Lancaster University

A Framework for Measuring, Normalising and Aggregating Security Costs in Cyber-Physical Systems

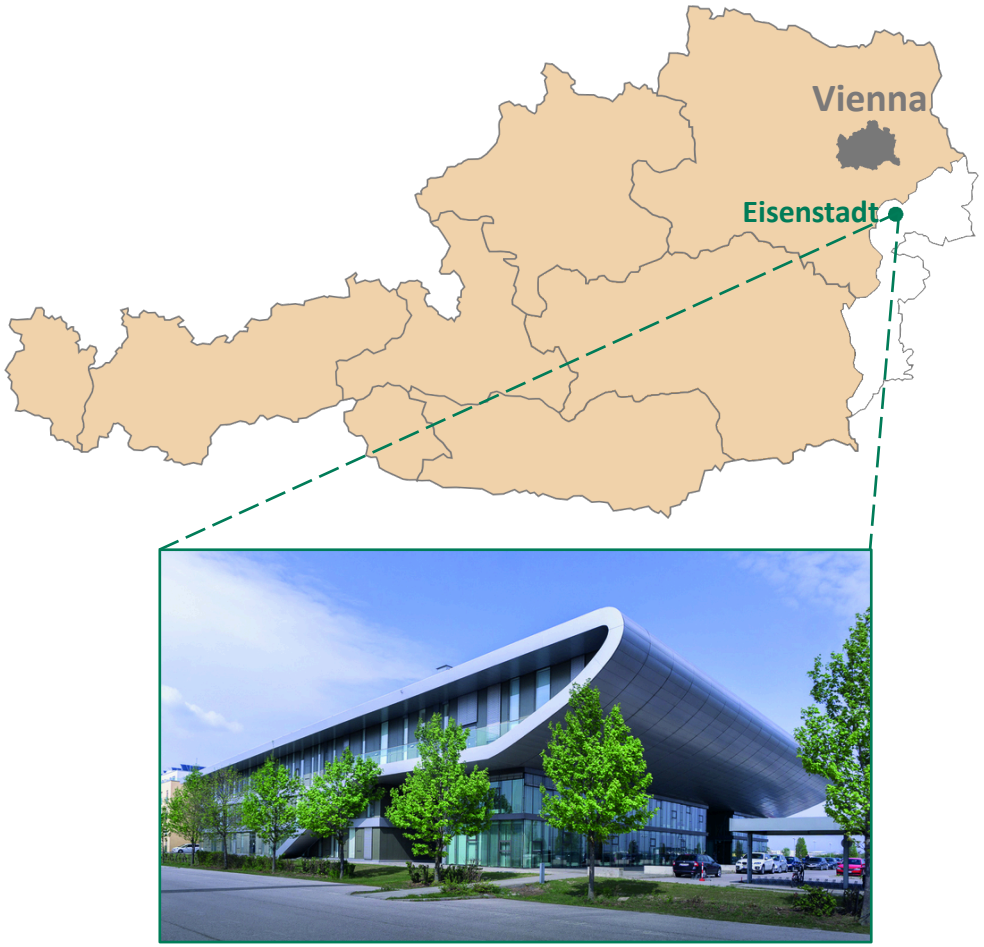
9 July 2020

Igor Ivkić

i.ivkic@lancaster.ac.uk

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

Lancaster University



Research & Teaching

PhD (3rd year)

Modelling Security Costs in Self-Adaptable Cyber-Physical Systems

- Supervisors:
  - Antonios Gouglidis
  - Andreas Mauthe
  - Markus Tauber

Agenda

Lancaster University

- Cyber-Physical Systems
- Onion Layer Model
- Experimental Setup
- Results
- Conclusions

A brief introduction to *Security Costs*

Lancaster University

Our genes are selfish!

Why are we
the way we are?

Broad applicability of the
“Selfish Gene”-theory
among flora and fauna.

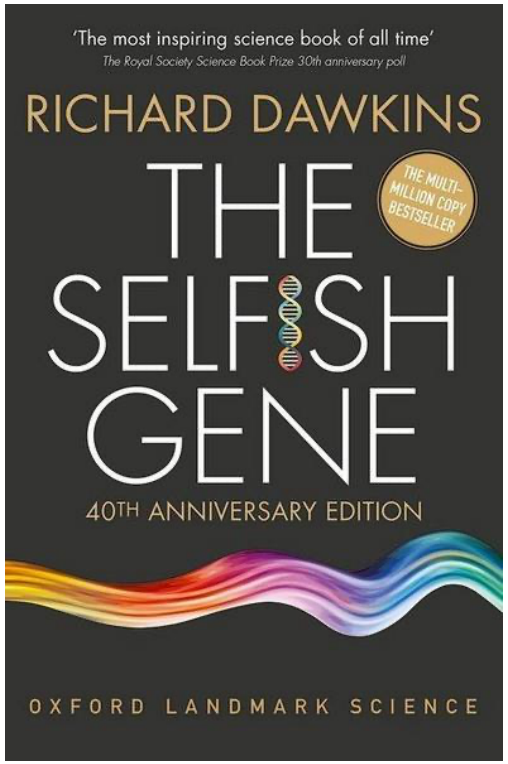


Fig. 1: The Selfish Gene (Dawkins, 1976)

Why do certain animals
have a certain number of
children (offspring)?

↓

Why does a specific
species of birds only lay a
total of 5 eggs max?
Why not more?

A brief introduction to *Security Costs*

Lancaster University

- Robert Trivers
  - Parental Investment and Sexual Selection (1972)
- How much does it ***cost*** to be a parent?
- How much kilocalories (kcal) do parents keep for themselves?
- Result: bird-parents lose weight during “feeding time”!

Fig. 2: Blackbird mother feeding her offspring (RNZ, 2016)

Definition of Cyber-Physical Systems

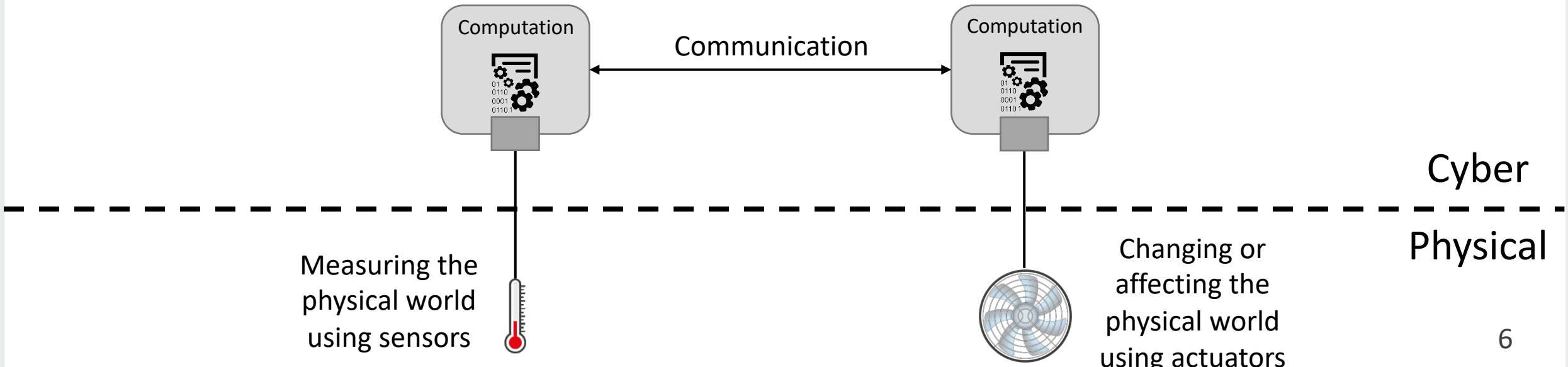


Fig. 3: Closed-Loop Control Logic (adapted from Rajkumar et al., 2016)

