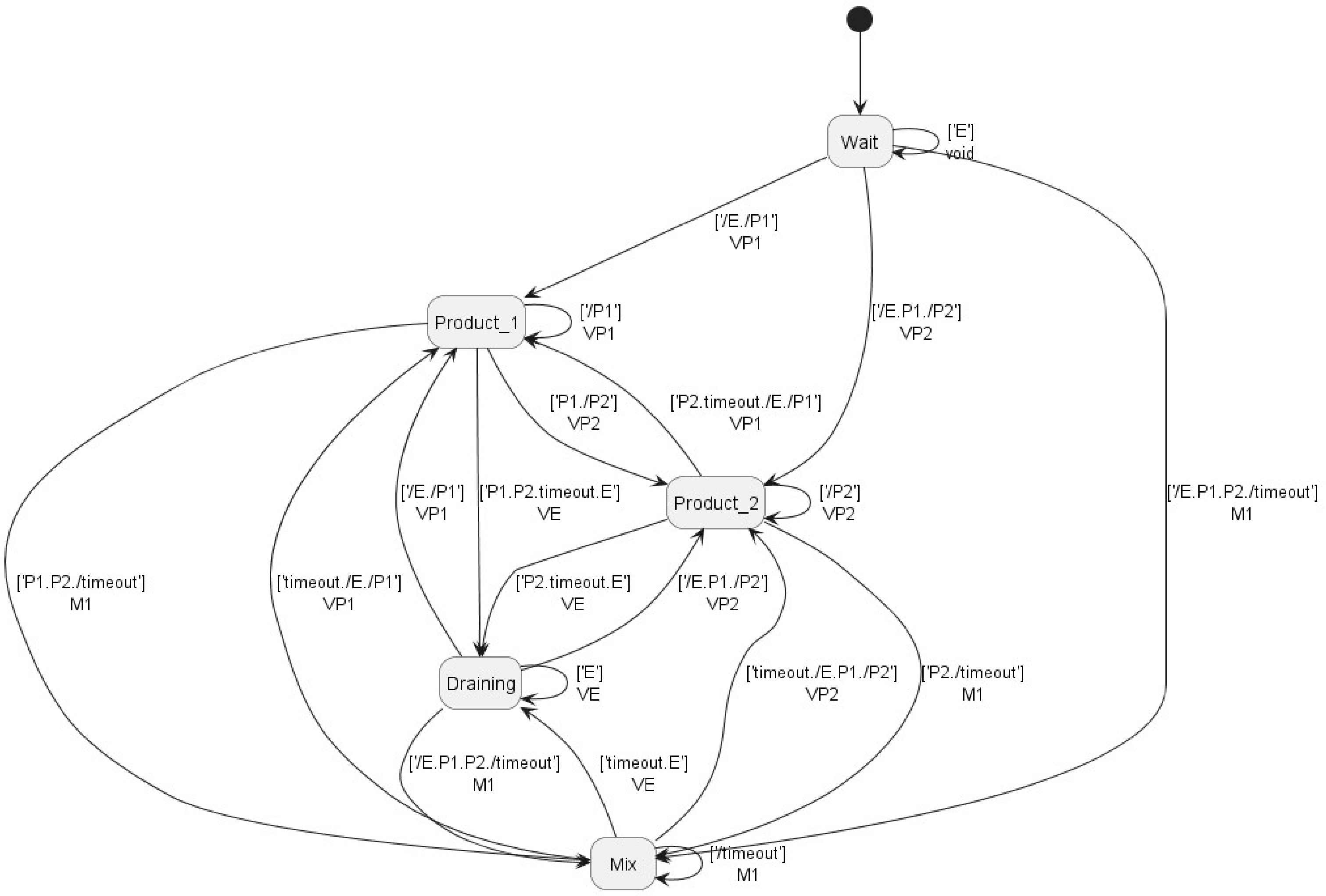


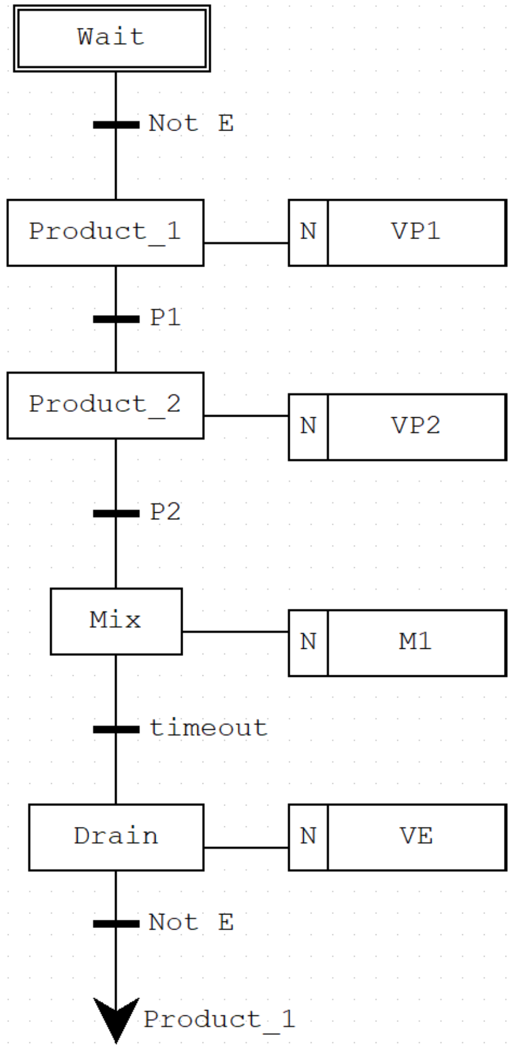
SFC



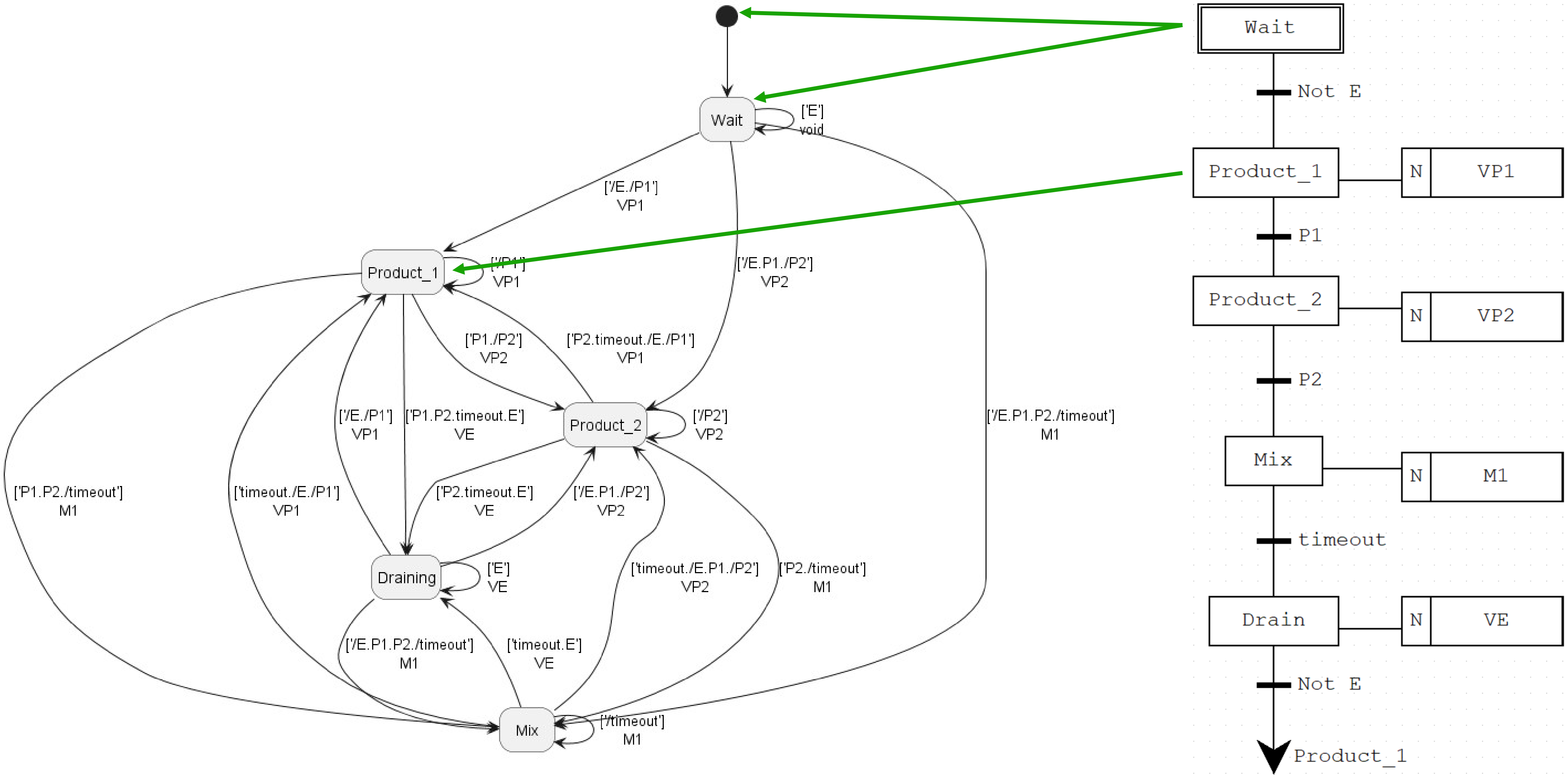
Finite-state transducer

Model Building

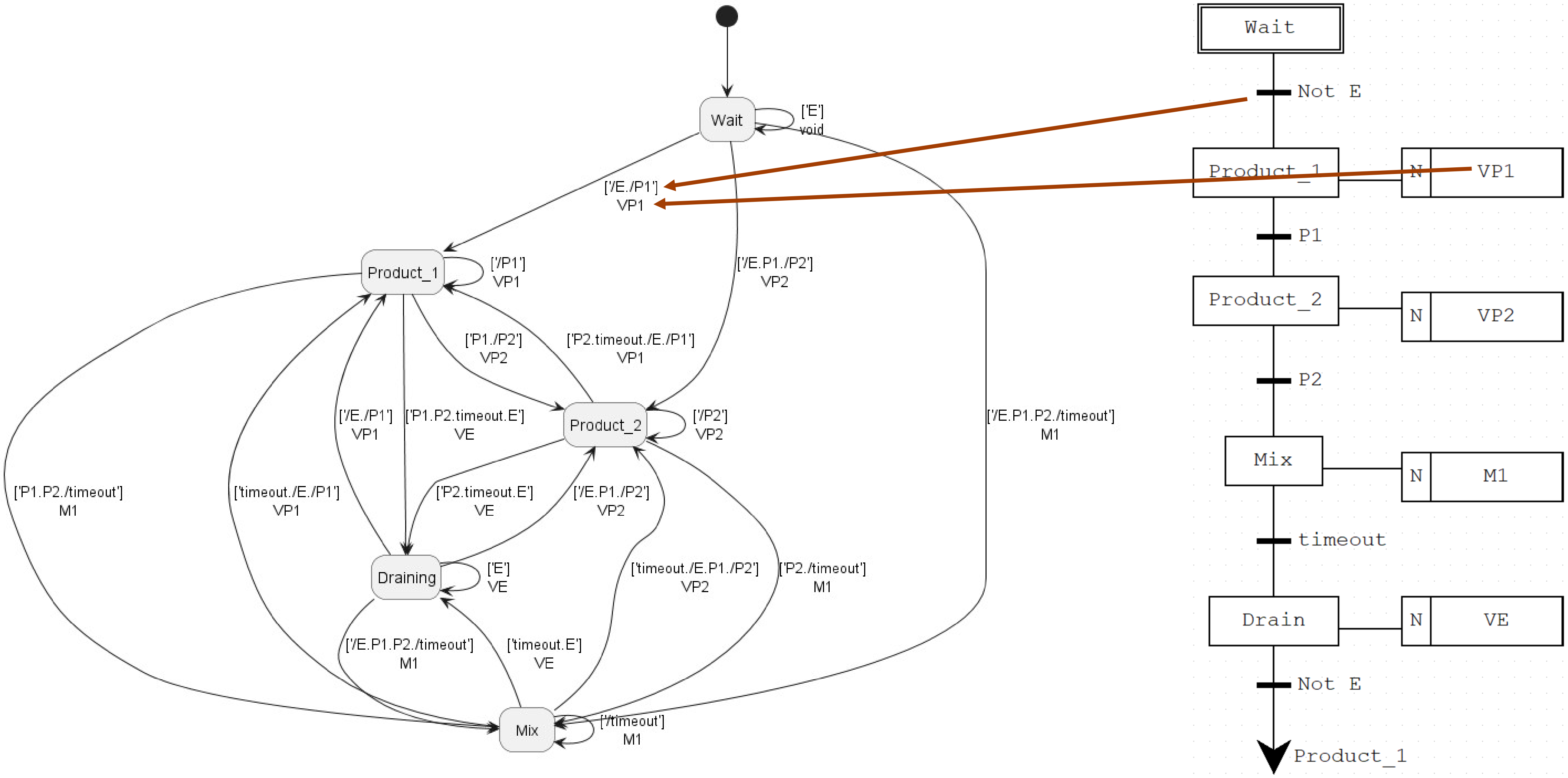




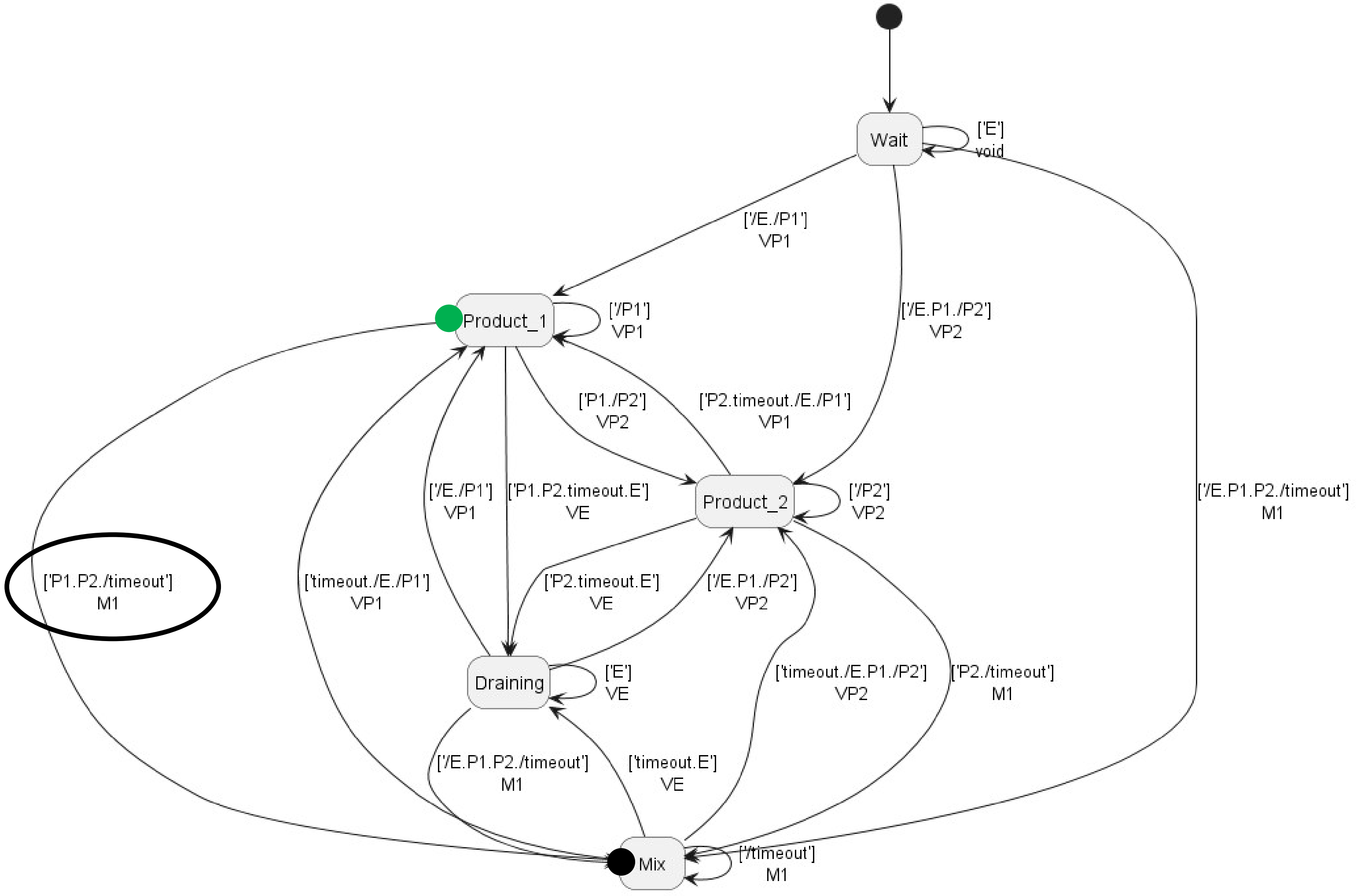
Model Building

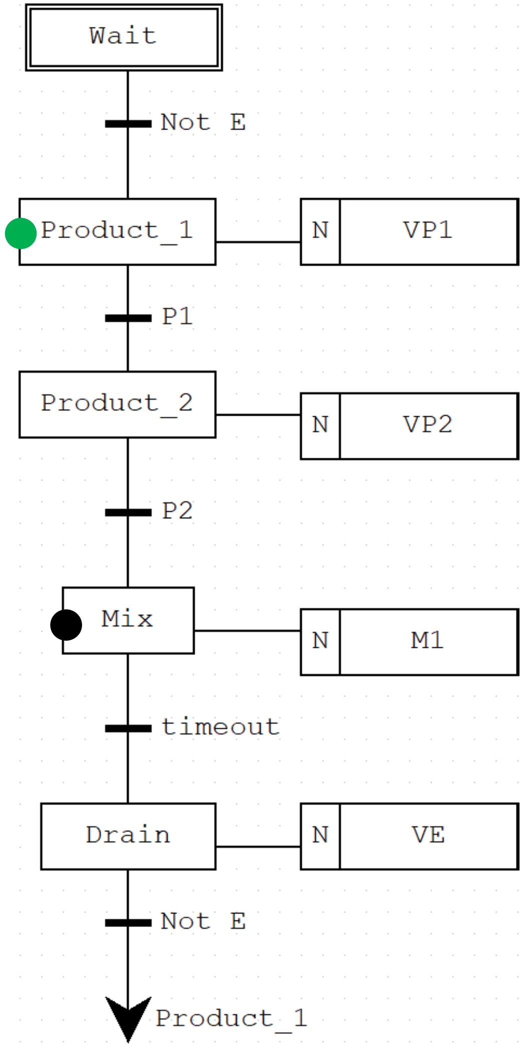


Model Building



Model Building

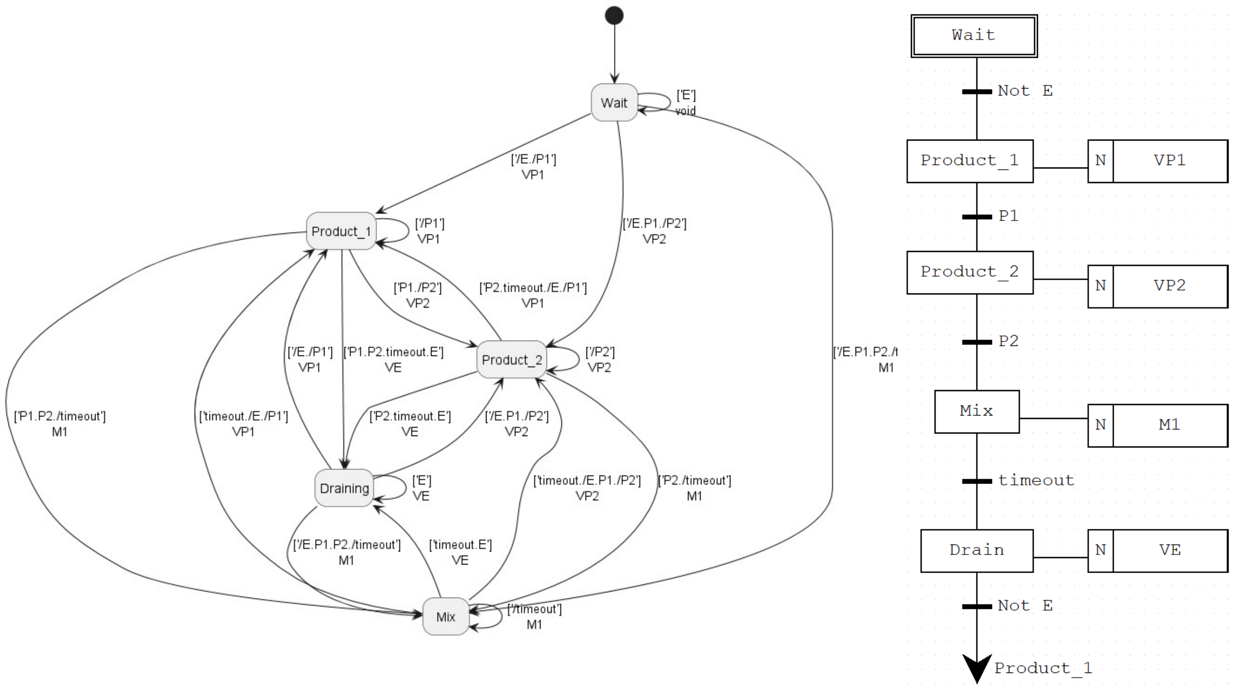




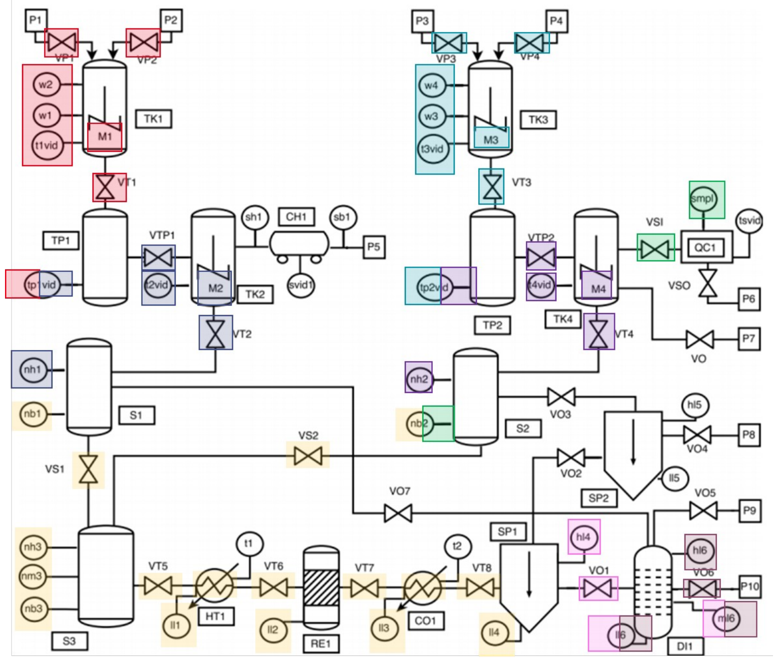
Calculate once upstream

Calculate each time

Objective



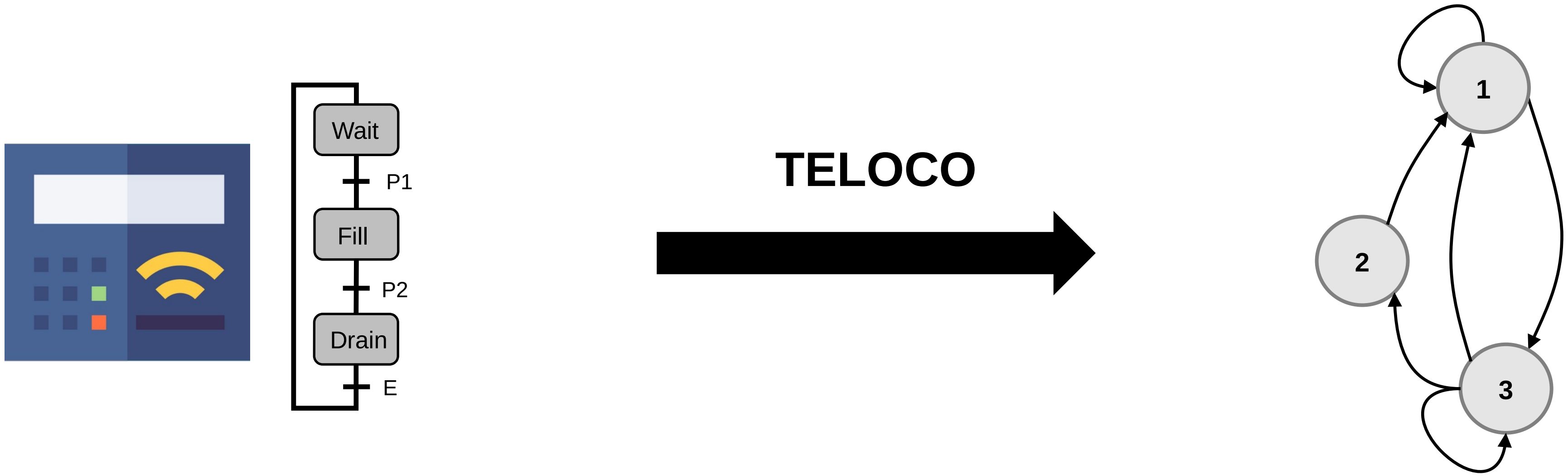
VS.



5 states

6.7 x 10^5 states

Model Building



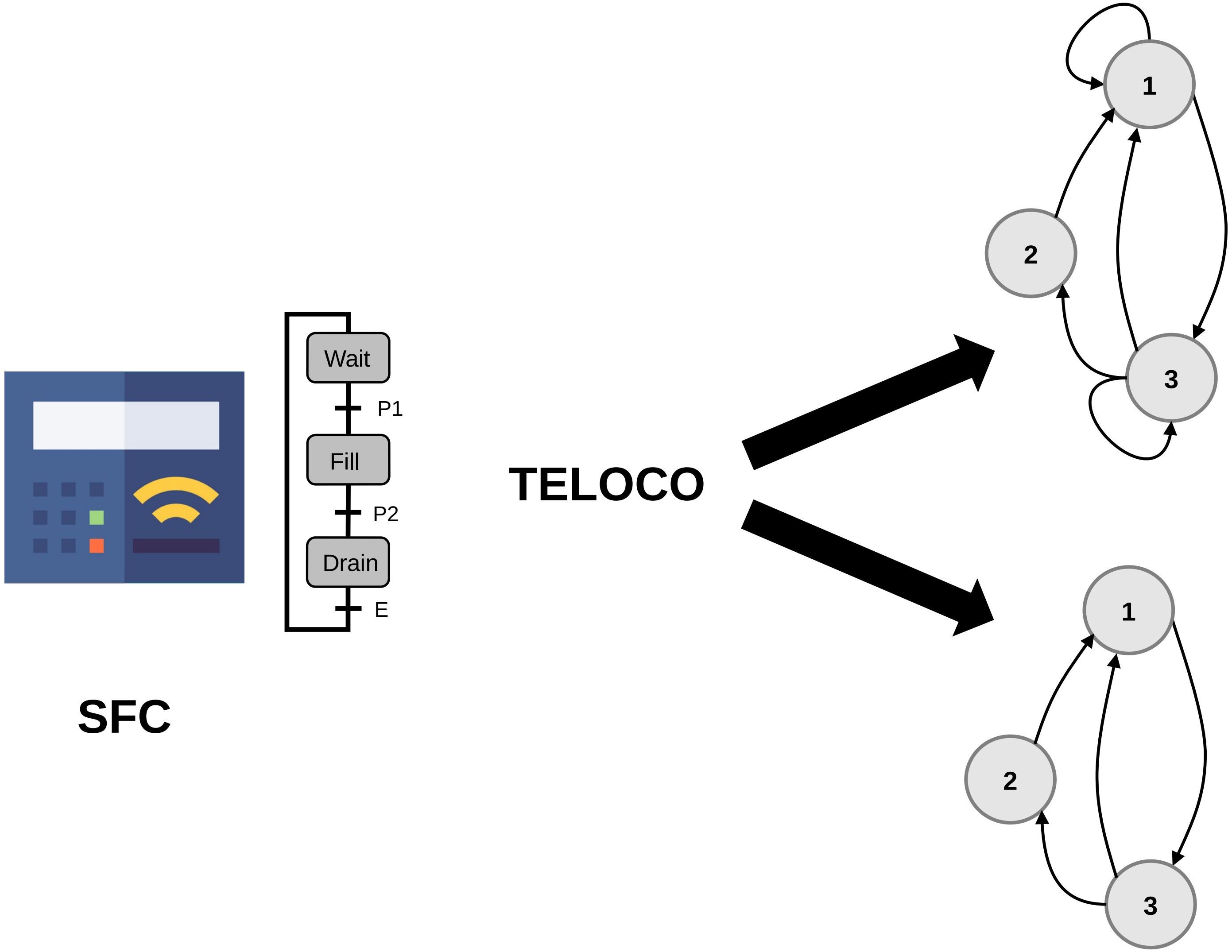
SFC

TELOCO

Finite-state transducer

J. Provost, J.-M. Roussel, et J.-M. Faure, « Translating Grafcet specifications into Mealy machines for conformance test purposes », *Control Engineering Practice*, sept. 2011, doi: 10.1016/j.conengprac.2010.10.001.

Model Building



Mealy machine => Too complex