Security Costs and Cyber-Physical Systems

Lancaster University

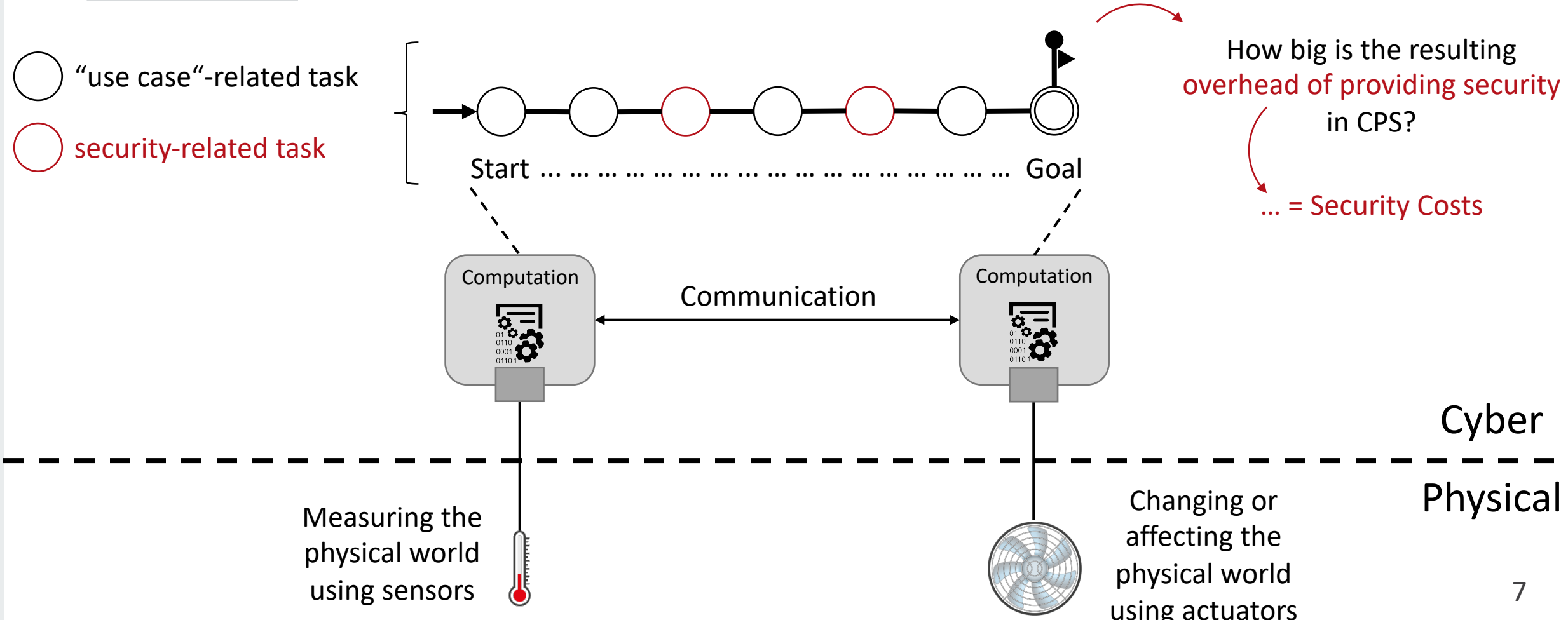
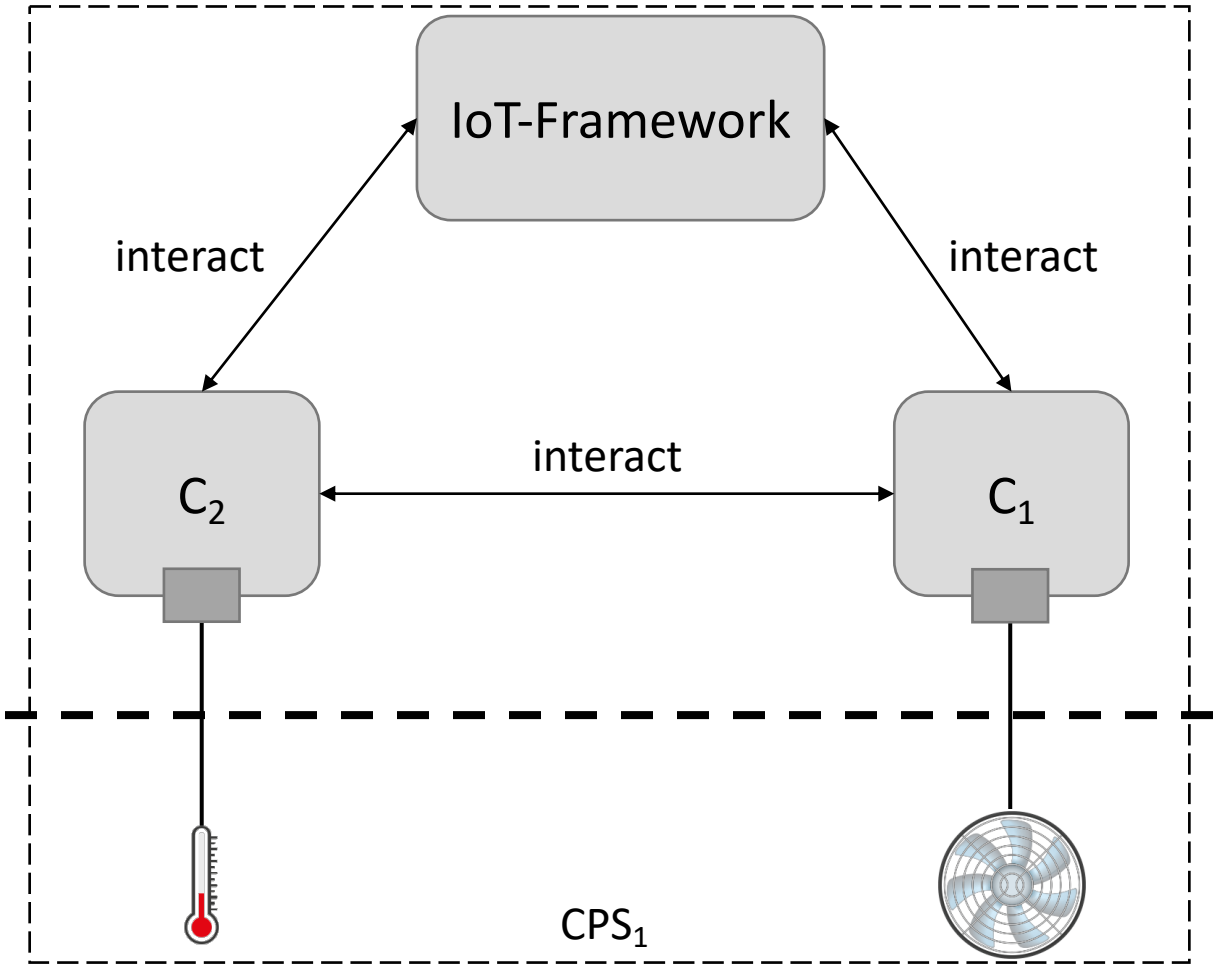


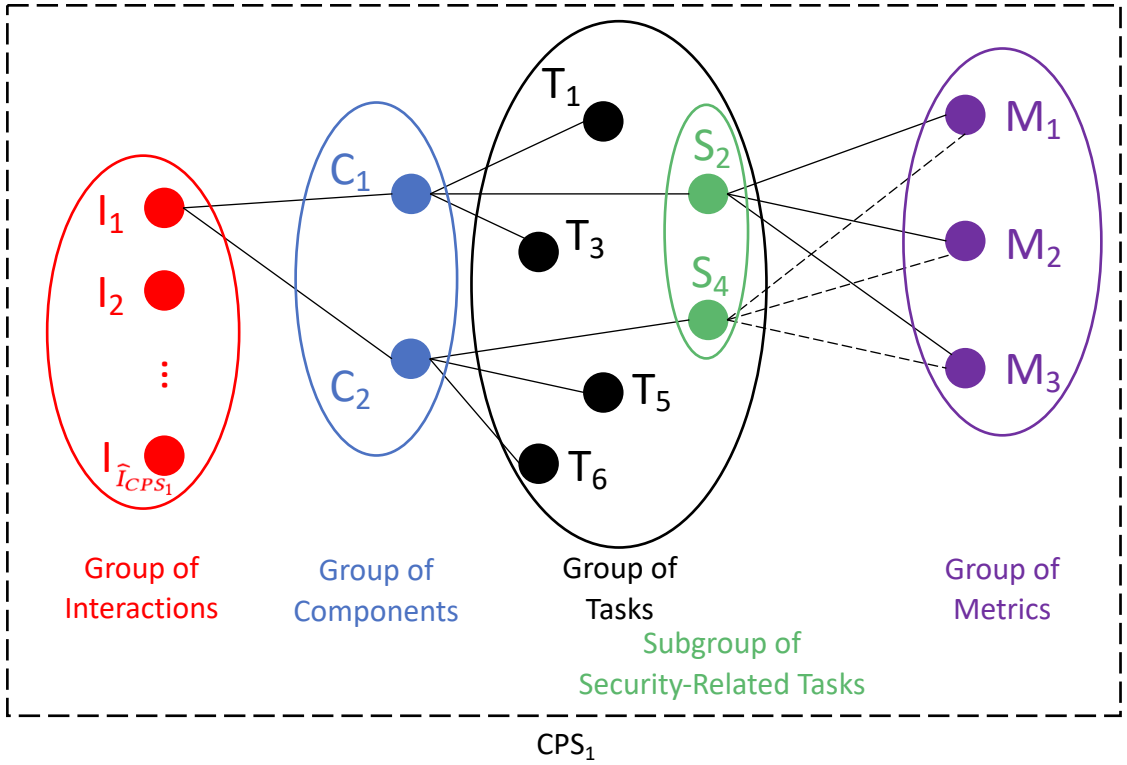
Fig. 3: Closed-Loop Control Logic (adapted from Rajkumar et al., 2016)

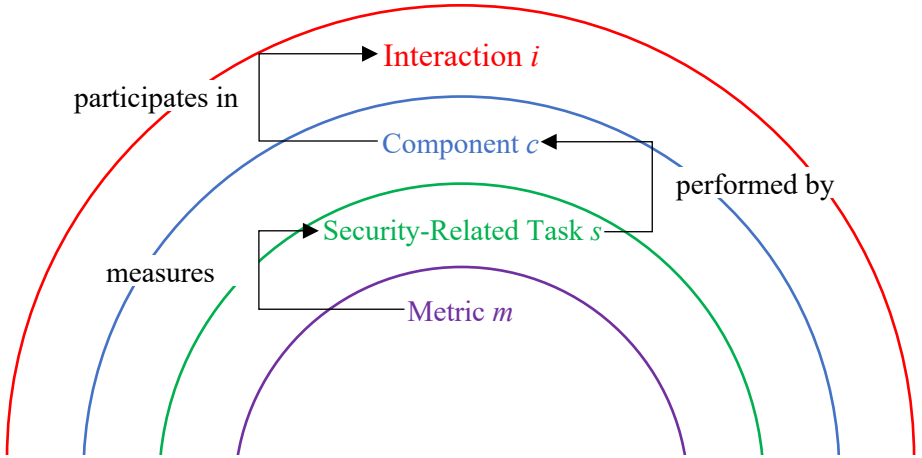
CPS & IoT & Frameworks



Modelling Security Costs in CPS

Lancaster University



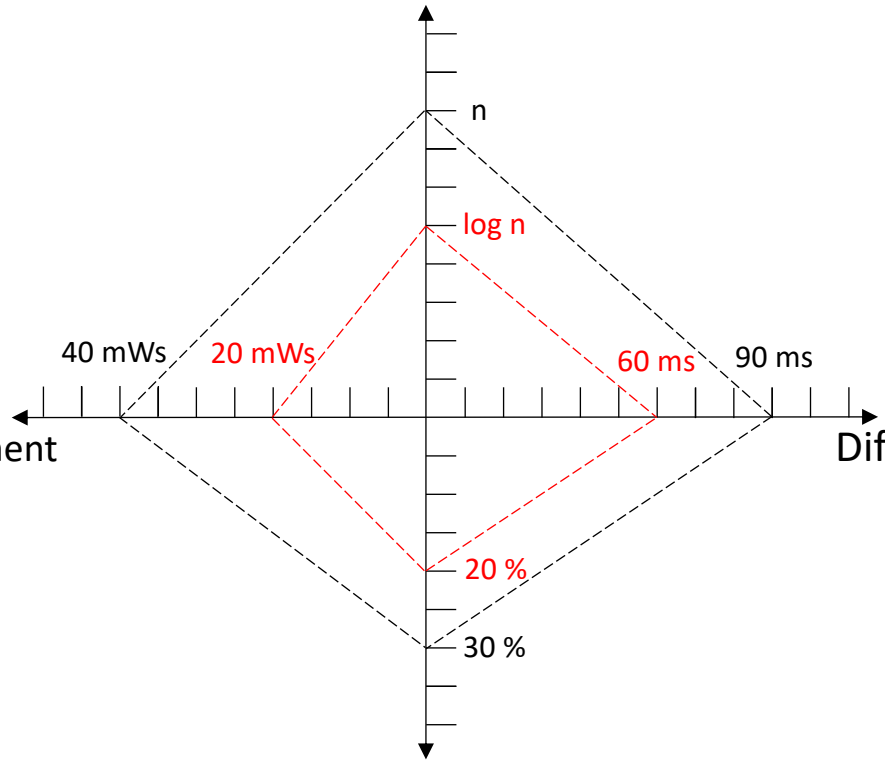


$$SecurityCosts_{CPS_1} = \sum_{i=1}^{\widehat{I}_{CPS_1}} \sum_{c=1}^{\widehat{C}_i} \sum_{s=1}^{\widehat{S}_c} \sum_{m=1}^{\widehat{M}_s}$$

Metric Types

Metric Type$_0$
Algorithmic Complexity Analysis

Big-O notation (algorithmic time complexity)