Requires Boolean minimization of transitions

Complexity = 2^{inputs} x states

Tennessee-Eastman => 2^{26} x $6{,}7.10^{5}$

≈ 10^{13}

Stable Location Automaton (SLA)

Complexity = states^{2}

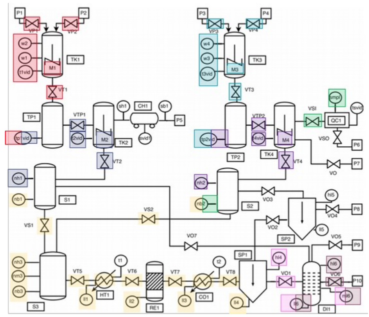
Tennessee-Eastman => $(6{,}7.10^{5})^{2}$

≈ 10^{11}

Model Building

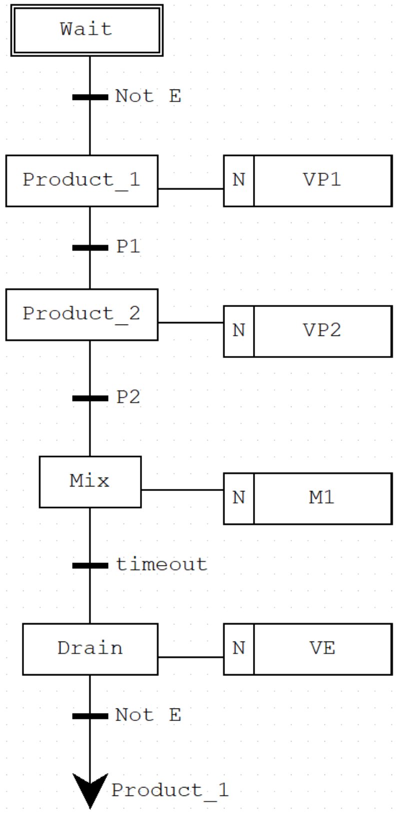
Modeling Time

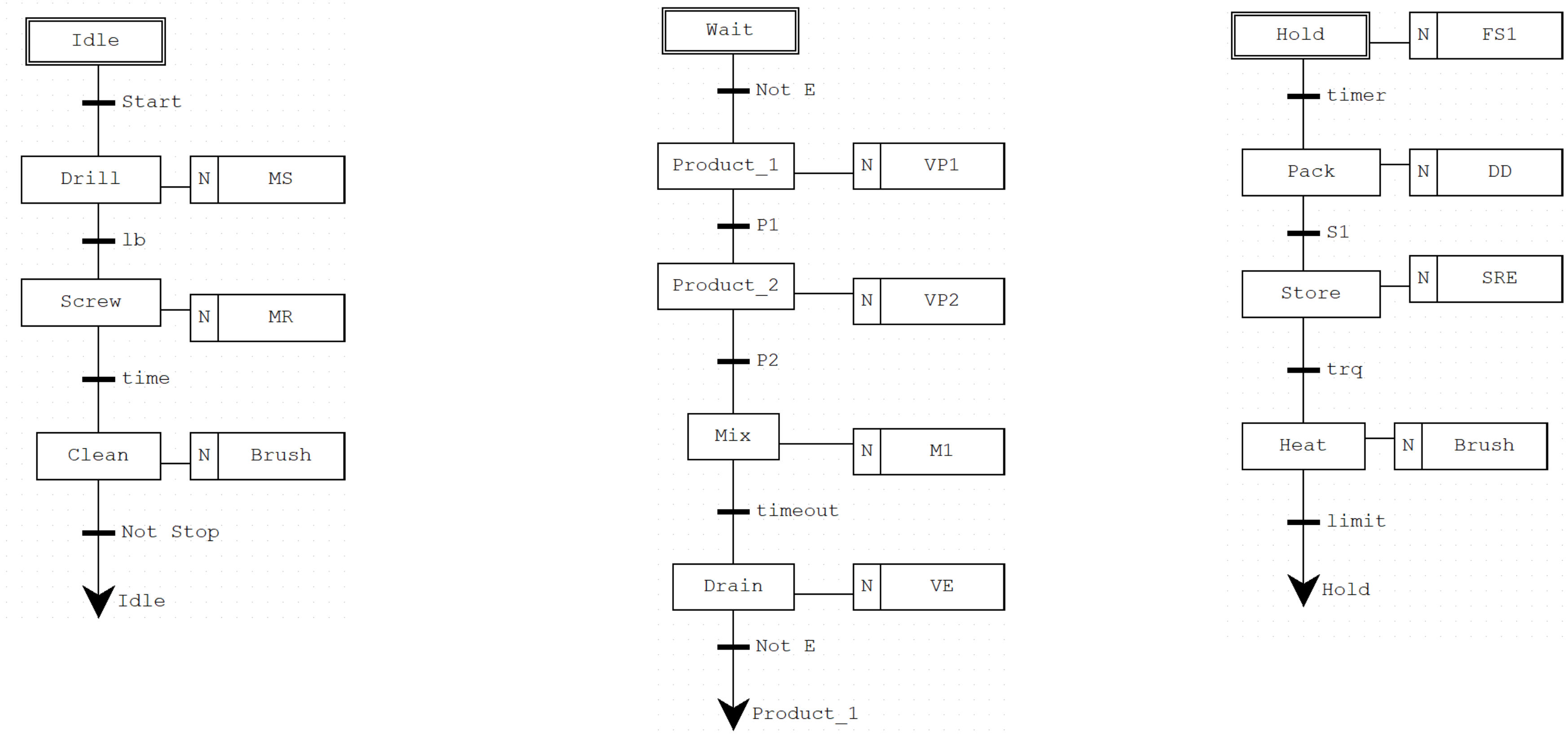
SLA	Mealy	Minimization	Inputs
1 ms	0 ms	372 ms	3
0 ms	0 ms	376 ms	4
0 ms	0 ms	382 ms	5
141 ms	51 ms	505 ms	9
42 ms	162 ms	17 219 ms	13
21 973 ms	30 190 ms	65 813 ms	13
1 320 ms	15 143 ms	1 381 511 ms	16
2 625 ms	46 875 ms	X	17
50 036 ms	994 192 ms	X	18
1 091 838 ms	X	X	18
X	X	X	26



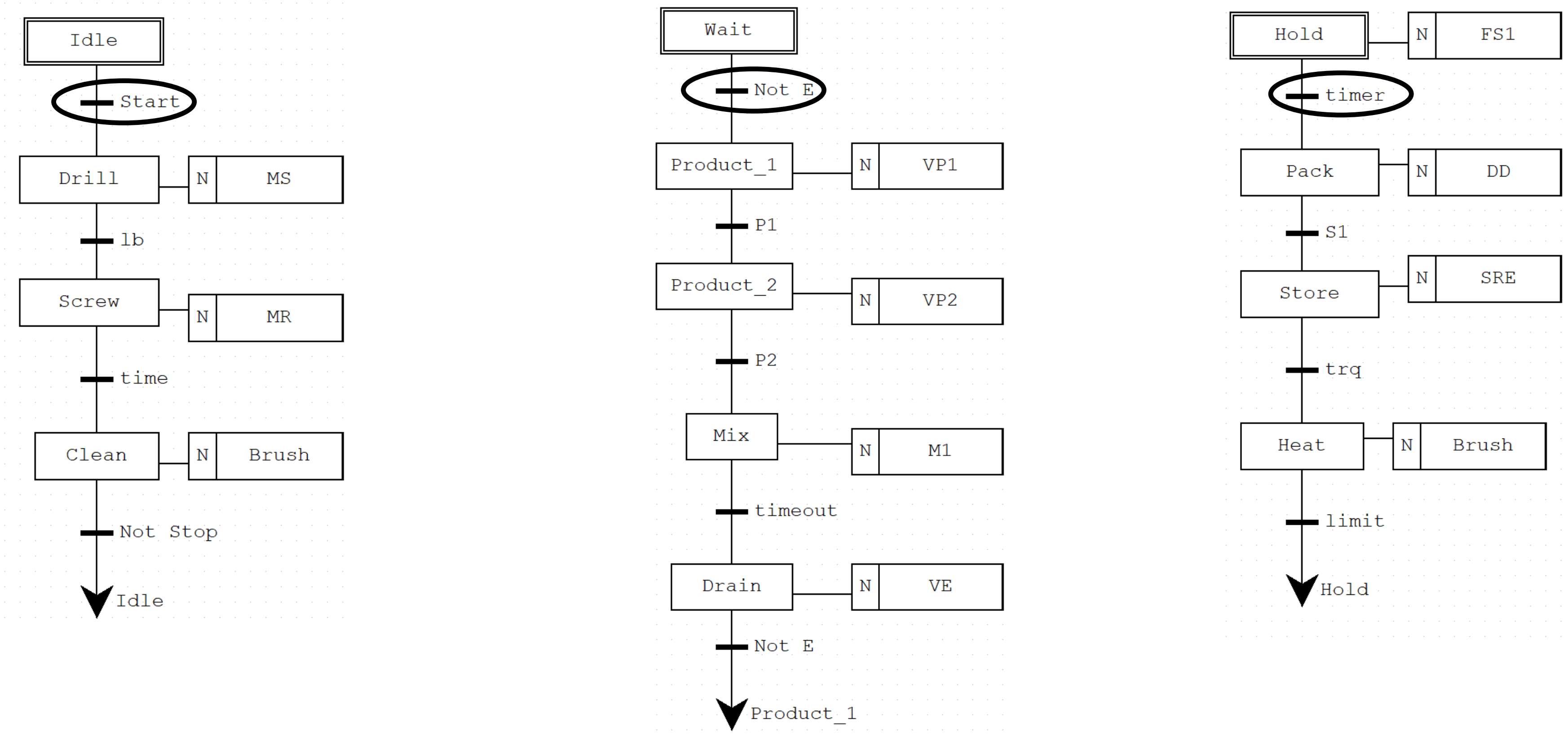
Tennessee-Eastman →

→ **Intel(R) Core(TM)i5-8365U @1,60GHz-1,90GHz and 16 Go of RAM.**

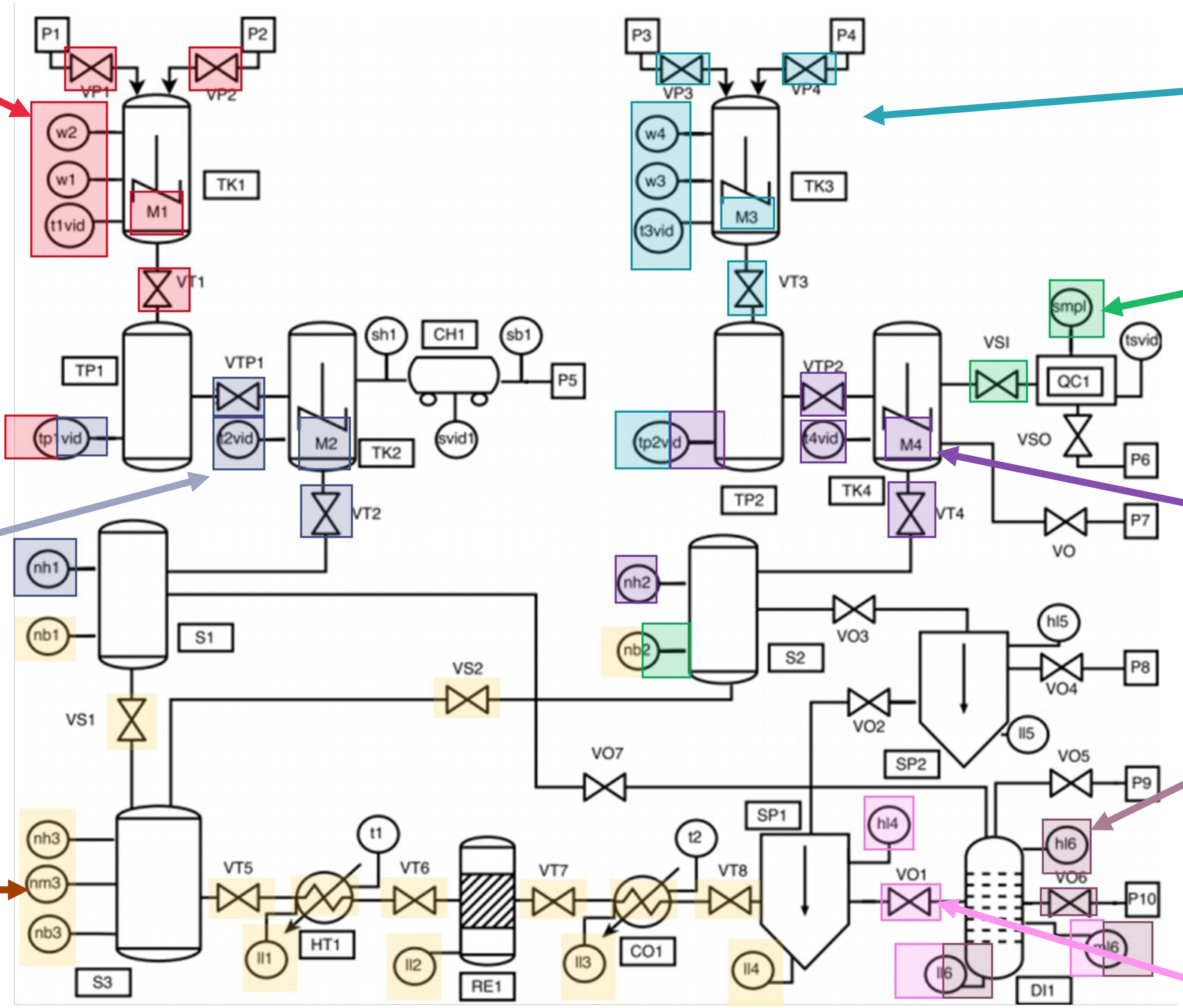

Wait
Not E
Product_1
N
VP1
P1
Product_2
N
VP2
P2
Mix
N
M1
timeout
Drain
N
VE
Not E
Product_1