Power consumption in milliWattseconds

Metric Type$_3$
Overall Result Measurement

Metric Type$_1$
Difference Measurement

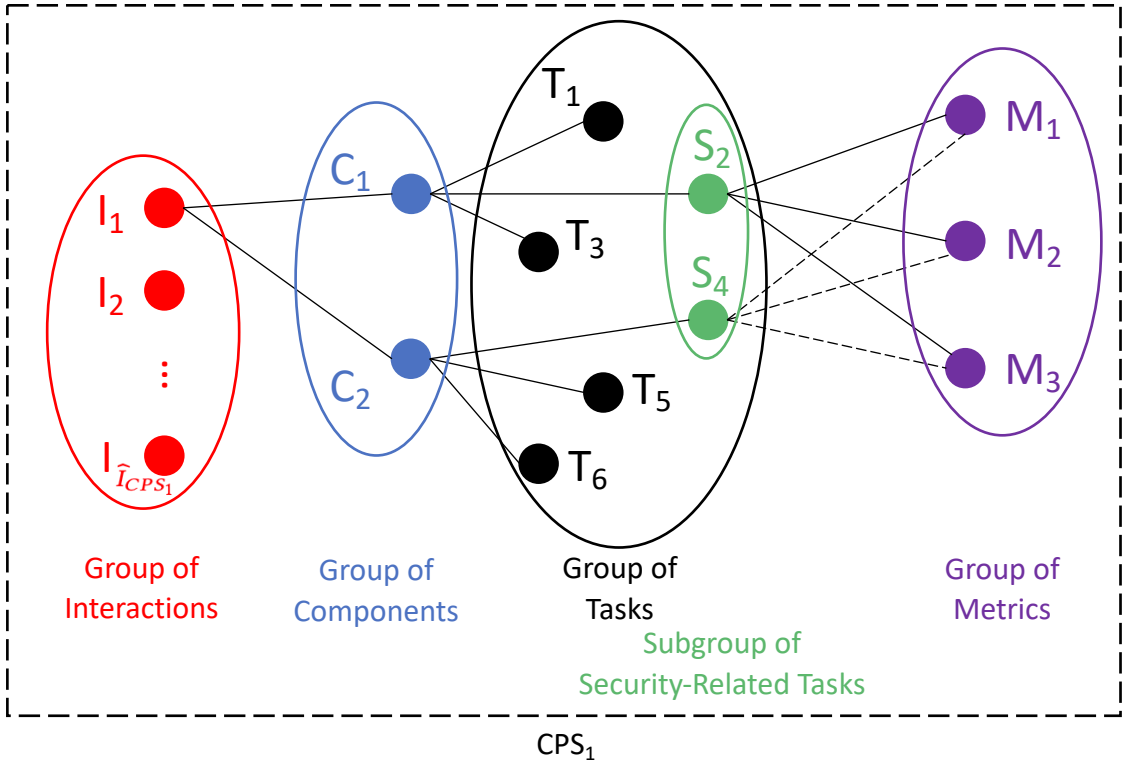
Execution time in milliseconds

Metric Type$_2$
Sample Measurement

CPU-usage in percent

Modelling Security Costs in CPS

Lancaster University



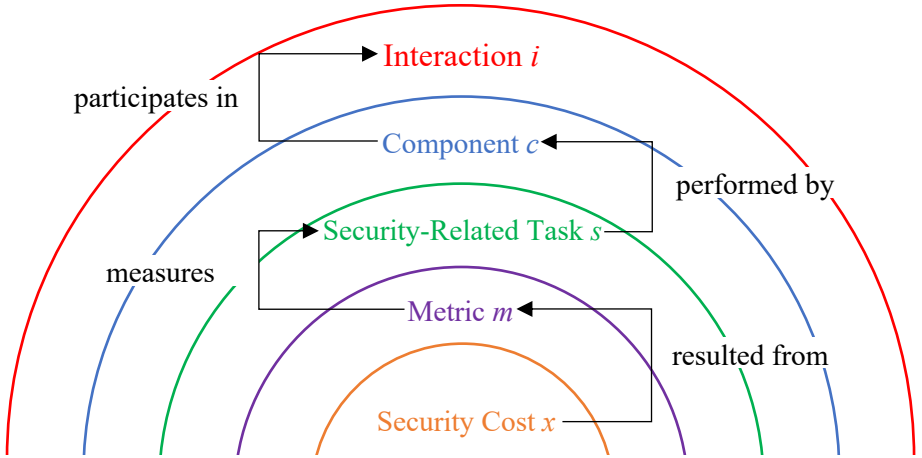


Fig. 4: Onion Layer Model (Ivkic et al., 2019)

$$SecurityCosts_{CPS_1} = \sum_{i=1}^{\hat{I}_{CPS_1}} \sum_{c=1}^{\hat{C}_i} \sum_{s=1}^{\hat{S}_c} \sum_{m=1}^{\hat{M}_s} \dot{x}_{icsm} * w_{MT_j}$$

Normalisation and Weight-Calculation

Raw measurement data

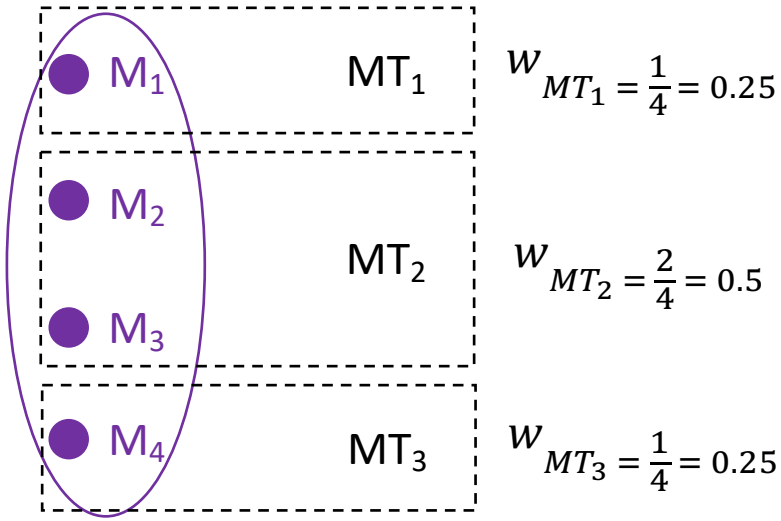
Tasks	Metrics			
	M1	M2	M3	M4
T1	10 ms	5 %	20 MB	3 Ws
T2	12 ms	10 %	30 MB	9 WS

MIN-MAX Normalisation

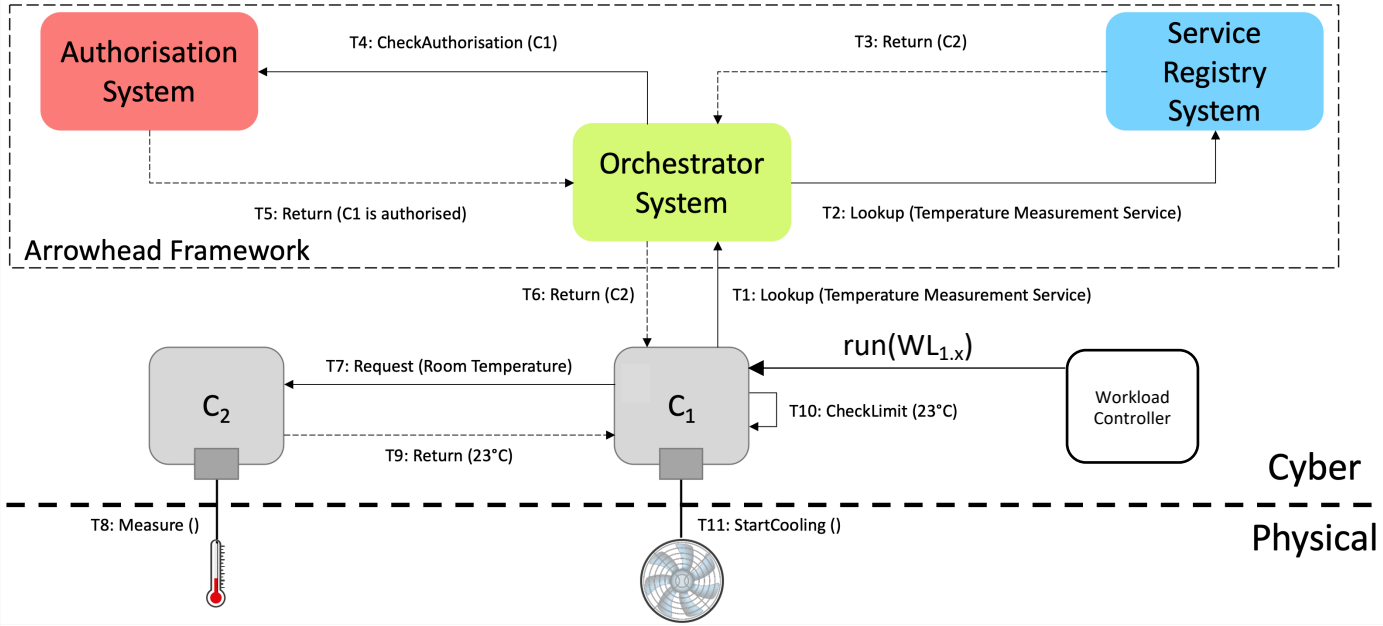
$$\dot{x} = a + \frac{(x - MIN_{MT_j}) * (b - a)}{MAX_{MT_j} - MIN_{MT_j}}$$