/!\ Not one big SFC but multiple smaller running at the same time



/!\ In the worst case, # states is not the sum of all states but the product



4 inputs
6 states

4 inputs
6 states

4 inputs
4 states

4 inputs
5 states

5 inputs
6 states

3 inputs
3 states

13 inputs
13 states

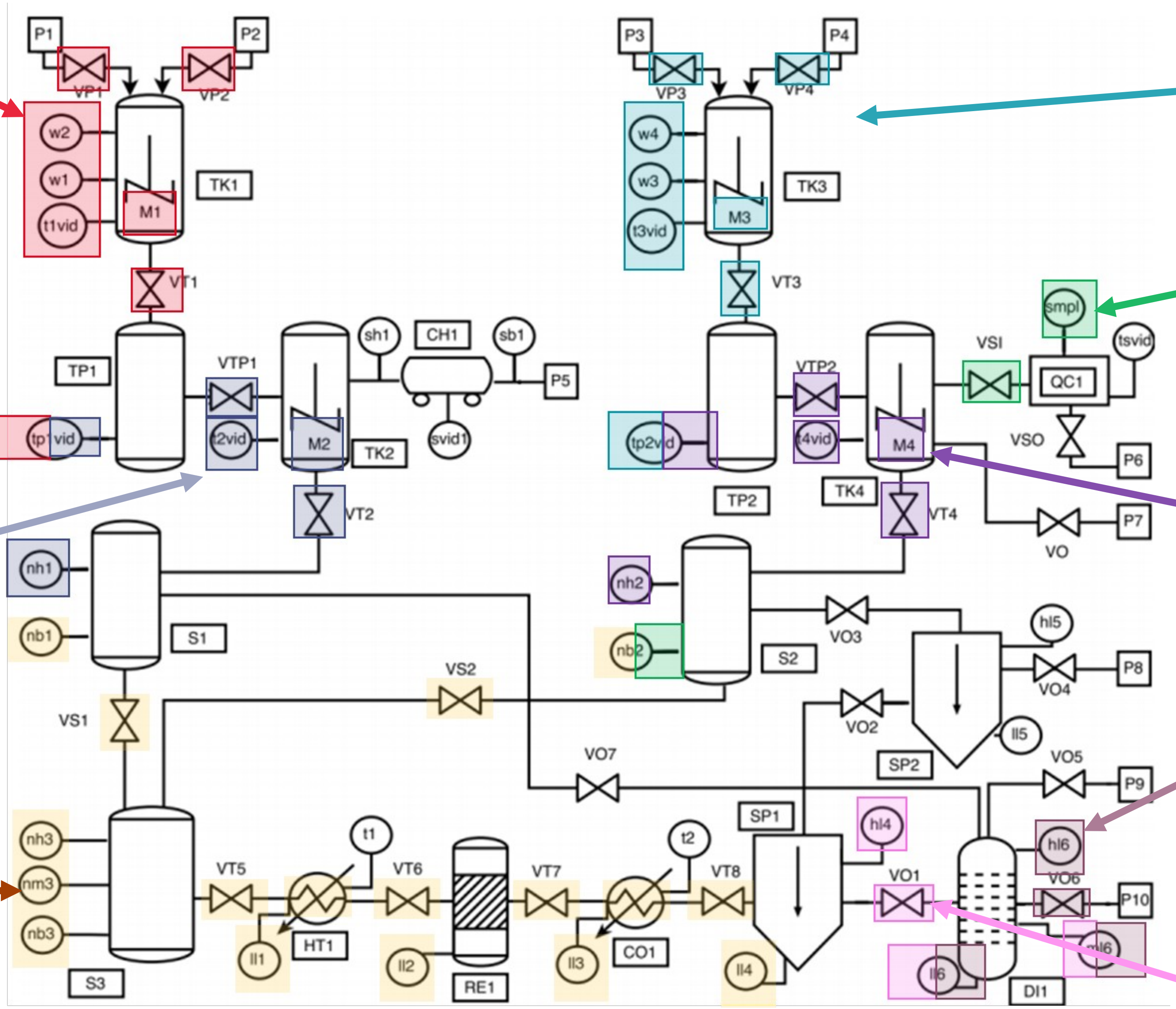
4 inputs
4 states

4 inputs
6 states

TOTAL: 6,7 . 10^5

4 inputs
5 states

13 inputs
13 states



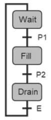
4 inputs
6 states

4 inputs
4 states

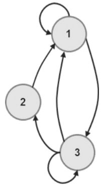
5 inputs
6 states

3 inputs
3 states

4 inputs
4 states

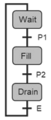


Model Building

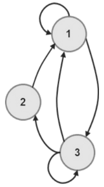


Modeling Time

SLA	Graphs	Inputs
1 ms	1	3
0 ms	1	4
0 ms	1	5
42 ms	1	13
141 ms	2	9
1 320 ms	2	16
2 625 ms	2	17
21 973 ms	3	13
50 036 ms	3	18
1 091 838 ms	4	18
X	8	26

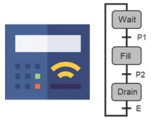


Model Building

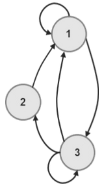


Modeling Time

SLA	Graphs	Inputs
1 ms	1	3
0 ms	1	4
0 ms	1	5
42 ms	1	13
141 ms	2	9
1 320 ms	2	16
2 625 ms	2	17
21 973 ms	3	13
50 036 ms	3	18
1 091 838 ms	4	18
X	8	26

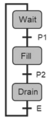


Model Building

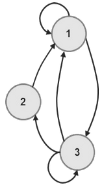


Modeling Time

SLA	Graphs	Inputs
1 ms	1	3
0 ms	1	4
0 ms	1	5
42 ms	1	13
141 ms	2	9
1 320 ms	2	16
2 625 ms	2	17
21 973 ms	3	13
50 036 ms	3	18
1 091 838 ms	4	18
X	8	26

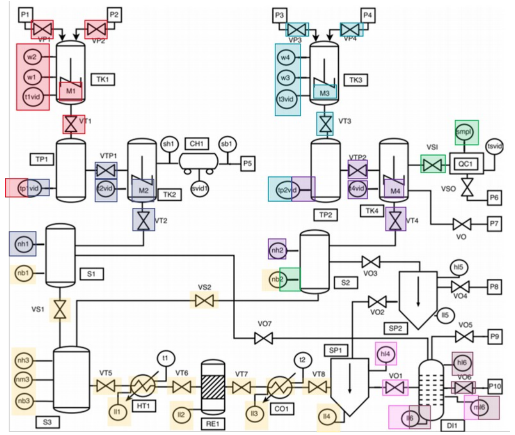


Model Building



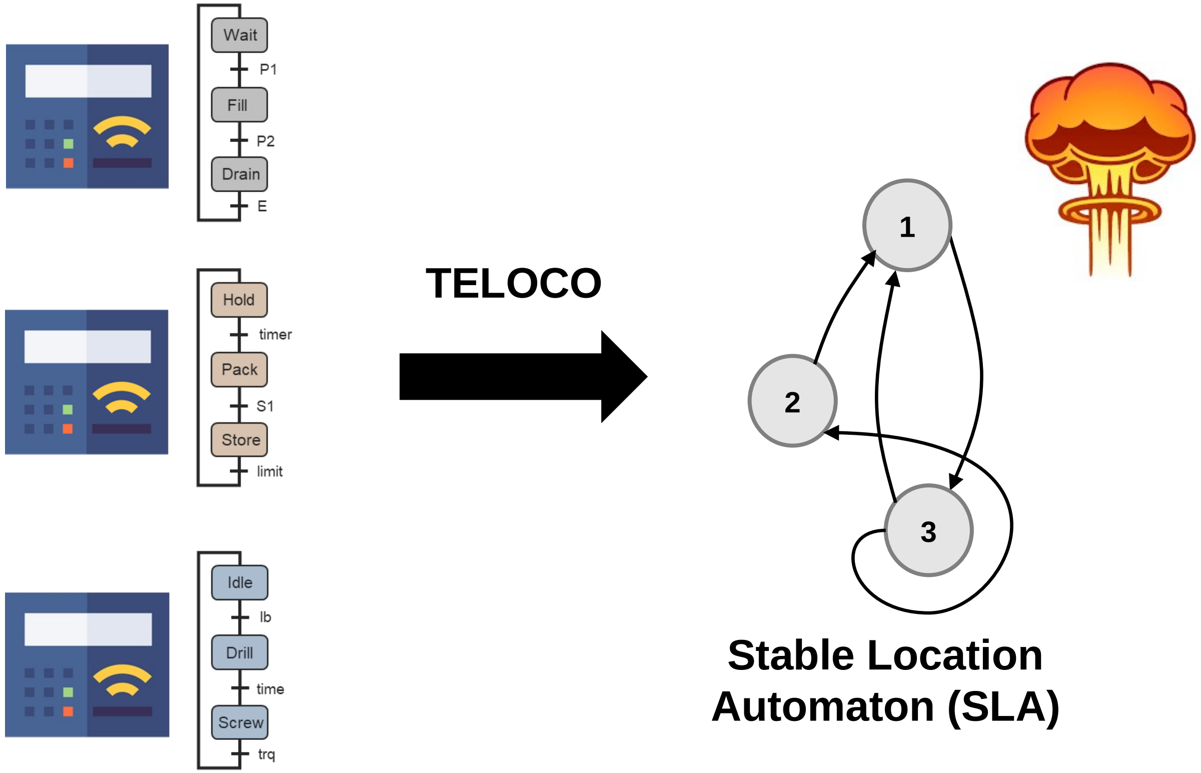
Modeling Time

SLA	Graphs	Inputs
1 ms	1	3
0 ms	1	4
0 ms	1	5
42 ms	1	13
141 ms	2	9
1 320 ms	2	16
2 625 ms	2	17
21 973 ms	3	13
50 036 ms	3	18
1 091 838 ms	4	18
X	8	26



Tennessee-Eastman →

Model Building

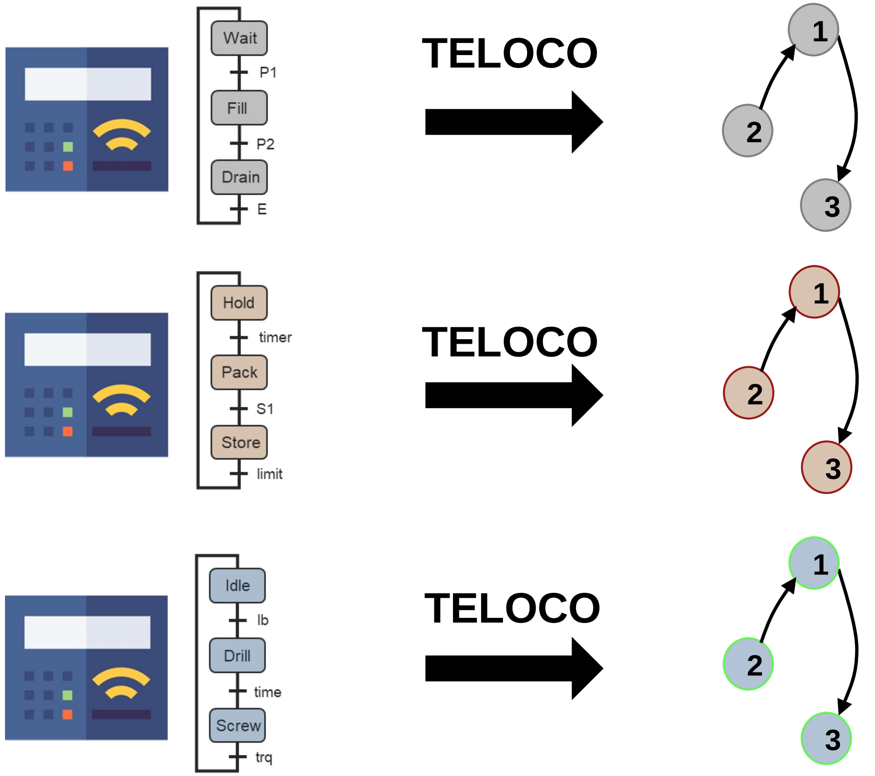


TELOCO

Stable Location Automaton (SLA)

SFC

Model Building



TELOCO

TELOCO

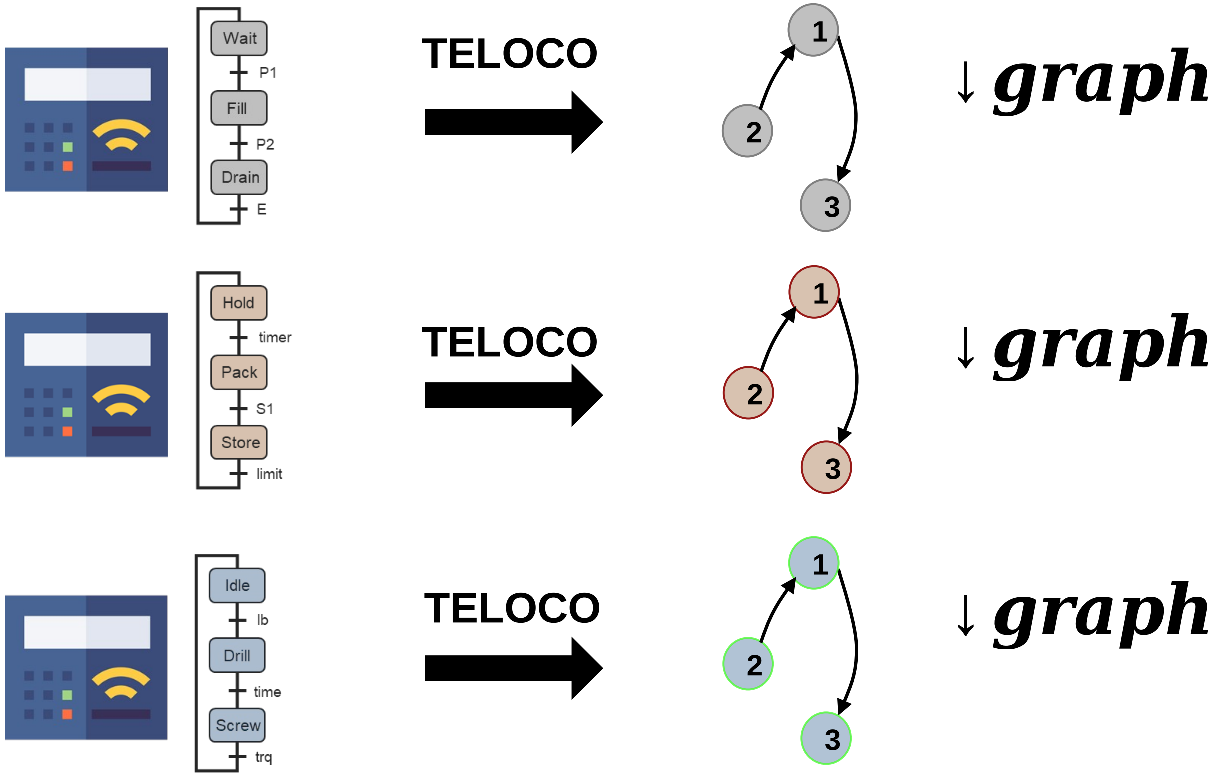
TELOCO

SFC

Stable Location Automaton (SLA)

Decomposition

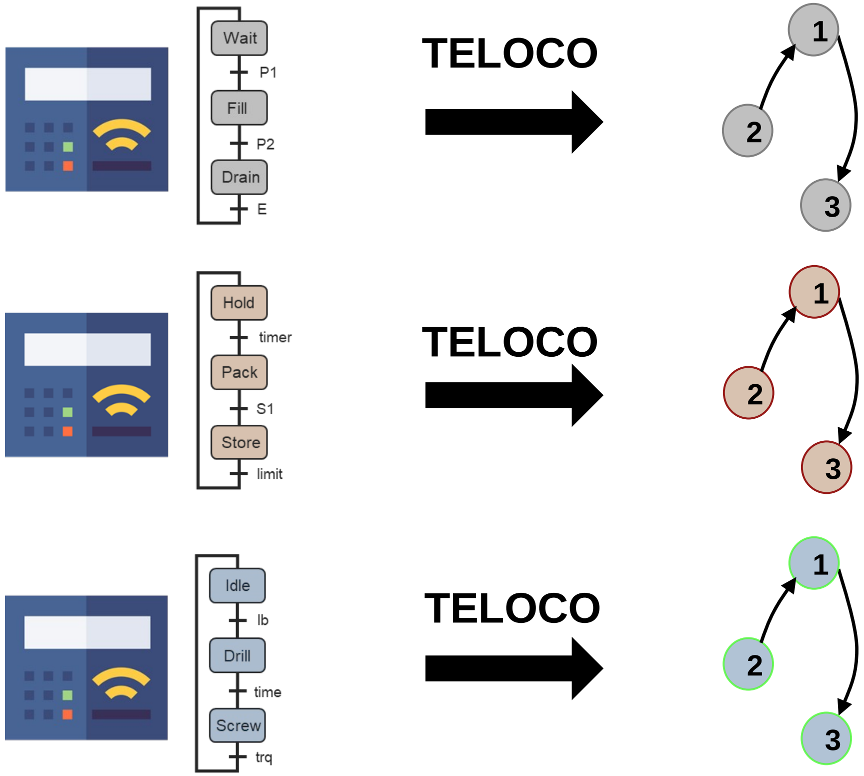
Model Building



SFC

Stable Location Automaton (SLA)

Model Building



$\downarrow graph$

$2^{\downarrow Tr}$

$\downarrow graph$

$2^{\downarrow Tr}$

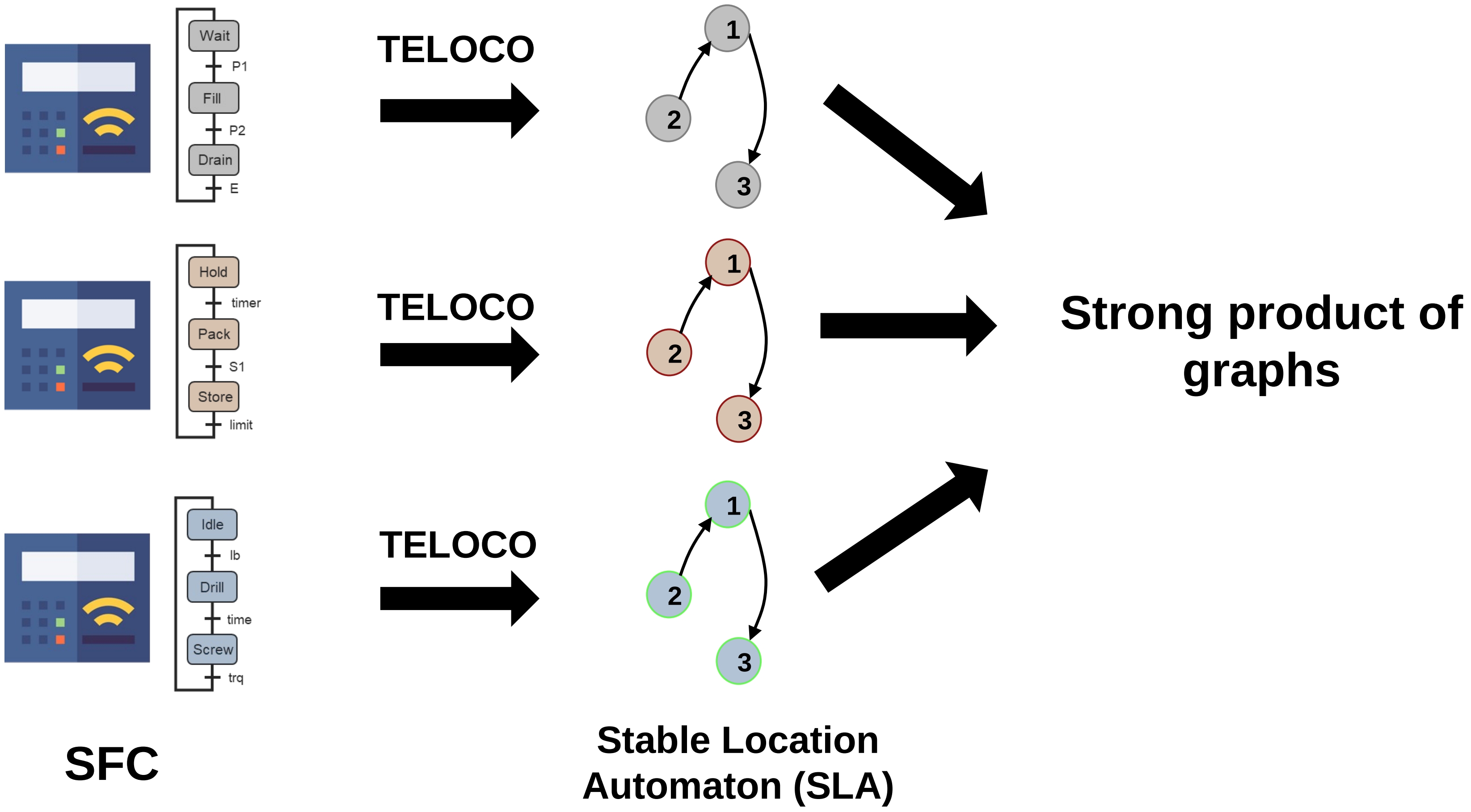
$\downarrow graph$

$2^{\downarrow Tr}$

SFC

Stable Location Automaton (SLA)

Model Building



TELOCO

TELOCO

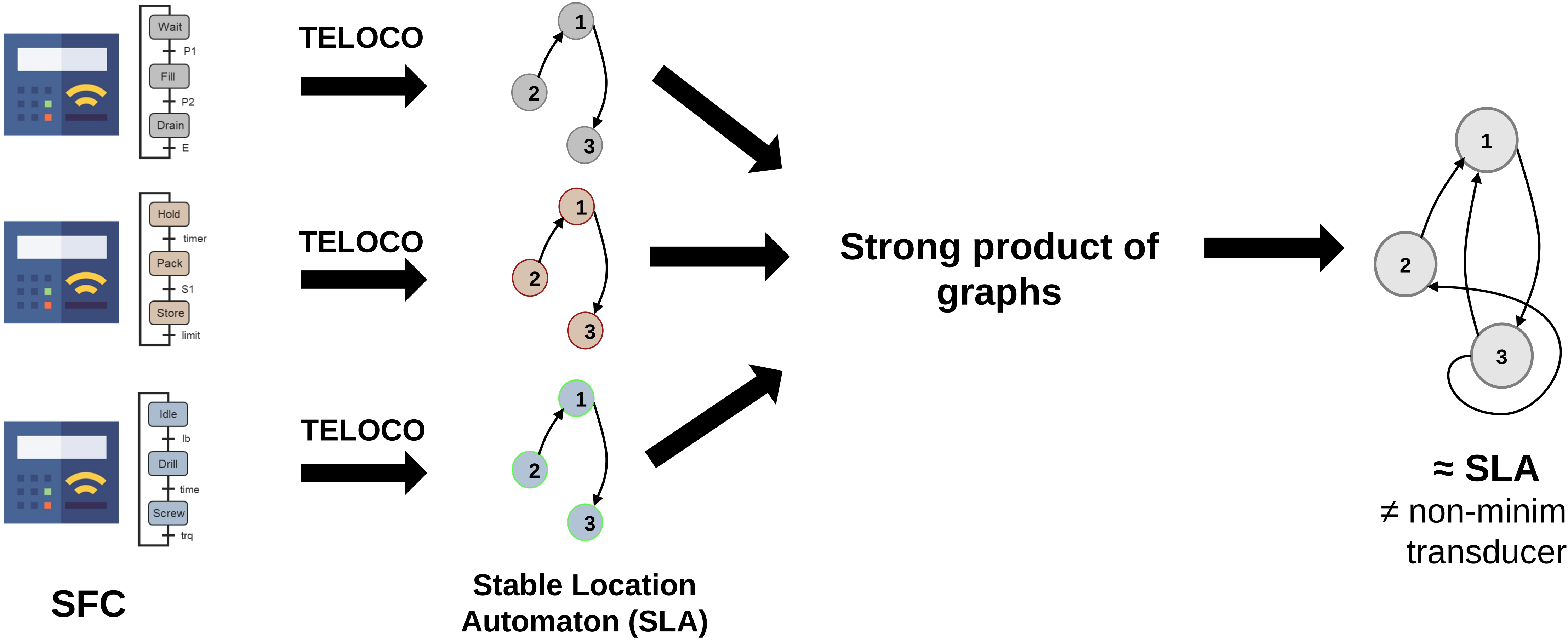
TELOCO

Strong product of graphs

SFC

Stable Location Automaton (SLA)

Model Building



TELOCO

TELOCO

TELOCO

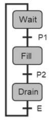
SFC

Stable Location Automaton (SLA)

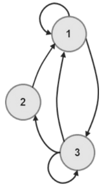
Strong product of graphs

≈ SLA

≠ non-minimal transducer

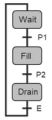


Model Building

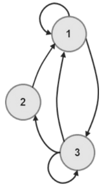


	Strong Product	SLA
4 graphs	2 636 ms	1 091 838 ms
5 graphs	43 420 ms	X
6 graphs	2 223 811 ms	X
8 graphs	X	X

Memory limitation
(375Gb RAM)



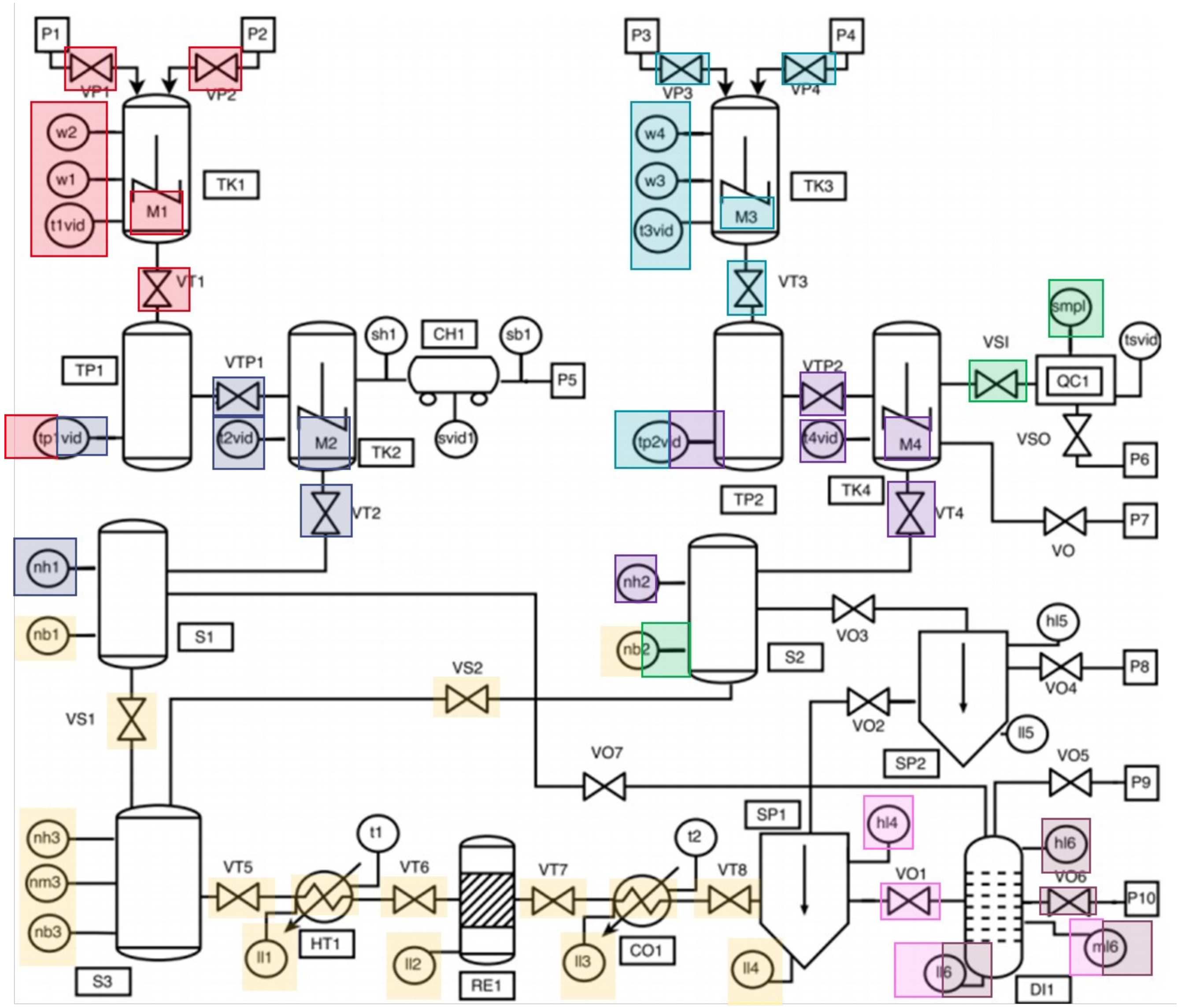
Model Building



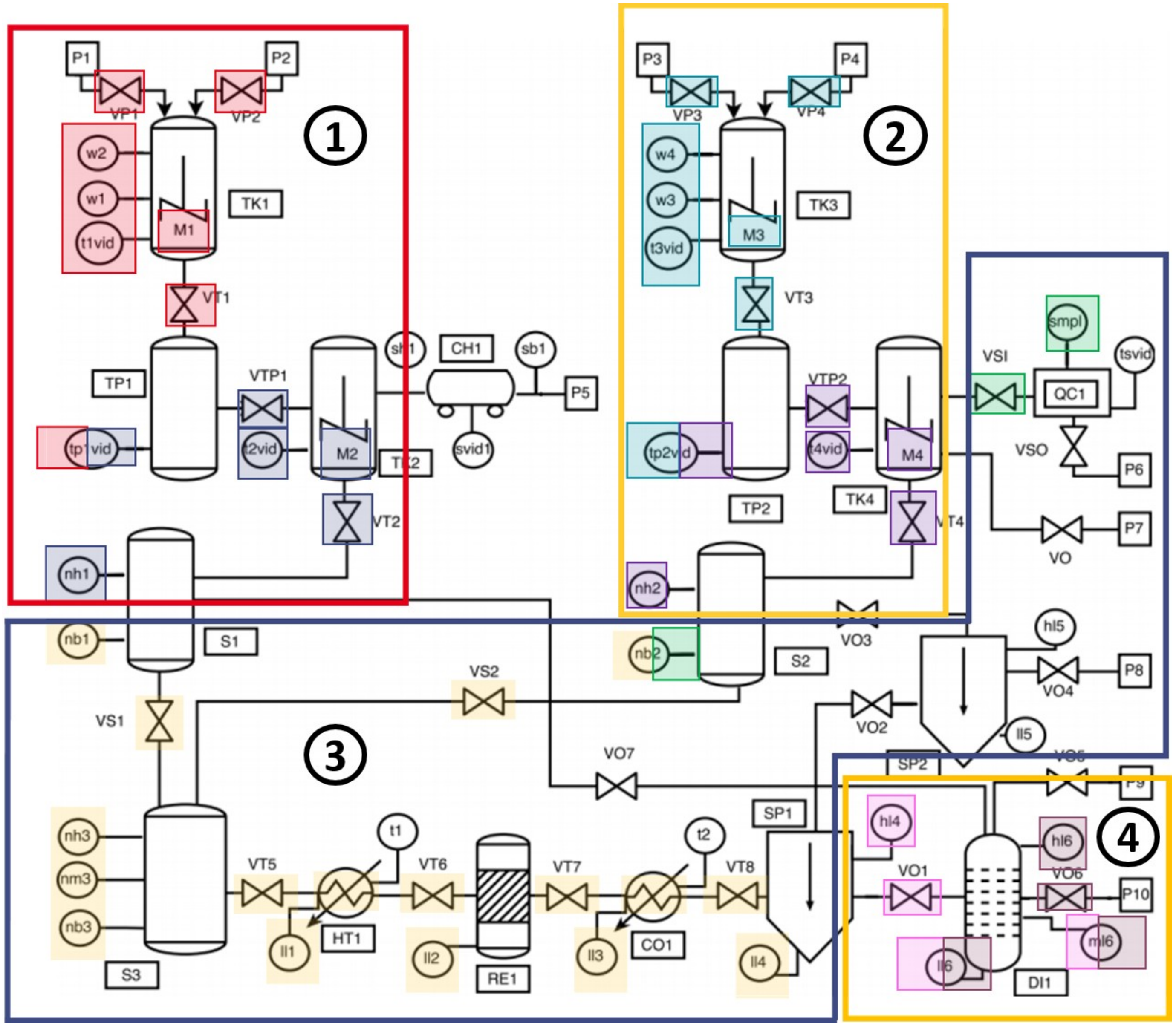
	Strong Product	SLA
4 graphs	2 636 ms	1 091 838 ms
5 graphs	43 420 ms	X
6 graphs	2 223 811 ms	X
8 graphs	X	X

→ **Decomposition into sub-processes**

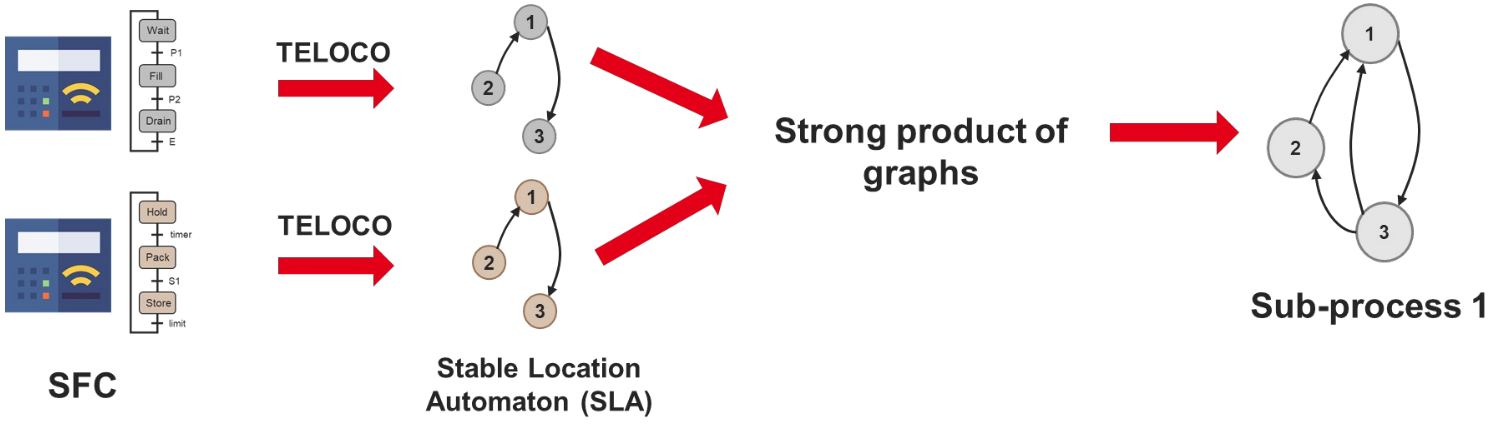
Model Building



Model Building



Model Building



SFC

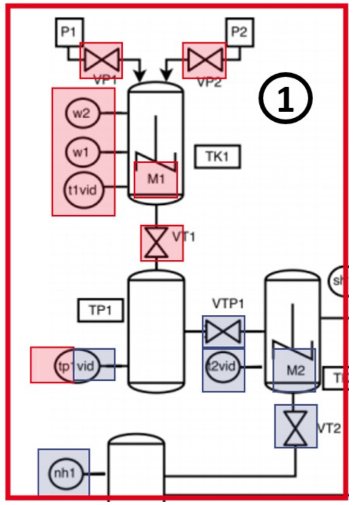
TELOCO

TELOCO

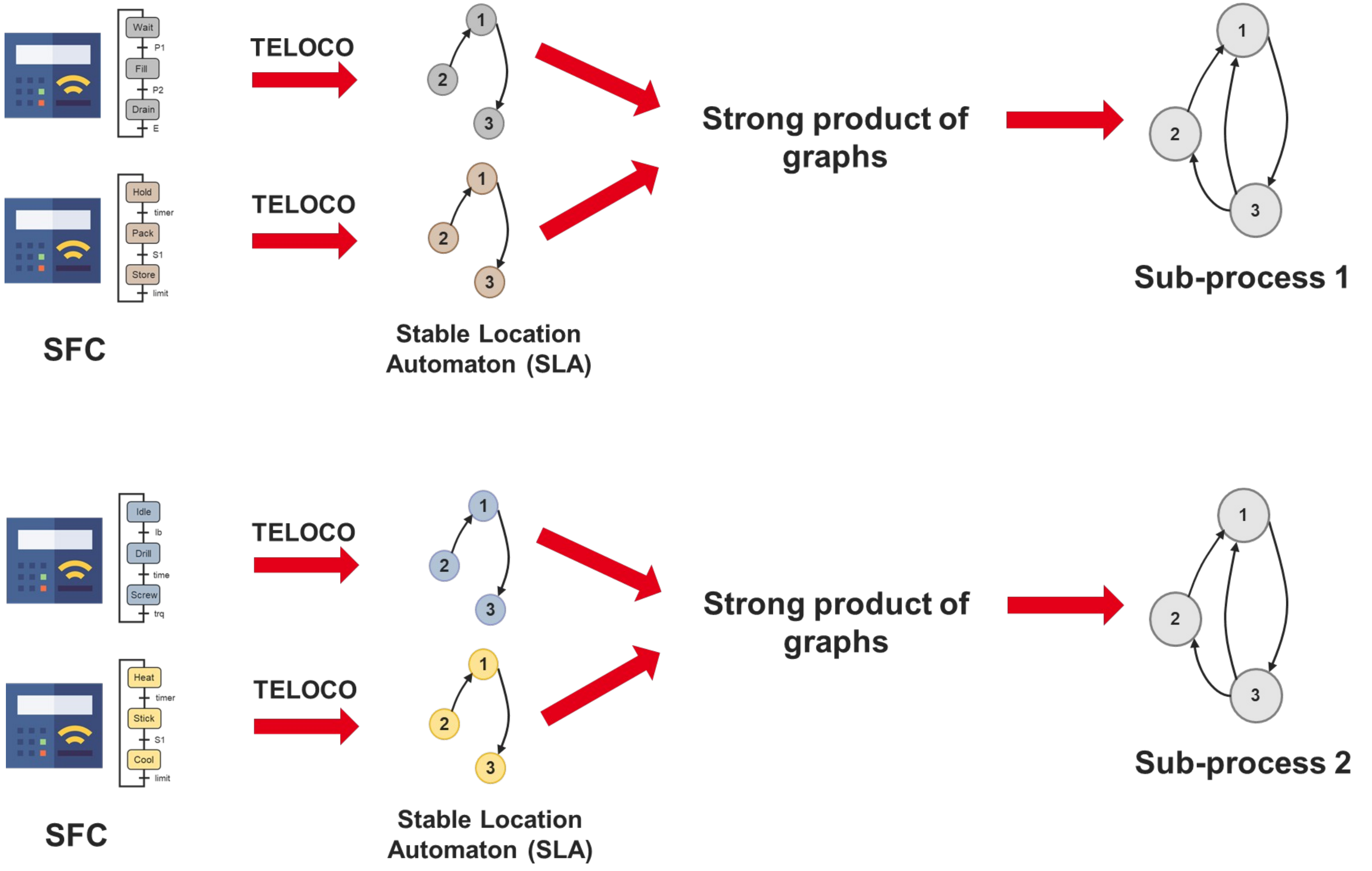
Stable Location Automaton (SLA)

Strong product of graphs

Sub-process 1



Model Building



TELOCO

TELOCO

TELOCO

TELOCO

SFC

SFC

Stable Location Automaton (SLA)

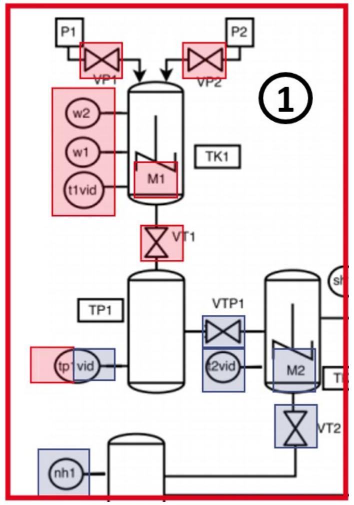
Stable Location Automaton (SLA)