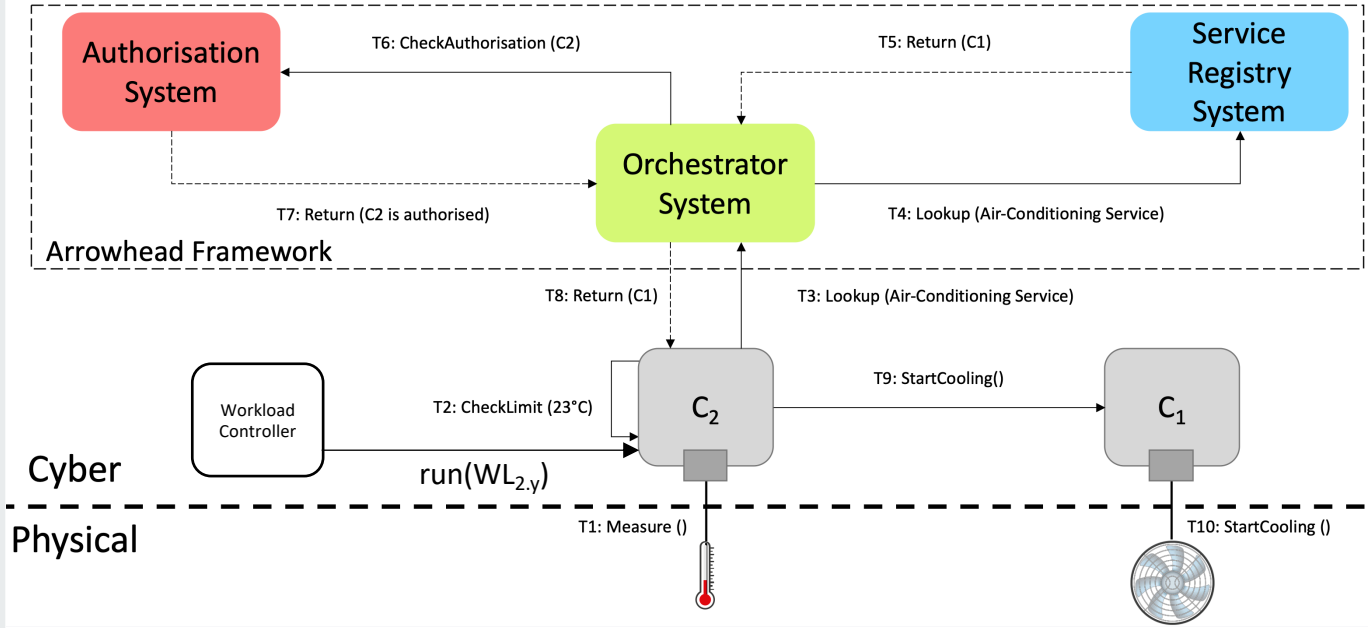
Normalised data

Tasks	Metrics			
	M1	M2	M3	M4
T1	0,1	0,05	0,4	0,3
T2	0,12	0,1	0,6	0,9



Total number of metrics used = 4





Use Case 1

vs.

Use Case 2

Table 1: Workloads used by the Workload Controller for the Experimental Study

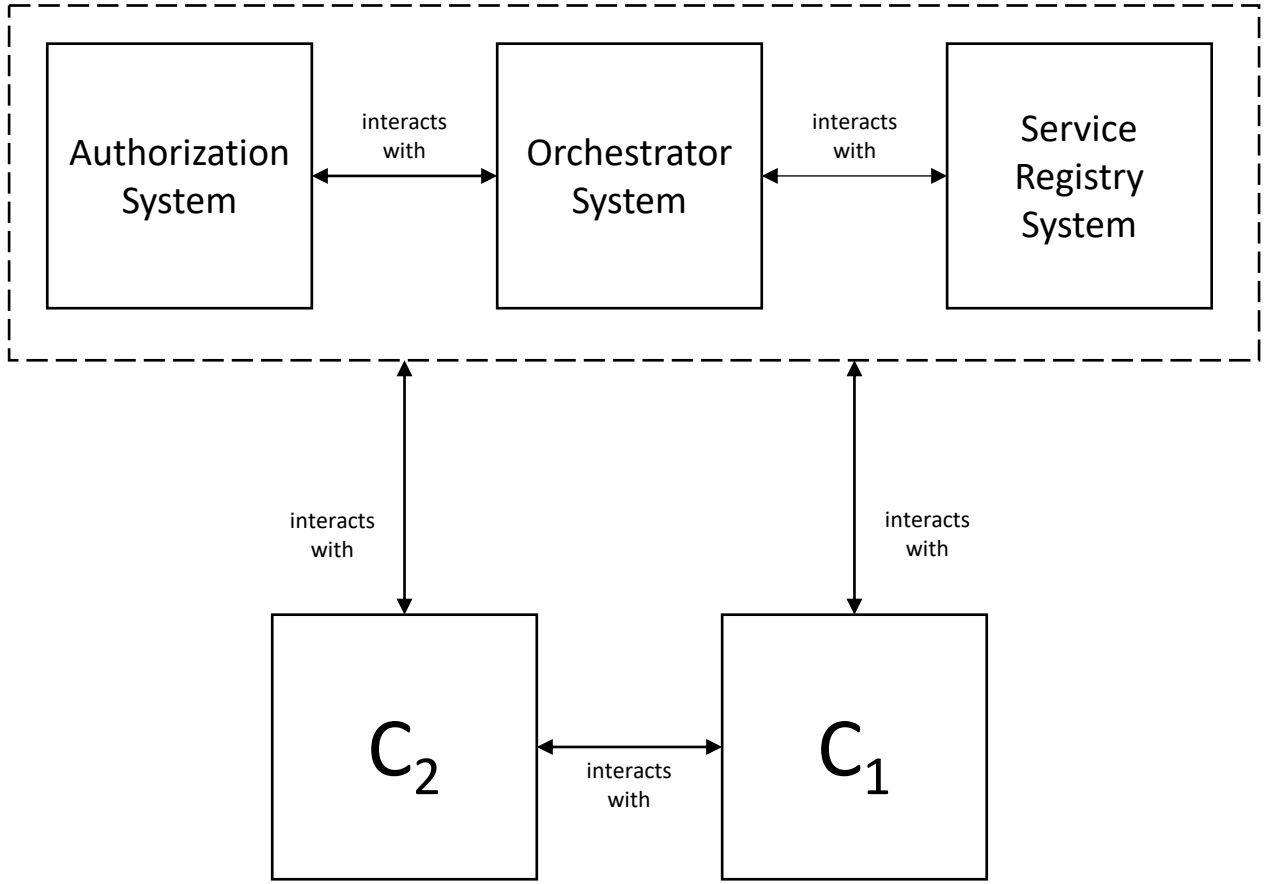
WL	Use Case	Runs	Temperature	Protocol
$WL_{1.1}$	Use Case 1	25 25	Measurement <25°C Measurement >25°C	HTTPS
$WL_{1.2}$	Use Case 1	25 25	Measurement <25°C Measurement >25°C	HTTP
$WL_{2.1}$	Use Case 2	25 25	Measurement <25°C Measurement >25°C	HTTPS
$WL_{2.2}$	Use Case 2	25 25	Measurement <25°C Measurement >25°C	HTTP