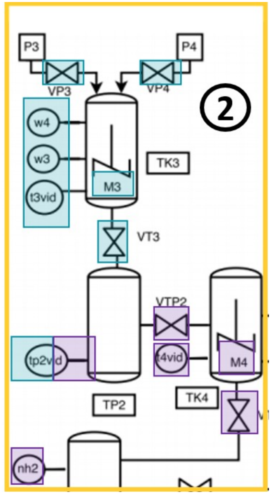
Strong product of graphs

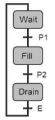
Strong product of graphs

Sub-process 1

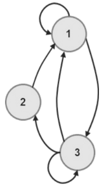
Sub-process 2

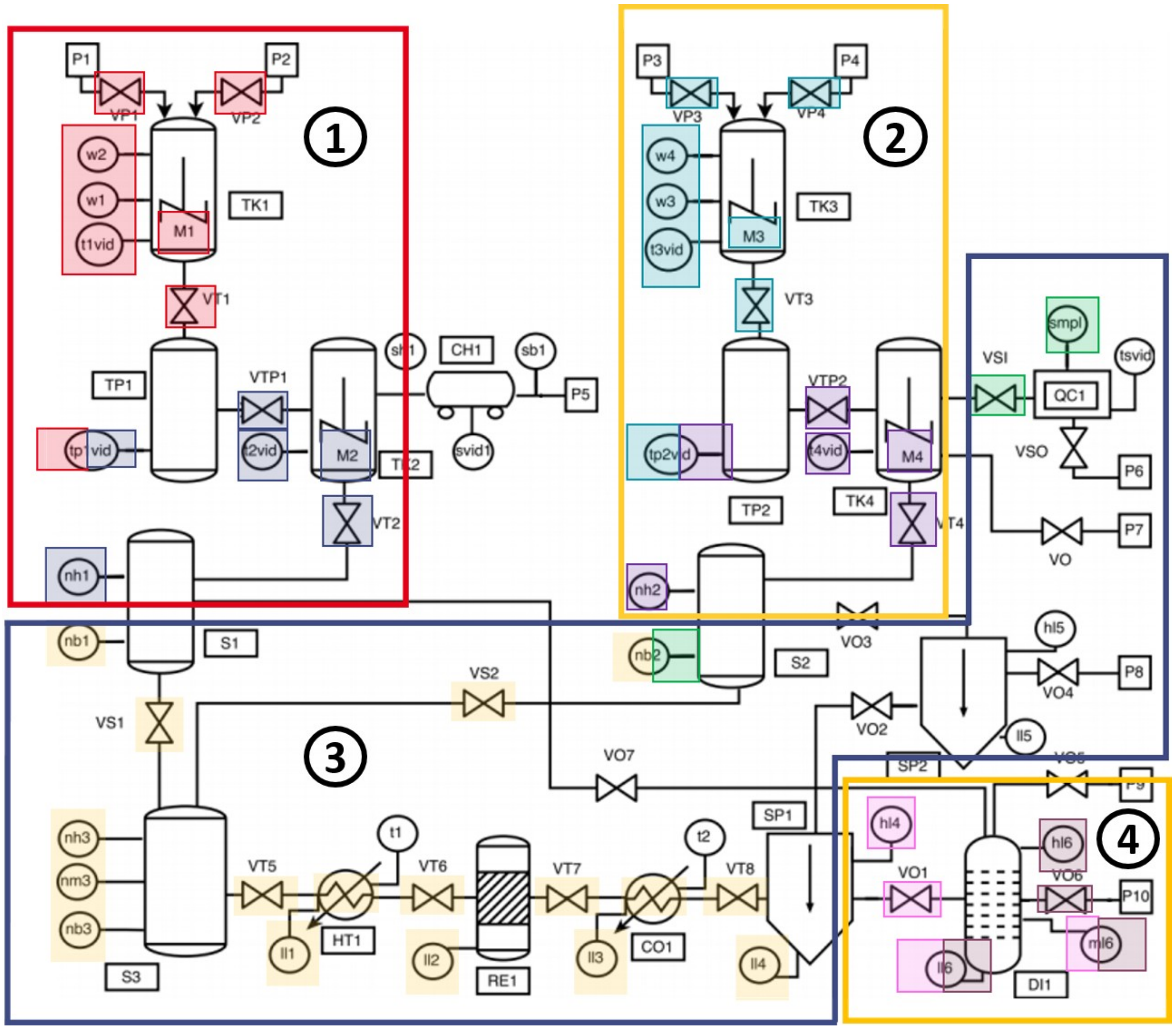




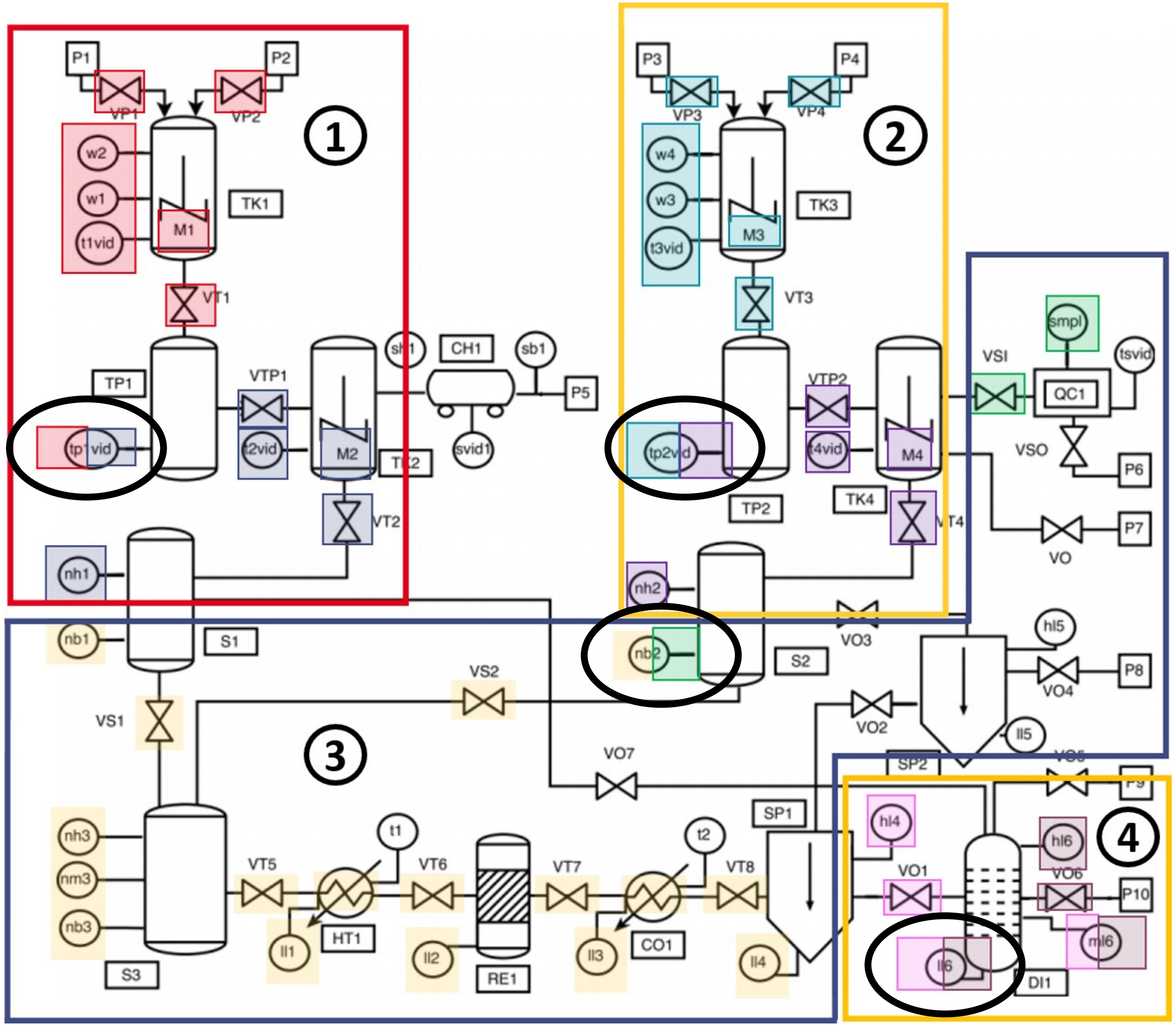


Model Building

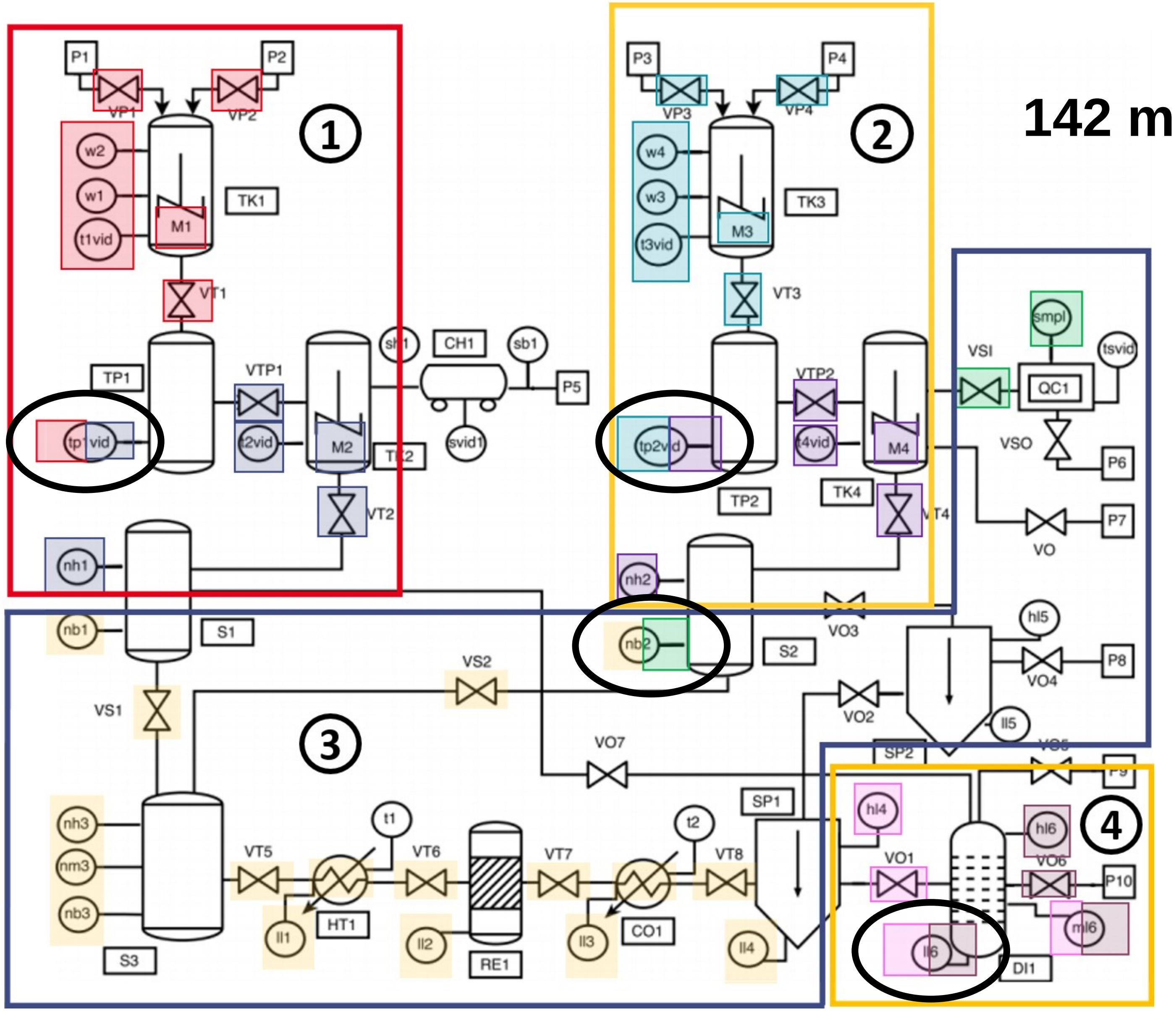




Model Building



Model Building



156 ms

142 ms

319 ms

133 ms

Model Building

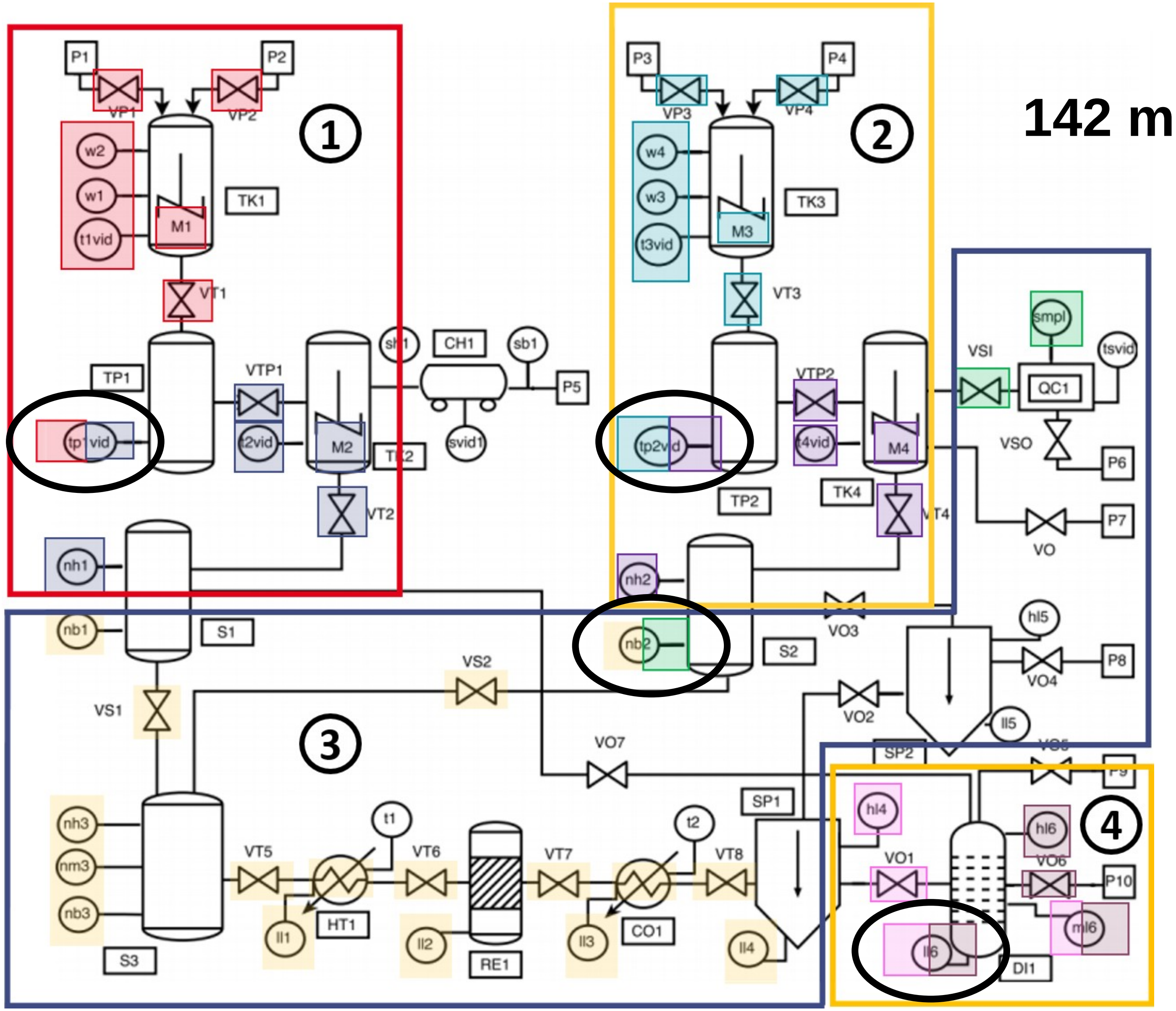
156 ms

142 ms

Global = 750 ms

319 ms

133 ms



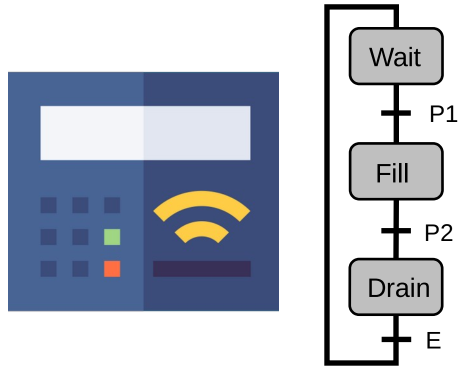
Contents

Identifying Cybersecurity Risk for System Safety

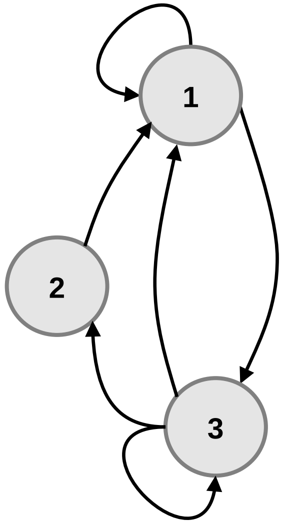
PLC-Logic Based Cybersecurity Risk Identification

- Model building
- Threat model application

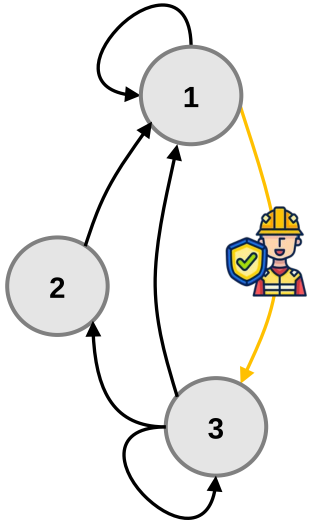
PLC-Logic Based Cybersecurity Risk Identification



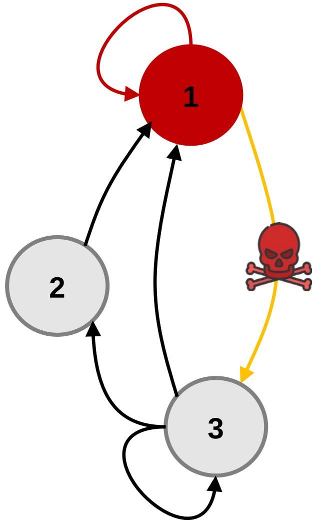
PLC logic



System model



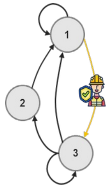
Safety



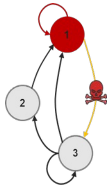
Attack scenarios

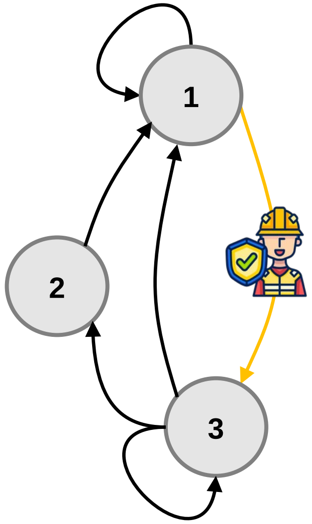
Model building

Threat model application

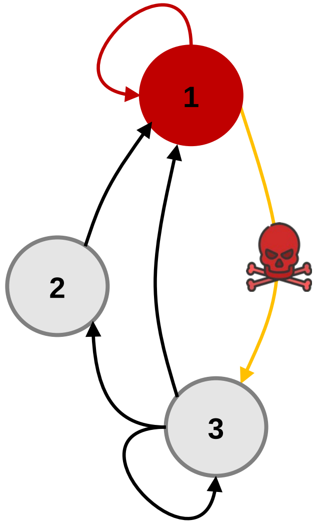


Threat model application



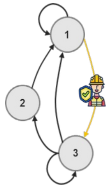


Safety



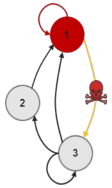
Attack scenarios

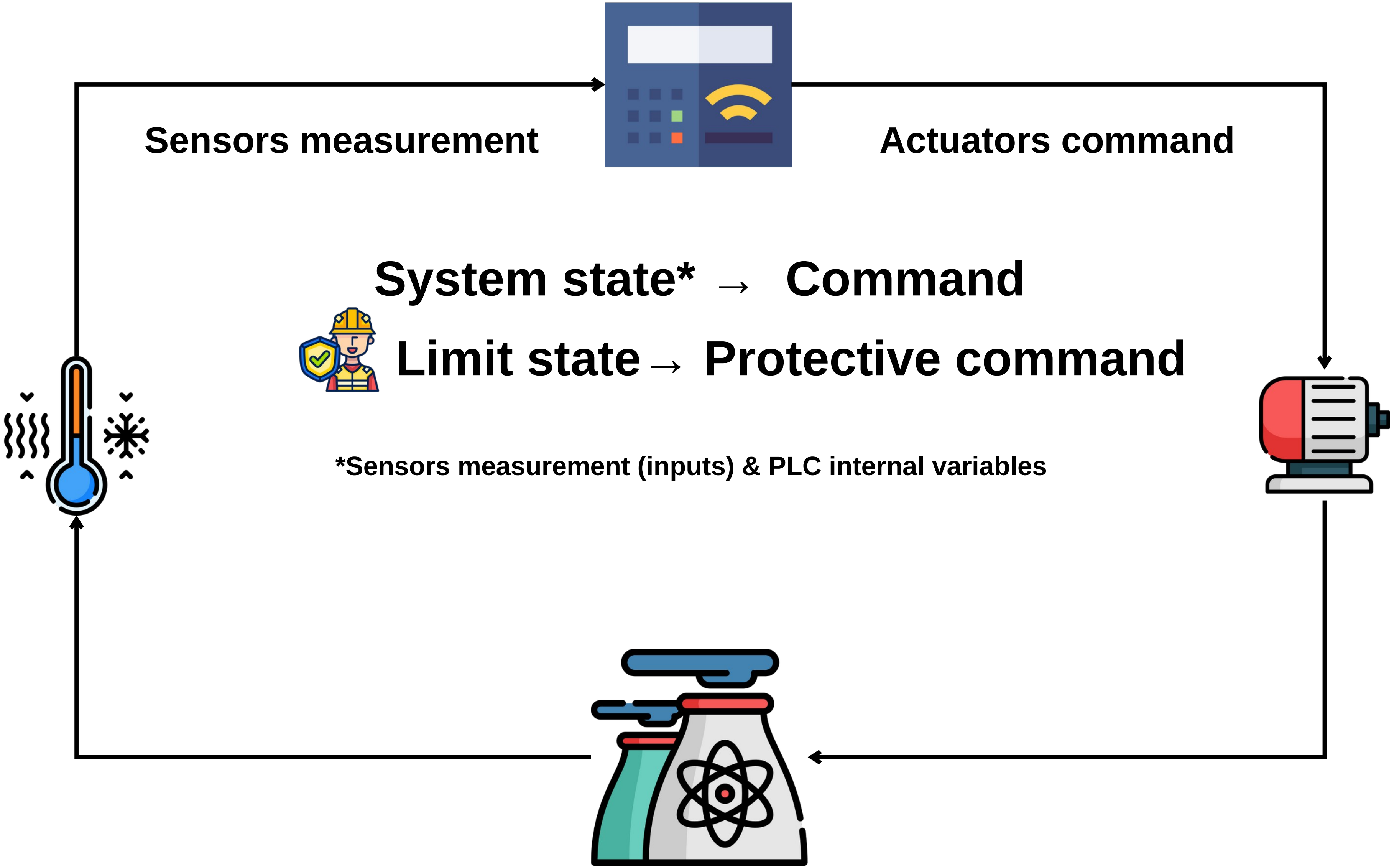
Threat model application



Threat model application

Threat model





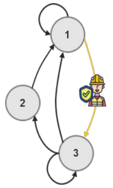
Sensors measurement

Actuators command

System state* → Command

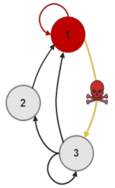
Limit state → Protective command

*Sensors measurement (inputs) & PLC internal variables

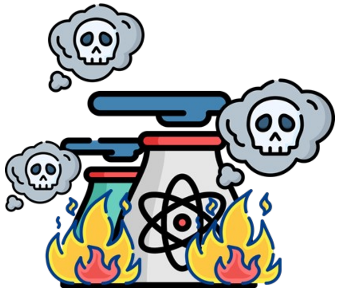


Threat model application

Threat model



Process Hazard Analysis (PHA)