Table 2: Measurement Metrics used for Measuring Security Costs for each Workload

Metric Type	Metric	Unit
MT_0	Algorithmic Time Complexity (Big-O)	-
MT_1	Duration of executing a specific task	Milliseconds (ms)
MT_2	CPU-usage	Percent (%)
MT_3	Power consumption	Milliwattseconds (mWs)

"Testbed"

Lancaster University

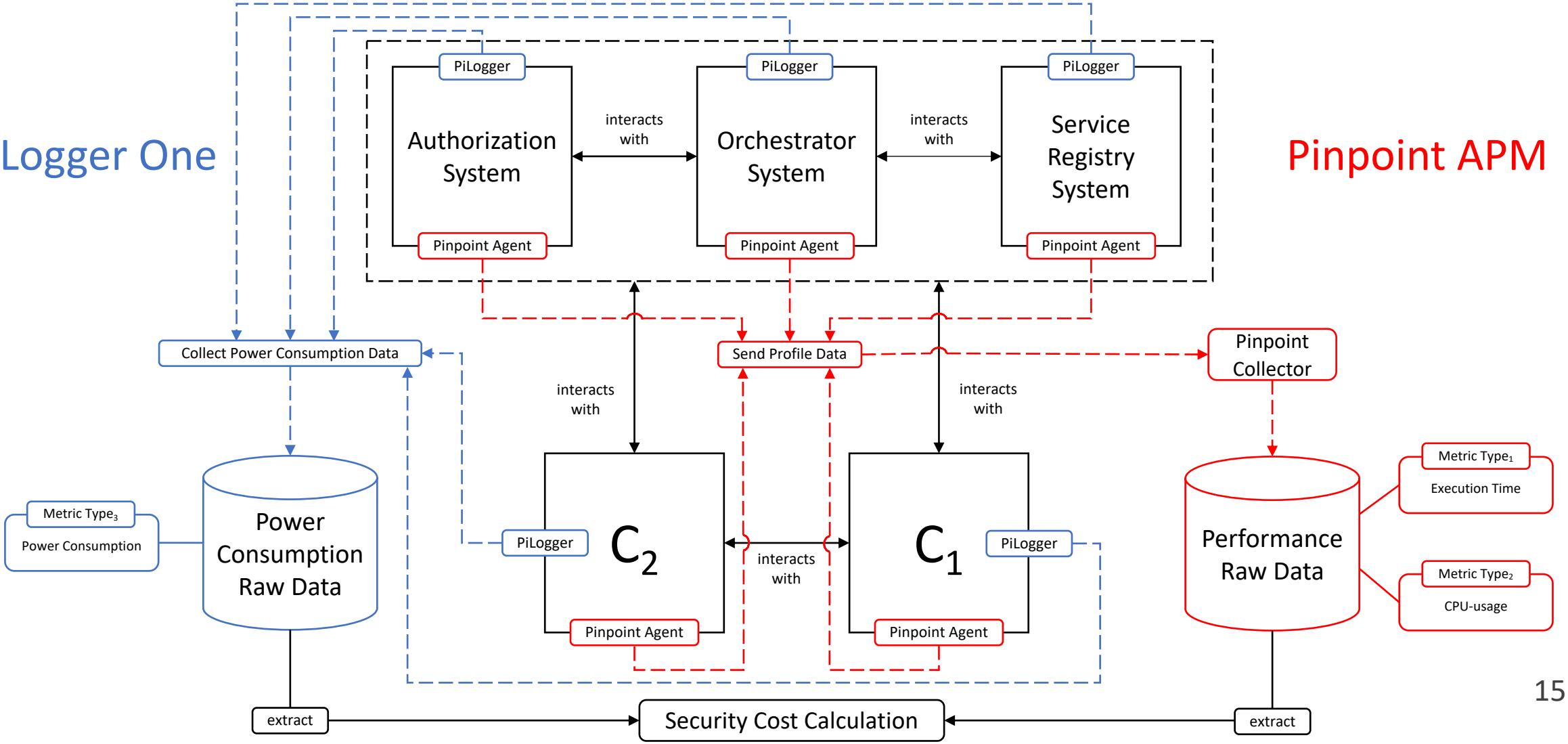


Measurement Tools and Metrics

Lancaster University

PiLogger One

Pinpoint APM



PiLogger One & Pinpoint APM

Lancaster University

PiLogger One

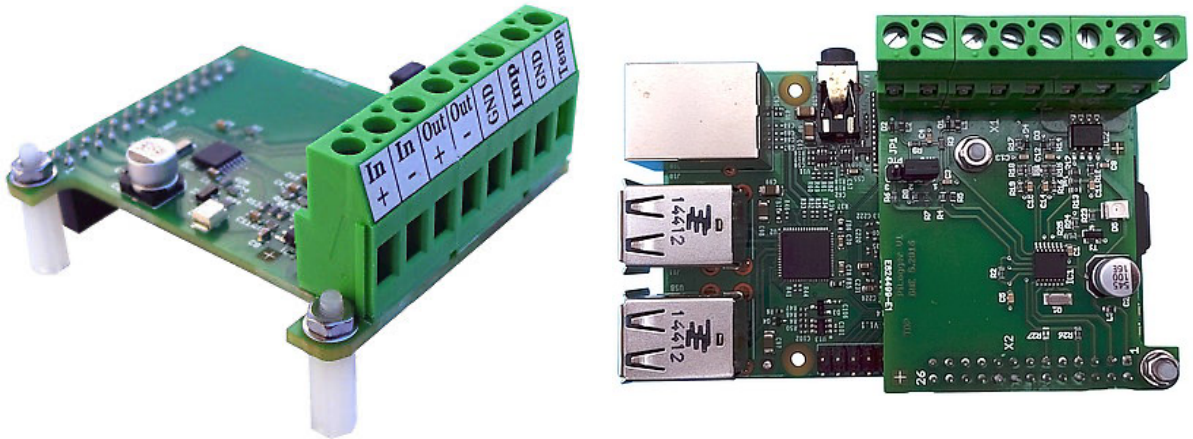


Fig. 5: Raspberry Pi add-on board for measuring power consumption (PiLogger, 2020)

Pinpoint APM

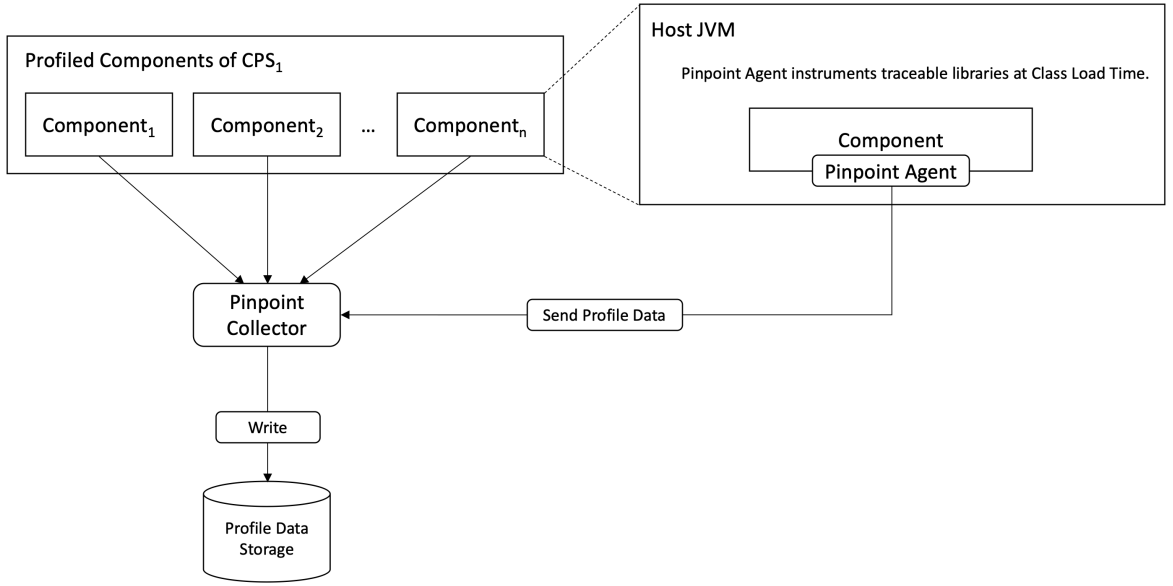


Fig. 6: Pinpoint Application Performance Management Architecture (Naver, 2020)

Security Cost Modelling Framework (SCMF)

Lancaster University

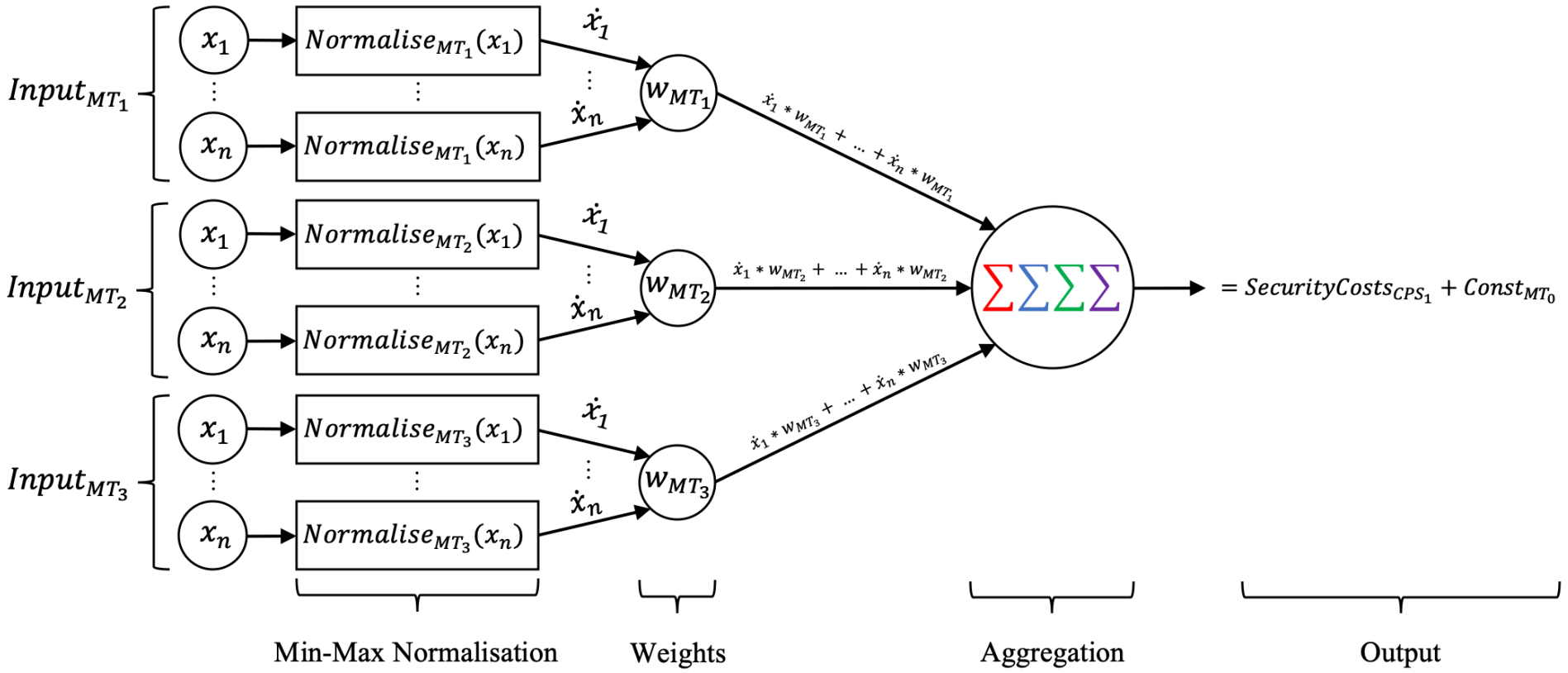


Fig. 7: A Holistic Approach for Normalising, Weighing and Aggregating Security Costs

Discussion

Table 3: Total Costs per Workload

		Total Costs						
WL	Measurement	Min	Max	Median	Mean	Std.Dev.	Std.Err.	∑
$WL_{1.1}$	$< 25°C$	0.00083	0.36000	0.01800	0.04377	0.05060	0.00221	53.92297
	$> 25°C$	0.00100	0.28755	0.02200	0.05894	0.07366	0.00321	
$WL_{1.2}$	$< 25°C$	0.00070	0.34000	0.02100	0.04876	0.05830	0.00254	53.51435
	$> 25°C$	0.00089	0.39874	0.02000	0.05317	0.06804	0.00297	
$WL_{2.1}$	$< 25°C$	0	0.08281	0	0.00472	0.01431	0.00062	36.15943
	$> 25°C$	0.00100	0.44075	0.02642	0.06415	0.08218	0.00359	
$WL_{2.2}$	$< 25°C$	0	0.10100	0	0.00480	0.01471	0.00064	31.57160
	$> 25°C$	0.00100	0.37200	0.02066	0.05534	0.07307	0.00319	

Table 4: Security Costs per Workload

		Security Costs						
WL	Measurement	Min	Max	Median	Mean	Std.Dev.	Std.Err.	∑
$WL_{1.1}$	$< 25°C$	0.00267	0.13728	0.01500	0.04714	0.05065	0.00414	17.61541
	$> 25°C$	0.00267	0.27930	0.02231	0.07030	0.08565	0.00699	
$WL_{1.2}$	$< 25°C$	0.00244	0.16359	0.01400	0.04861	0.05337	0.00436	16.08108
	$> 25°C$	0.00178	0.23166	0.01500	0.05859	0.07342	0.00599	
$WL_{2.1}$	$< 25°C$	0	0	0	0	0	0	10.97640
	$> 25°C$	0.00267	0.29200	0.02486	0.07318	0.08504	0.00694	
$WL_{2.2}$	$< 25°C$	0	0	0	0	0	0	10.02343
	$> 25°C$	0.00200	0.31474	0.02239	0.06682	0.08074	0.00659	