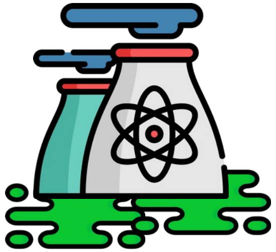


Sensor A & Actuator 1

Sensor A /Actuator 1

(Sensors B & /C) & /Actuator 2

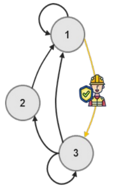
Sensors B & /C Actuator 2



Sensor D & (Actuators 3 | 4)

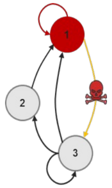
Sensor D /Actuator 3 & /Actuator 4

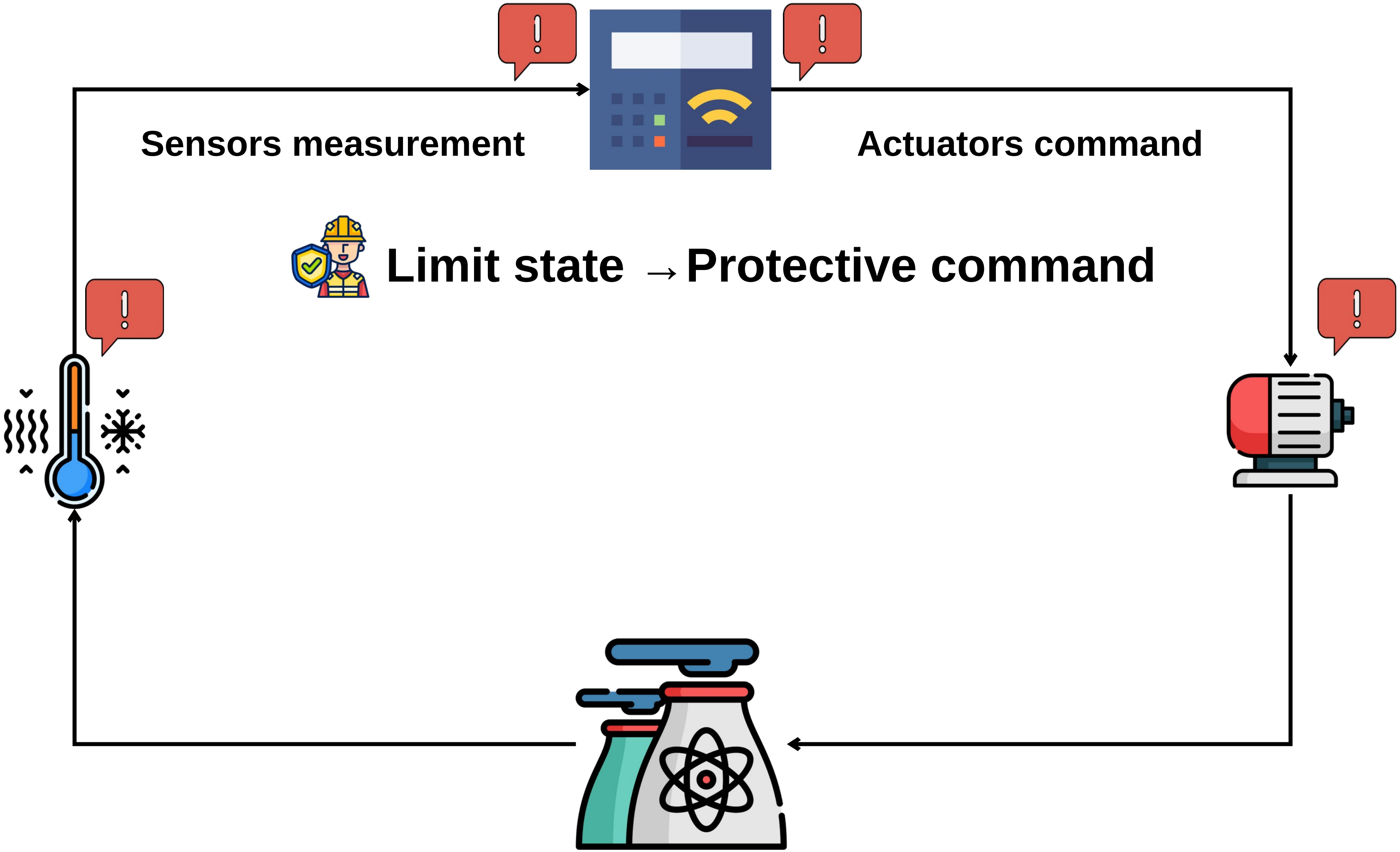
Limit state → Protective command



Threat model application

Threat model

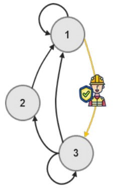




Sensors measurement

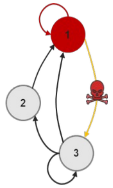
Actuators command

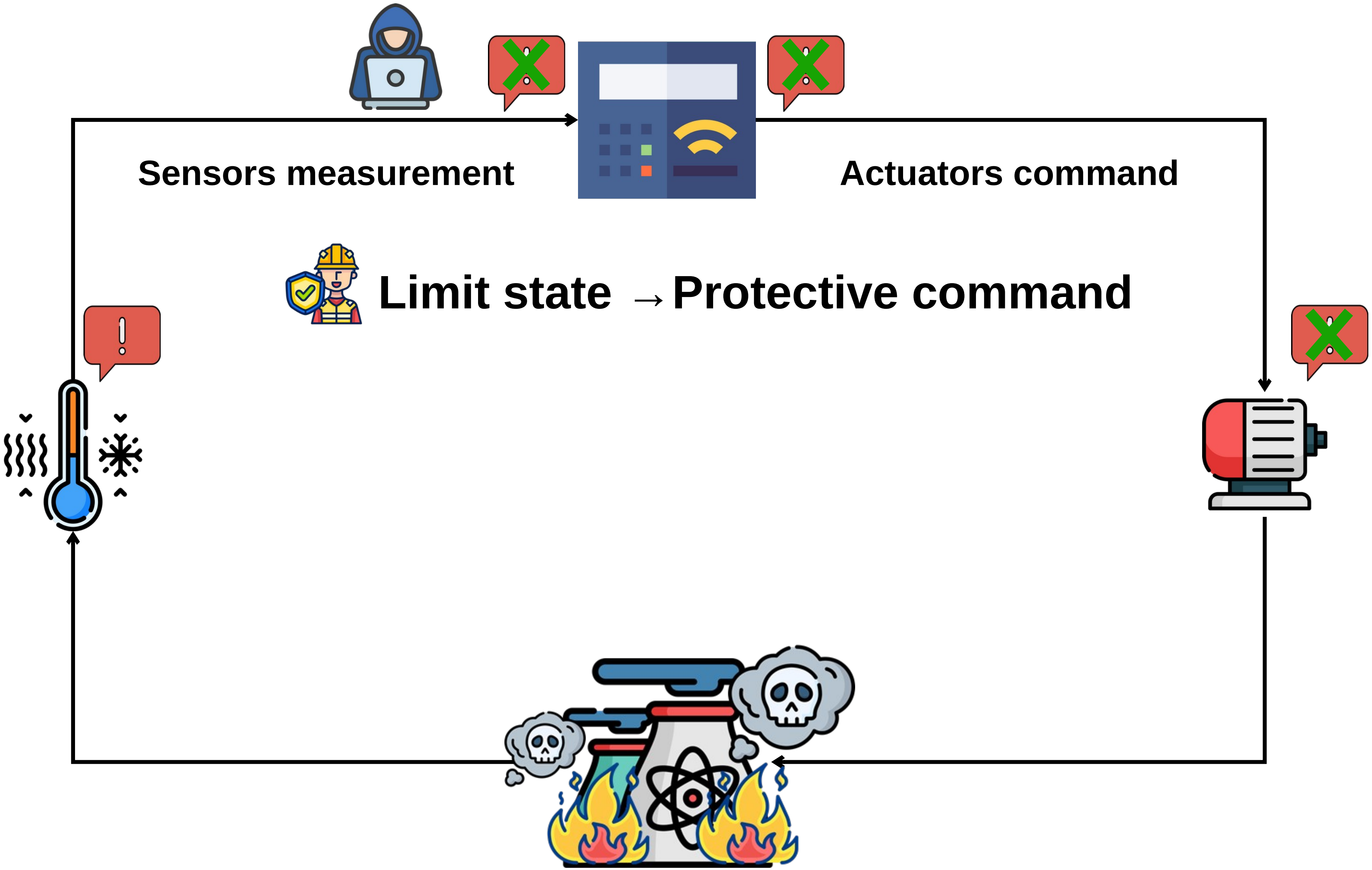
Limit state → Protective command



Threat model application

Threat model

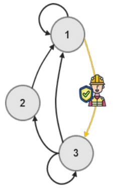




Sensors measurement

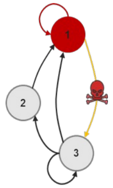
Actuators command

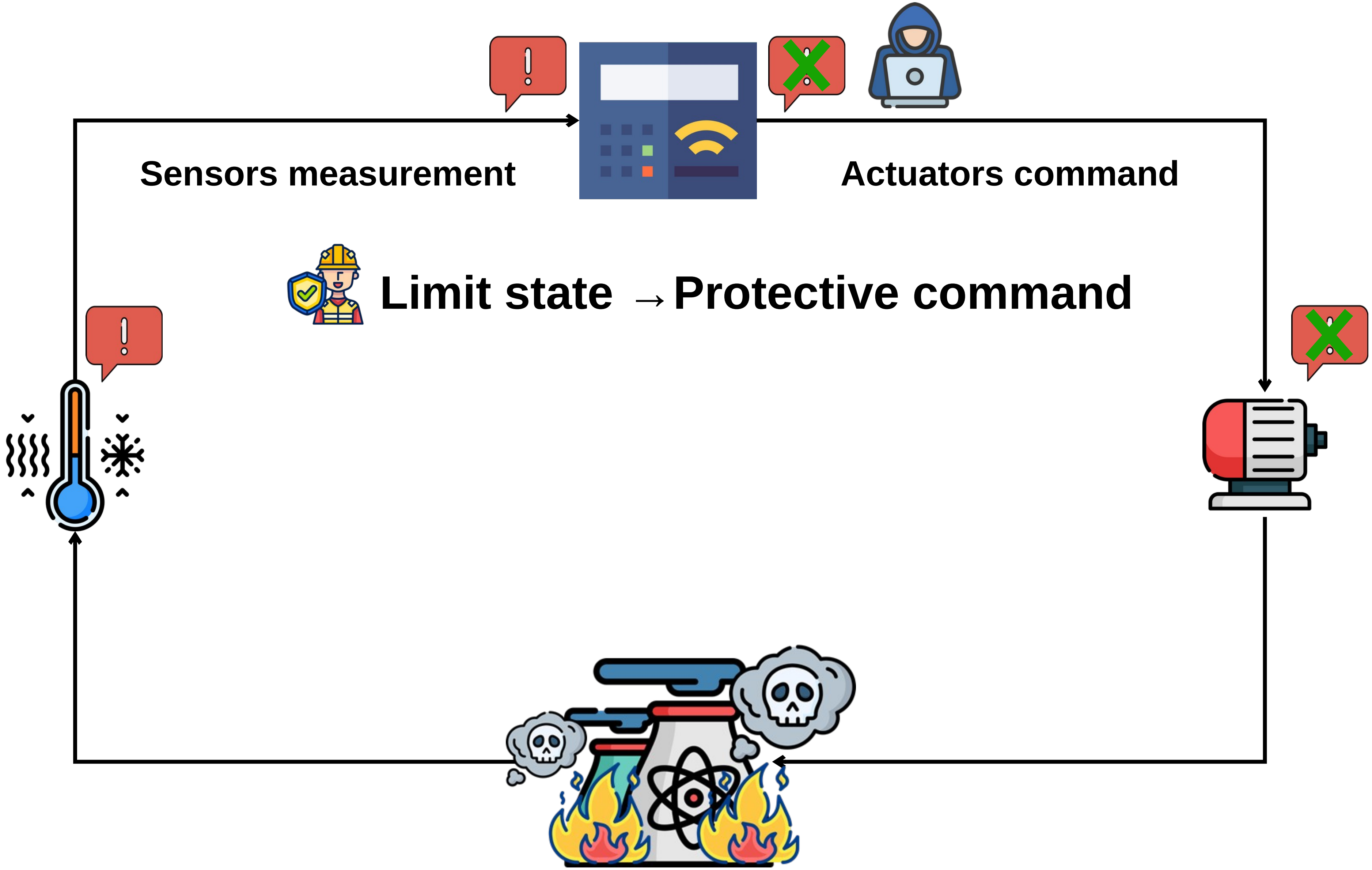
Limit state → Protective command



Threat model application

Threat model

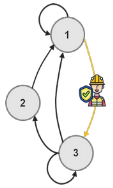




Sensors measurement

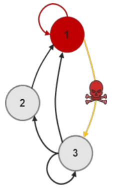
Actuators command

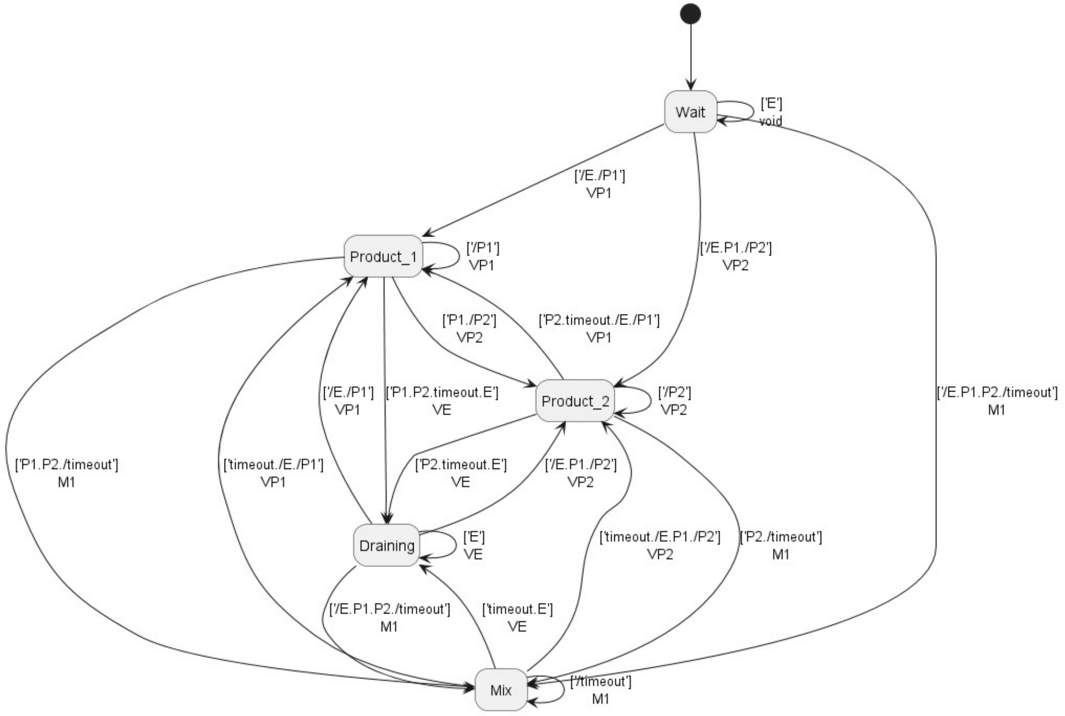
Limit state → Protective command

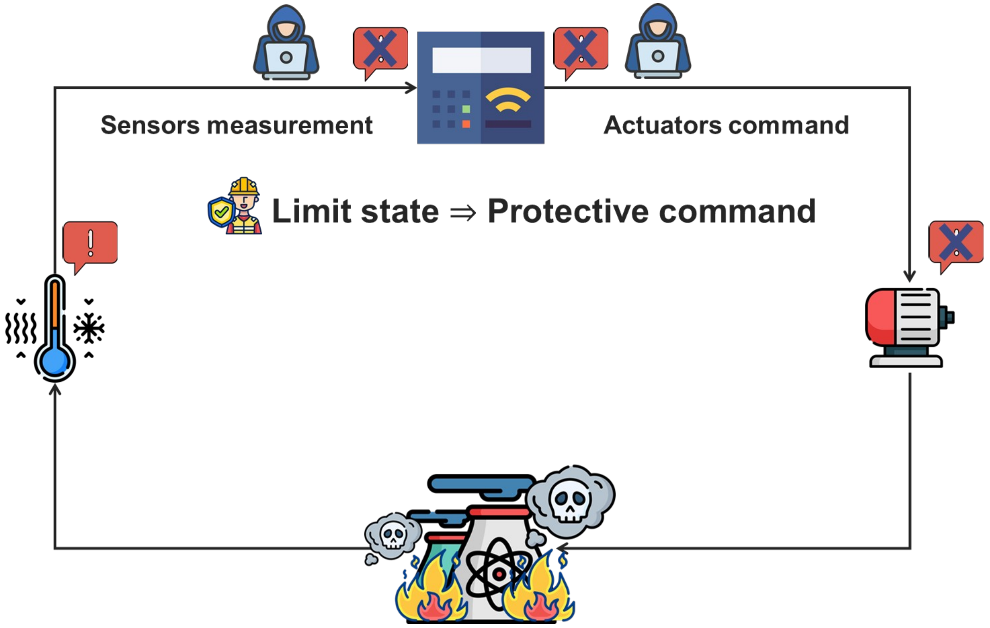


Threat model application

Application



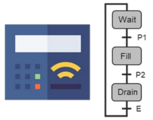




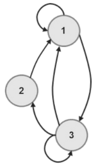
?

System Model ⟷ **Threat Model**

Threat model application



PLC logic



System model

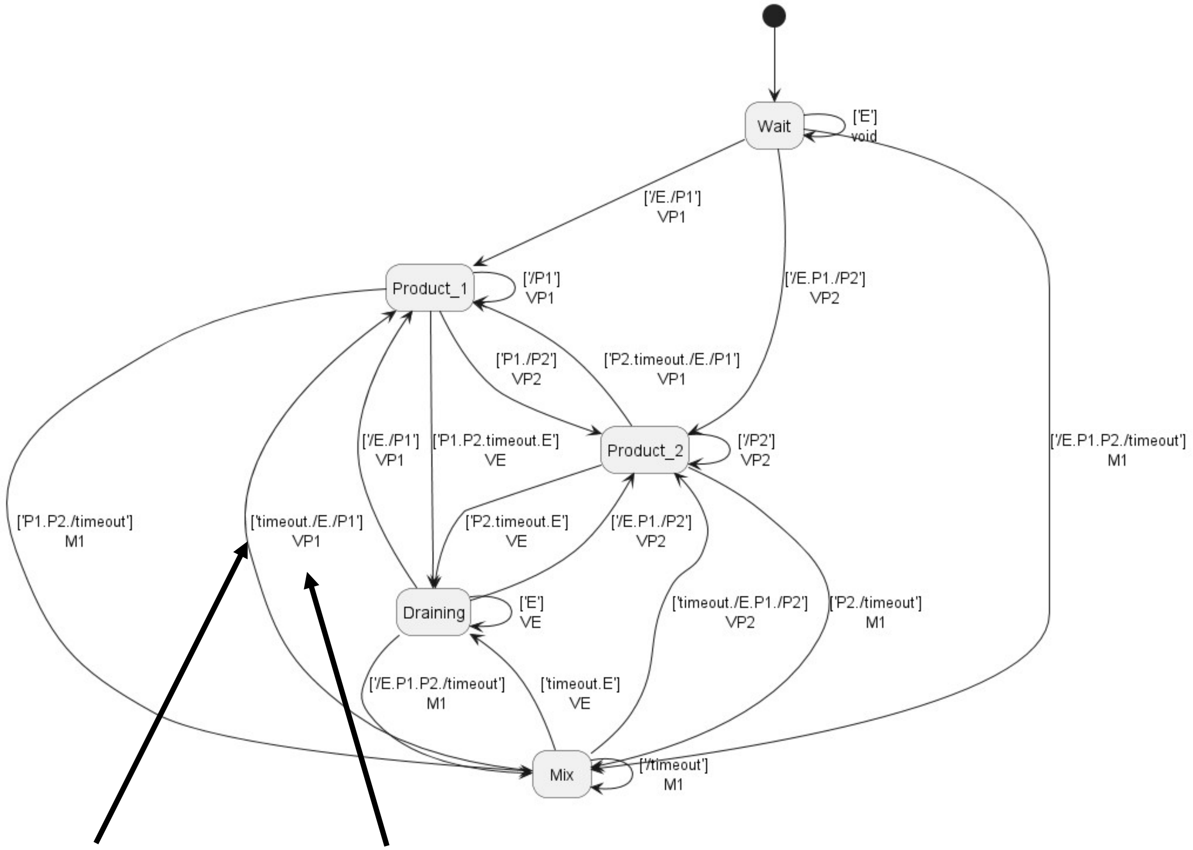
Threat model application

Application

Inputs ⟹ Outputs

↓ ↓

Limit state → Protective command

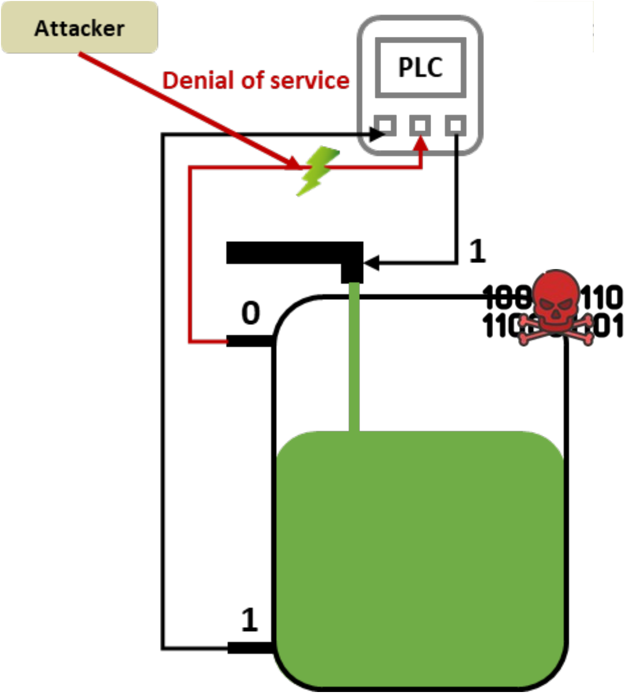


Inputs ⟹ Outputs ➡ SLA transition

Threat model application

Application

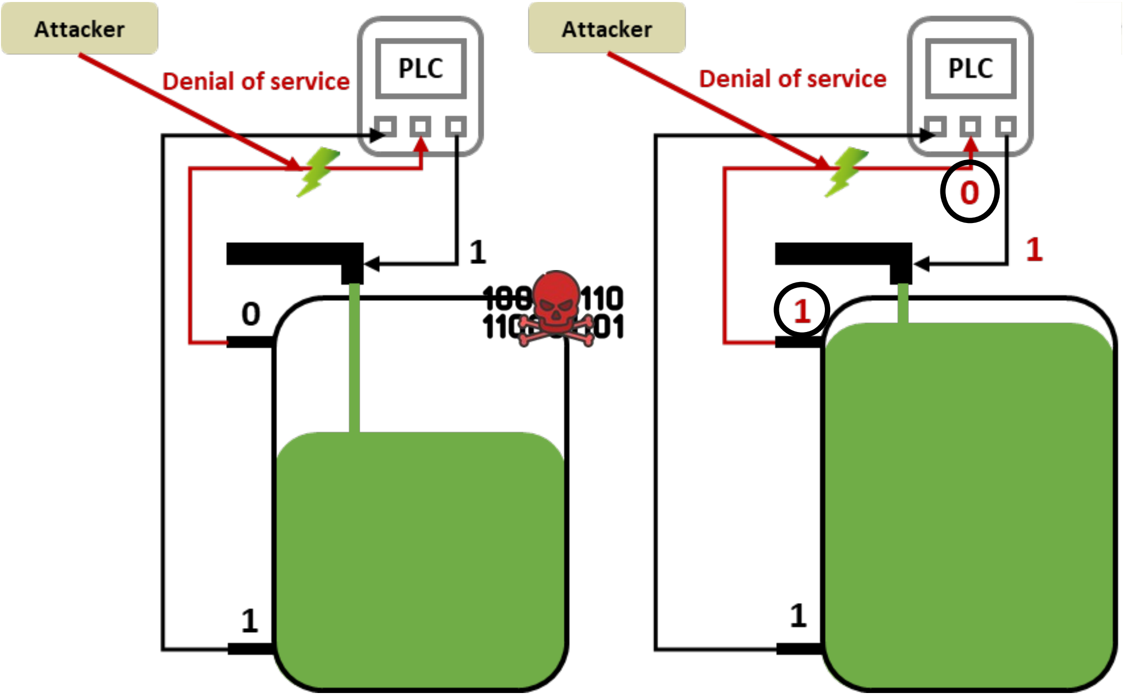
Block a state change



Threat model application

Application

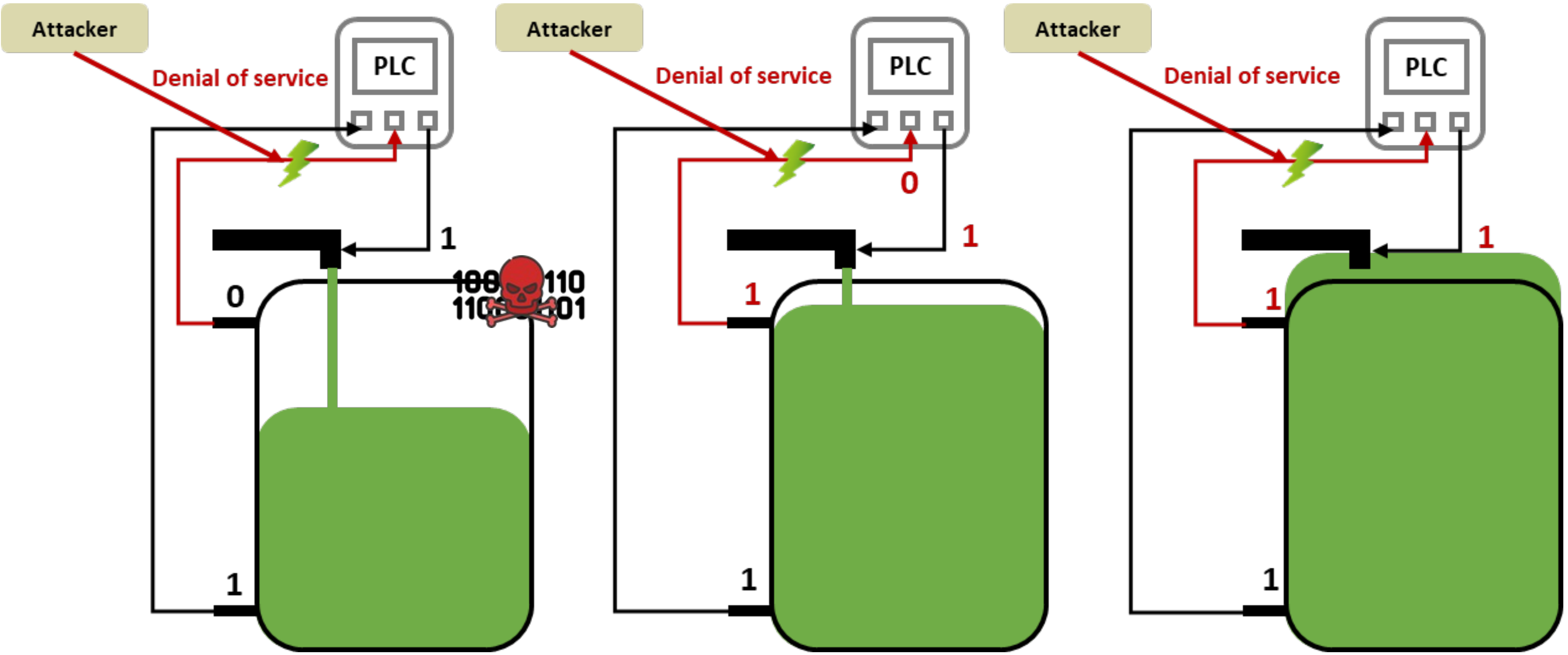
Block a state change

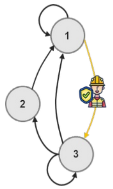


Threat model application

Application

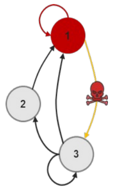
Block a state change



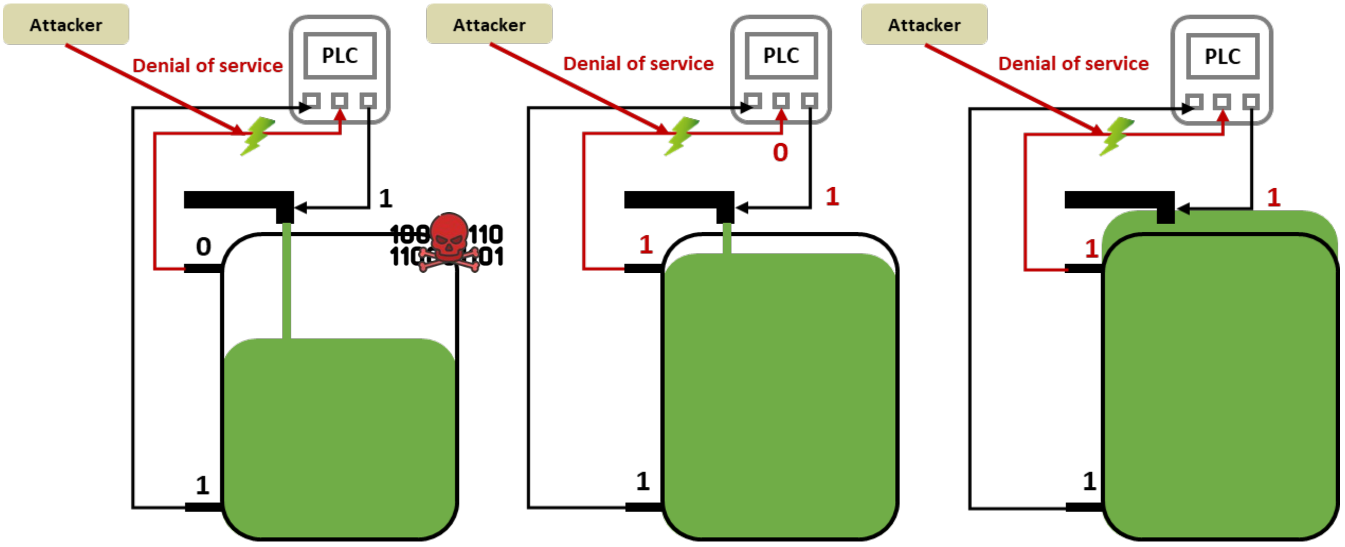


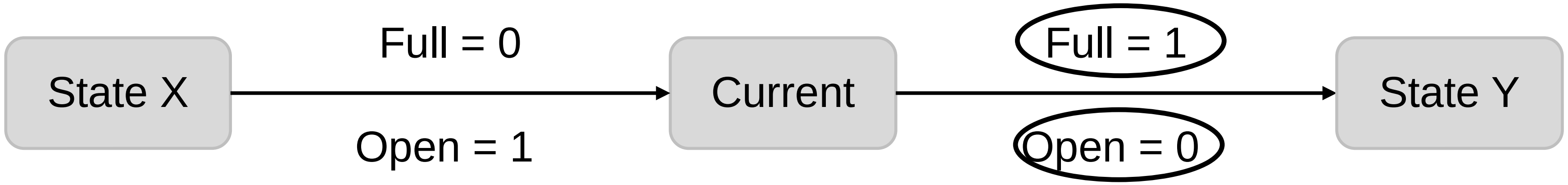
Threat model application

Application



Block a state change



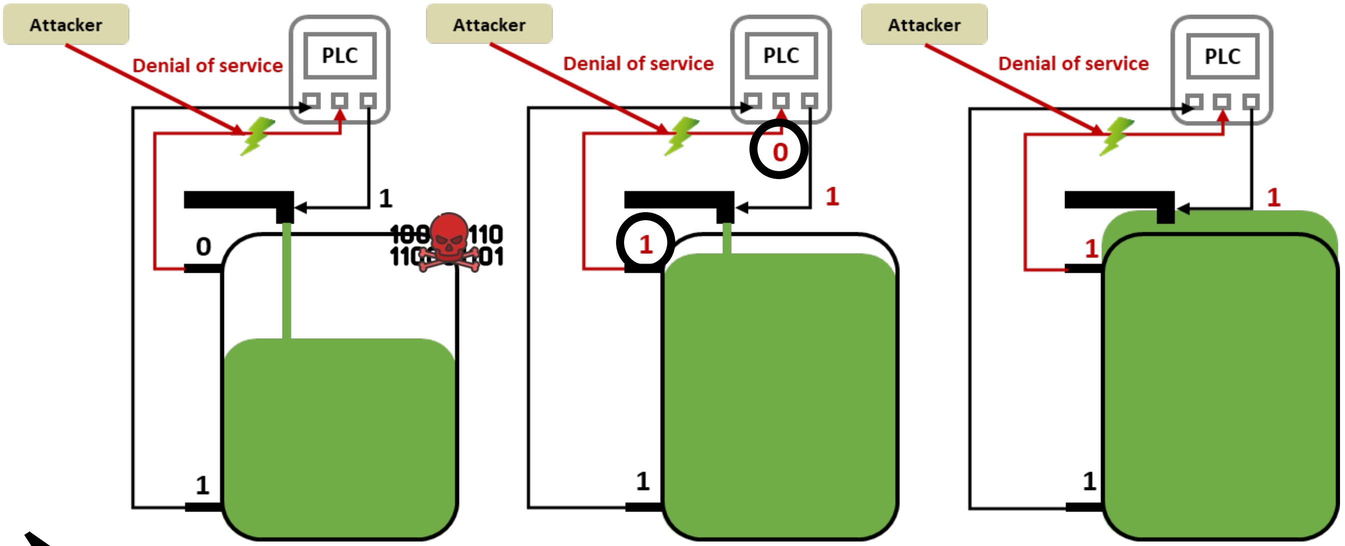


Limit state ⇒ Protective command

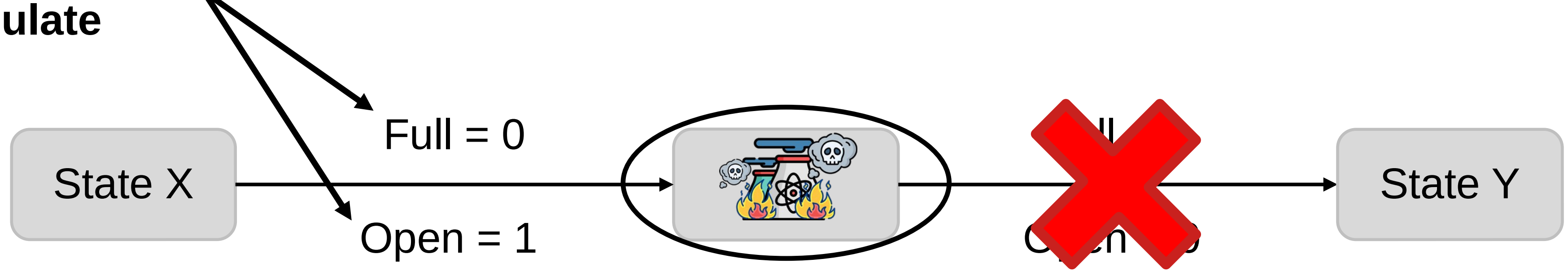
Threat model application

Application

Block a state change



Variables to manipulate

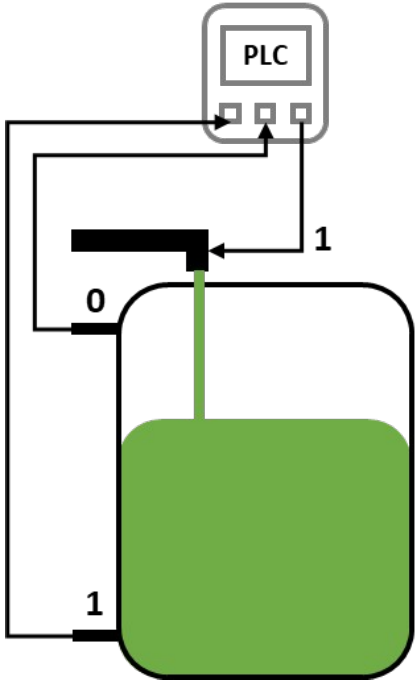


Limit state ⇒ Protective command

Threat model application

Application

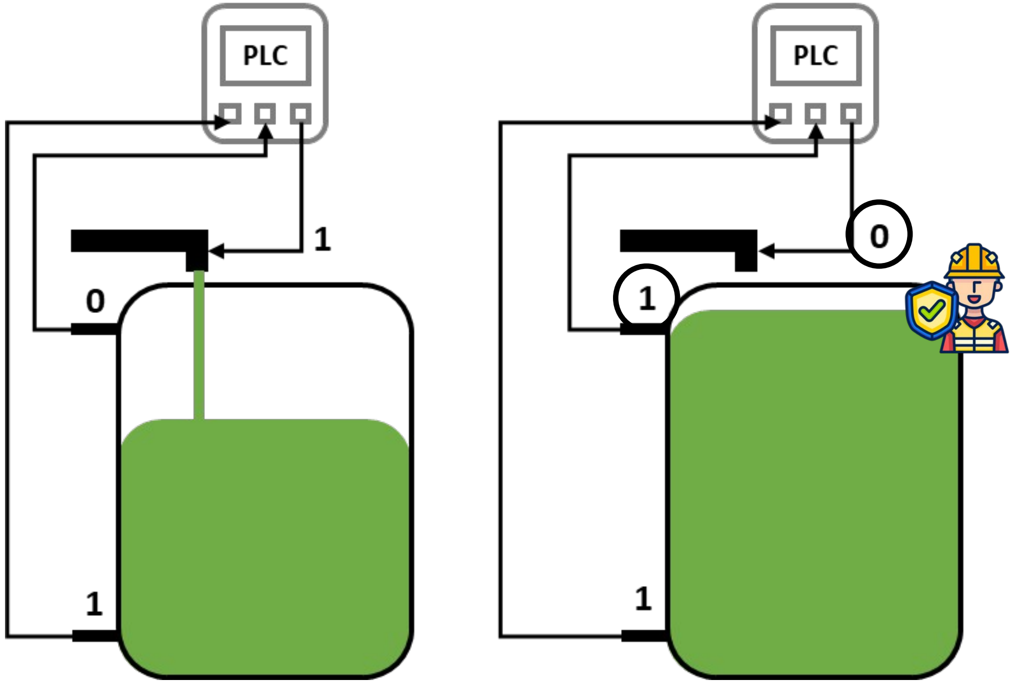
Force a state change



Threat model application

Application

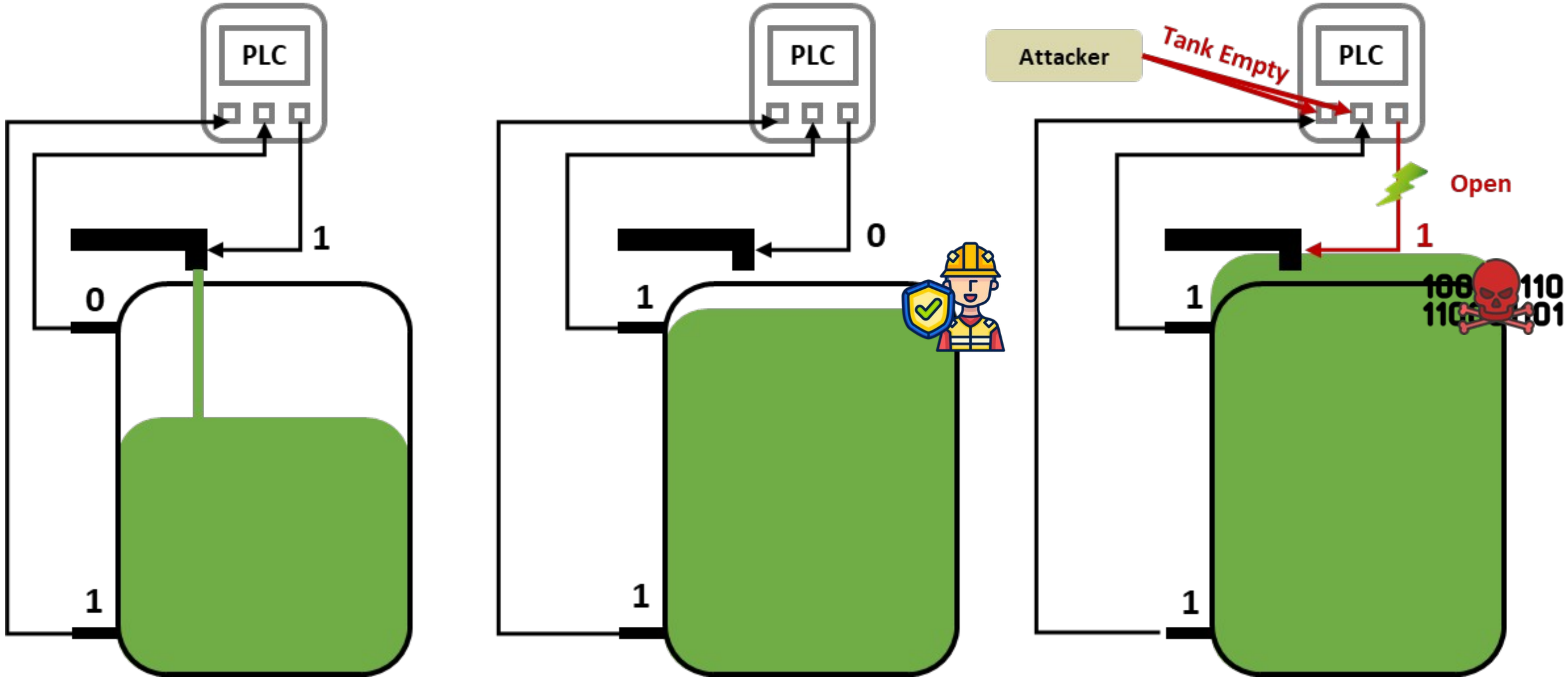
Force a state change

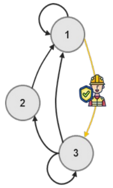


Threat model application

Application

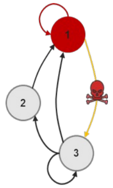
Force a state change



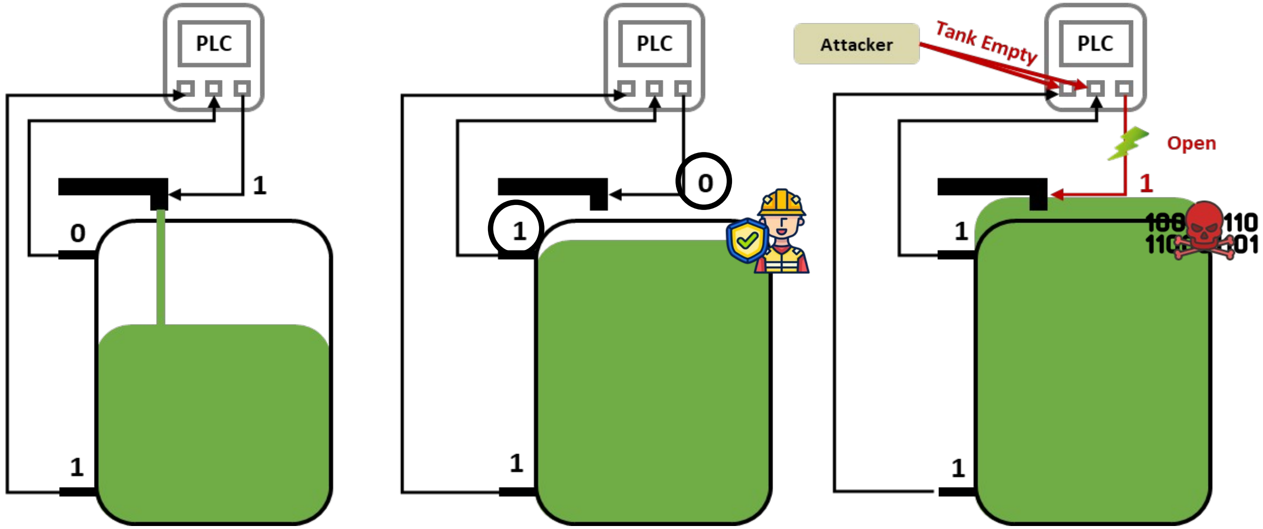


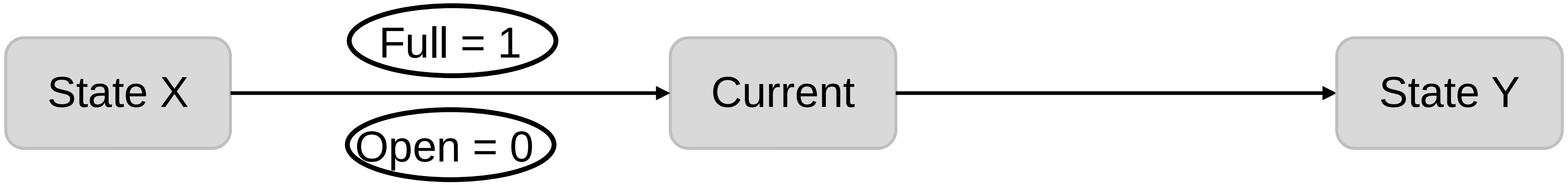
Threat model application

Application



Force a state change



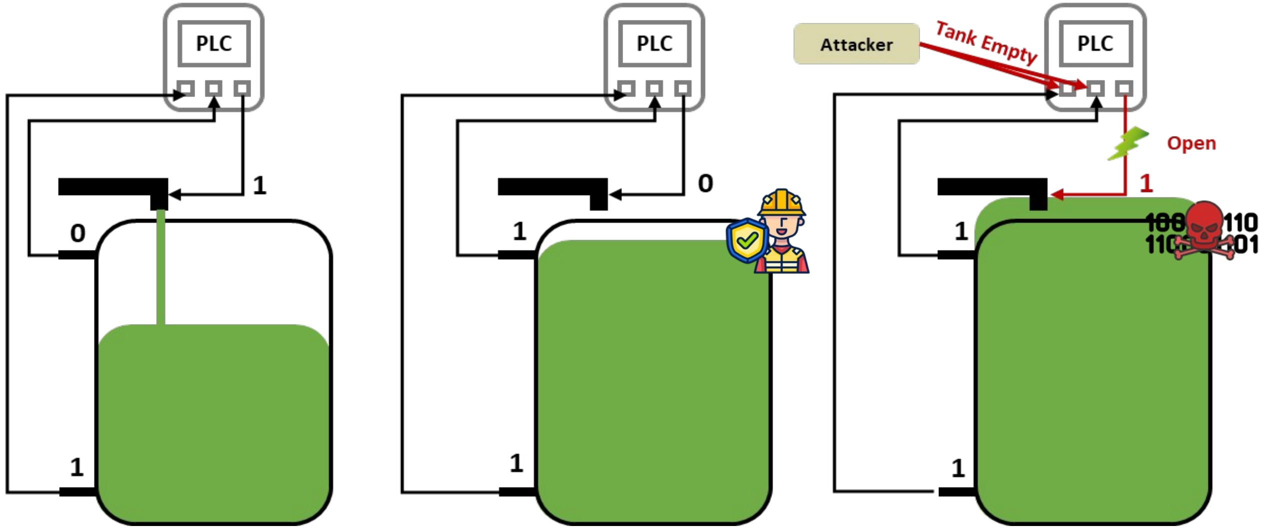


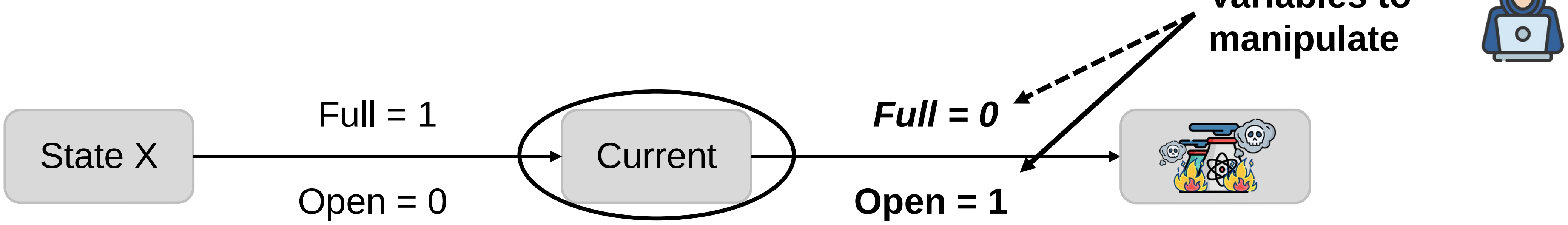
Limit state ⇒ Protective command

Threat model application

Application

Force a state change

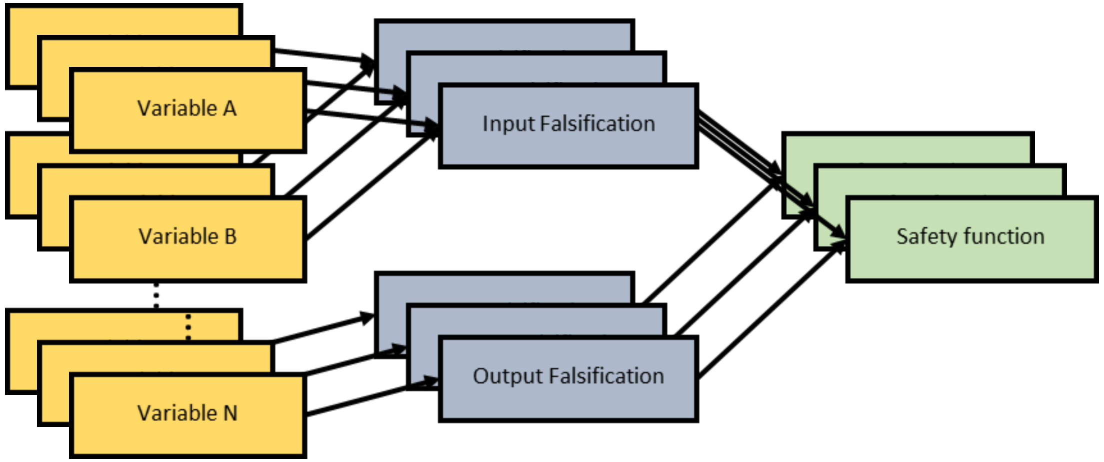




Limit state ⇒ Protective command

Threat model application

Application

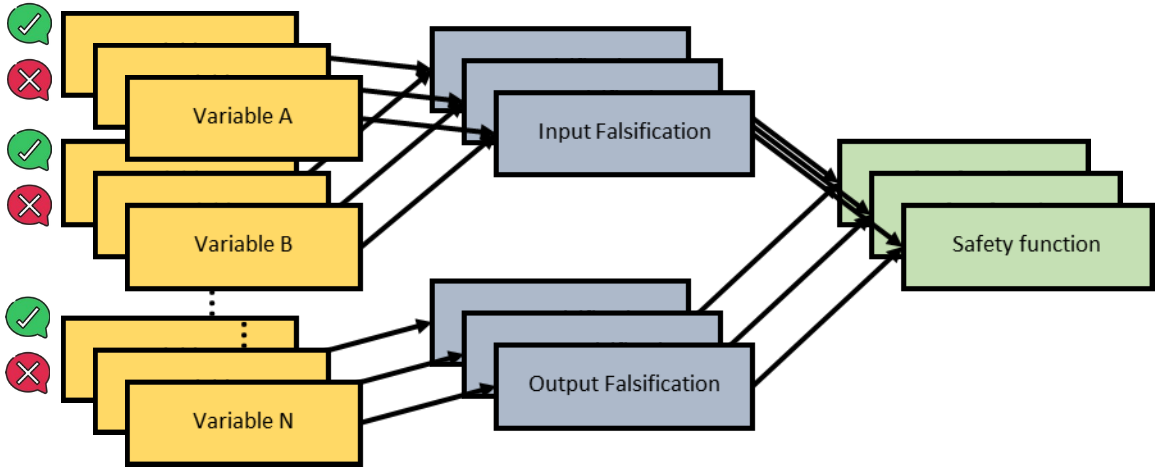


Theoretical Attack Scenarios

Threat model application

Application

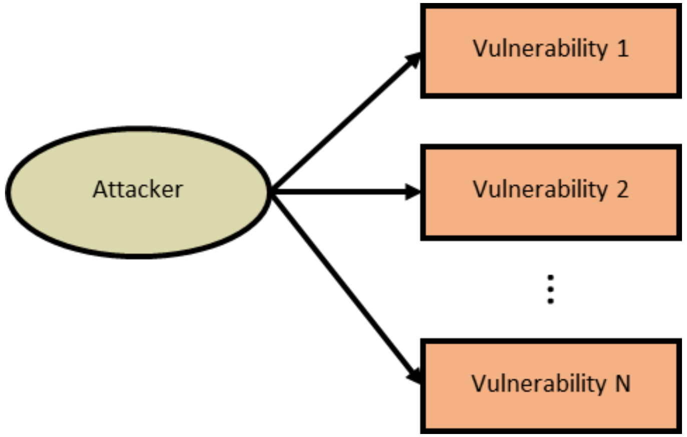
Realizable?



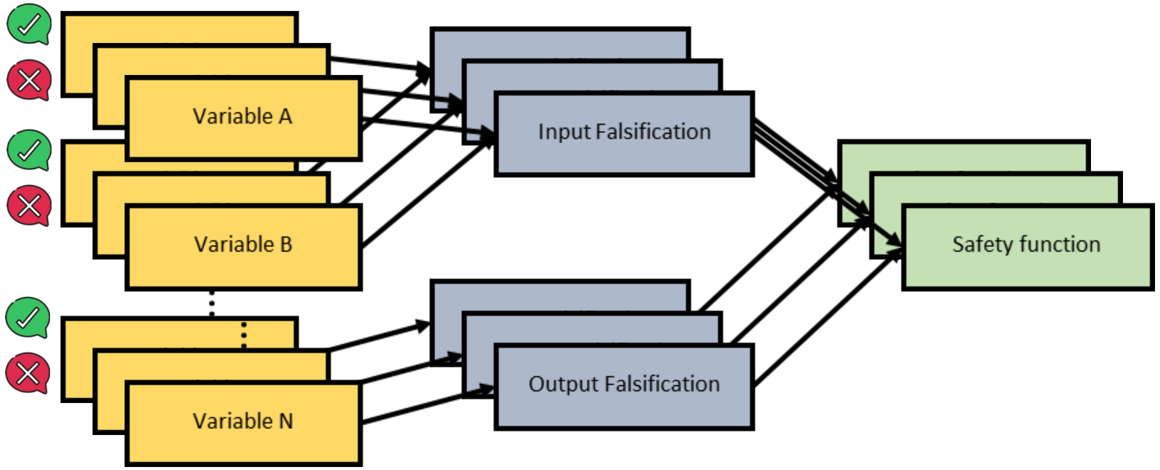
Theoretical
Attack Scenarios

Threat model application

Application



Realizable?

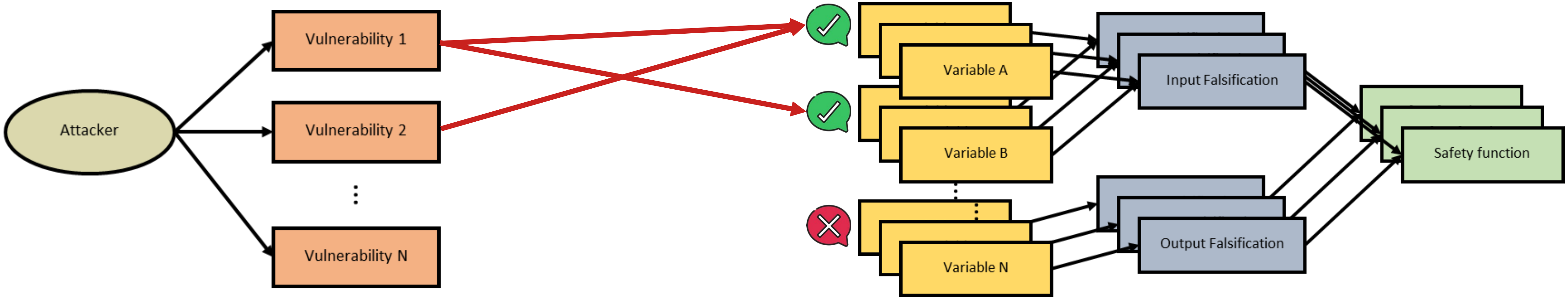


System Vulnerabilities

Theoretical Attack Scenarios

Threat model application

Application

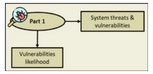


System Vulnerabilities

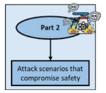
Theoretical Attack Scenarios

Contents

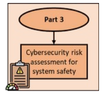
Cybersecurity Risk Assessment for System Safety



What an attacker can do



What an attacker might do



Is it serious ?

Identifying Cybersecurity Risk for System Safety

Literature Review & Classification

PLC-Logic Based Cybersecurity Risk Identification

Conclusion and perspectives

Conclusion & Perspectives

→ **Main Goal: Predict impacts of cyberattacks on safety**

  → *“Is this cyberattack impacting the real world?”*

→ **Attempts to model large industrial control systems**

  → Still facing combinatorial explosion

  → But able to represent realistic-ish systems

→ **A very simplified attacker model based on safety protective commands**

Perspectives:

→ **Take into account other PLC program languages (Ladder, FBD, etc) and discrete/continuous variables:**

  → Will most likely involve SMT solvers and optimization techniques

→ **Consider more powerful attacker models:**

  → Not limited to 1 step...

  → Attack trees, Markov chains, Dolev Yao intruder, etc

Thank you for your attention

Picture by tasukaran from Pixabay - Pictograms designed by Freepik - Domino effect icons created by lutfix – Flaticon -State of the art icons created by Three musketeers - Flaticon

Conclusion & Perspectives

International Peer-Reviewed Conferences with Proceedings

M. Da Silva, M. Puys, P.-H. Thevenon, et S. Mocanu, « **PLC Logic-Based Cybersecurity Risks Identification for ICS** », in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, Benevento Italy: ACM, août 2023, p. 1-10. doi: 10.1145/3600160.3605067.

M. Da Silva, M. Puys, P.-H. Thevenon, S. Mocanu, et N. Nkawa, « **Automated ICS template for STRIDE Microsoft Threat Modeling Tool** », in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, Benevento Italy: ACM, août 2023, p. 1-7. doi: 10.1145/3600160.3605068.

International Peer-Reviewed Journals *(under review)*

M. Da Silva, M. Puys, P.-H. Thevenon, et S. Mocanu, **Safety-Security Convergence: Automation of IEC 62443-3-2,** Computers & Security.

National Events (RESSI)

M. Da Silva, M. Puys, P.-H. Thevenon, et S. Mocanu, **Automatisation de l'analyse des risques de cybersécurité des systèmes industriels**. In *Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, RESSI 2022, Chambon-sur-Lac, France*, 2022.

M. Da Silva, M. Puys, P.-H. Thevenon, et S. Mocanu, **Convergence sûreté-sécurité des Systèmes de Contrôle Industriel**. In *Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, RESSI 2024, Eppe-Sauvage, France*, 2024.

Patent

Mike Da Silva, Pierre-Henri Thevenon, Maxime Puys, Stéphane Mocanu. **Procédé et dispositif d'identification des risques de cyberattaques**. France, N° de brevet: FR3144328. 2024. **Method and device for identifying risks of cyberattacks**. United States, Patent n° : US20240211607A1. 2024.