Use Case 1: $SecurityCosts_{CPS_1} = (53.92297 - 53.51435) + 17.61541 = 18.02403 + f_{MT_0}(n)$

Use Case 2: $SecurityCosts_{CPS_1} = (36.15943 - 31.57160) + 10.97640 = 15.56423 + f_{MT_0}(n)$

→ Algorithmic Complexity Constants

Discussion

Lancaster University

≈ 30% of all tasks performed are security-related

Table 3: Total Costs per Workload

		Total Costs						
WL	Measurement	Min	Max	Median	Mean	Std.Dev.	Std.Err.	∑
$WL_{1.1}$	$< 25°C$	0.00083	0.36000	0.01800	0.04377	0.05060	0.00221	53.92297
	$> 25°C$	0.00100	0.28755	0.02200	0.05894	0.07366	0.00321	
$WL_{1.2}$	$< 25°C$	0.00070	0.34000	0.02100	0.04876	0.05830	0.00254	53.51435
	$> 25°C$	0.00089	0.39874	0.02000	0.05317	0.06804	0.00297	
$WL_{2.1}$	$< 25°C$	0	0.08281	0	0.00472	0.01431	0.00062	36.15943
	$> 25°C$	0.00100	0.44075	0.02642	0.06415	0.08218	0.00359	
$WL_{2.2}$	$< 25°C$	0	0.10100	0	0.00480	0.01471	0.00064	31.57160
	$> 25°C$	0.00100	0.37200	0.02066	0.05534	0.07307	0.00319	

Table 4: Security Costs per Workload

		Security Costs						
WL	Measurement	Min	Max	Median	Mean	Std.Dev.	Std.Err.	∑
$WL_{1.1}$	$< 25°C$	0.00267	0.13728	0.01500	0.04714	0.05065	0.00414	17.61541
	$> 25°C$	0.00267	0.27930	0.02231	0.07030	0.08565	0.00699	
$WL_{1.2}$	$< 25°C$	0.00244	0.16359	0.01400	0.04861	0.05337	0.00436	16.08108
	$> 25°C$	0.00178	0.23166	0.01500	0.05859	0.07342	0.00599	
$WL_{2.1}$	$< 25°C$	0	0	0	0	0	0	10.97640
	$> 25°C$	0.00267	0.29200	0.02486	0.07318	0.08504	0.00694	
$WL_{2.2}$	$< 25°C$	0	0	0	0	0	0	10.02343
	$> 25°C$	0.00200	0.31474	0.02239	0.06682	0.08074	0.00659	

Use Case 1: $SecurityCosts_{CPS_1} = (53.92297 - 53.51435) + 17.61541 = 18.02403 + f_{MT_0}(n)$

Use Case 2: $SecurityCosts_{CPS_1} = (36.15943 - 31.57160) + 10.97640 = 15.56423 + f_{MT_0}(n)$

→ Algorithmic Complexity Constants

Discussion

The cost of "S" in HTTPS

Table 3: Total Costs per Workload

WL	Measurement	Total Costs Min	Max	Median	Mean	Std.Dev.	Std.Err.	∑
$WL_{1.1}$	$< 25°C$	0.00083	0.36000	0.01800	0.04377	0.05060	0.00221	53.92297
	$> 25°C$	0.00100	0.28755	0.02200	0.05894	0.07366	0.00321	
$WL_{1.2}$	$< 25°C$	0.00070	0.34000	0.02100	0.04876	0.05830	0.00254	53.51435
	$> 25°C$	0.00089	0.39874	0.02000	0.05317	0.06804	0.00297	
$WL_{2.1}$	$< 25°C$	0	0.08281	0	0.00472	0.01431	0.00062	36.15943
	$> 25°C$	0.00100	0.44075	0.02642	0.06415	0.08218	0.00359	
$WL_{2.2}$	$< 25°C$	0	0.10100	0	0.00480	0.01471	0.00064	31.57160
	$> 25°C$	0.00100	0.37200	0.02066	0.05534	0.07307	0.00319	

Table 4: Security Costs per Workload

WL	Measurement	Security Costs Min	Max	Median	Mean	Std.Dev.	Std.Err.	∑
$WL_{1.1}$	$< 25°C$	0.00267	0.13728	0.01500	0.04714	0.05065	0.00414	17.61541
	$> 25°C$	0.00267	0.27930	0.02231	0.07030	0.08565	0.00699	
$WL_{1.2}$	$< 25°C$	0.00244	0.16359	0.01400	0.04861	0.05337	0.00436	16.08108
	$> 25°C$	0.00178	0.23166	0.01500	0.05859	0.07342	0.00599	
$WL_{2.1}$	$< 25°C$	0	0	0	0	0	0	10.97640
	$> 25°C$	0.00267	0.29200	0.02486	0.07318	0.08504	0.00694	
$WL_{2.2}$	$< 25°C$	0	0	0	0	0	0	10.02343
	$> 25°C$	0.00200	0.31474	0.02239	0.06682	0.08074	0.00659	

Use Case 1: $SecurityCosts_{CPS_1} = (53.92297 - 53.51435) + 17.61541 = 18.02403 + f_{MT_0}(n)$

Use Case 2: $SecurityCosts_{CPS_1} = (36.15943 - 31.57160) + 10.97640 = 15.56423 + f_{MT_0}(n)$

→ Algorithmic Complexity Constants

Discussion

Lancaster University

In general: Use Case 2 performs better than Use Case 1

Table 3: Total Costs per Workload

		Total Costs						
WL	Measurement	Min	Max	Median	Mean	Std.Dev.	Std.Err.	∑
$WL_{1.1}$	$< 25°C$	0.00083	0.36000	0.01800	0.04377	0.05060	0.00221	53.92297
	$> 25°C$	0.00100	0.28755	0.02200	0.05894	0.07366	0.00321	
$WL_{1.2}$	$< 25°C$	0.00070	0.34000	0.02100	0.04876	0.05830	0.00254	53.51435
	$> 25°C$	0.00089	0.39874	0.02000	0.05317	0.06804	0.00297	
$WL_{2.1}$	$< 25°C$	0	0.08281	0	0.00472	0.01431	0.00062	36.15943
	$> 25°C$	0.00100	0.44075	0.02642	0.06415	0.08218	0.00359	
$WL_{2.2}$	$< 25°C$	0	0.10100	0	0.00480	0.01471	0.00064	31.57160
	$> 25°C$	0.00100	0.37200	0.02066	0.05534	0.07307	0.00319	

Table 4: Security Costs per Workload

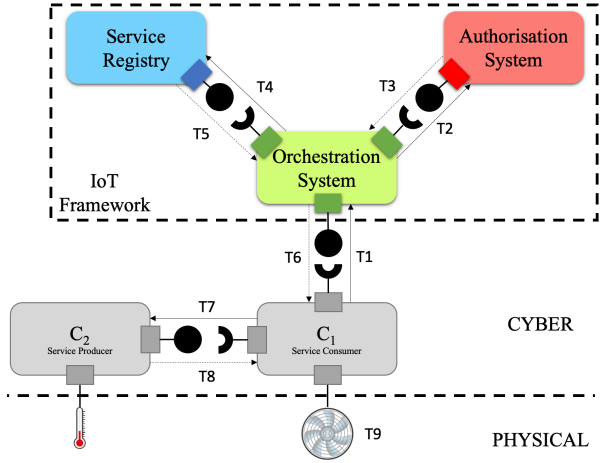
		Security Costs						
WL	Measurement	Min	Max	Median	Mean	Std.Dev.	Std.Err.	∑
$WL_{1.1}$	$< 25°C$	0.00267	0.13728	0.01500	0.04714	0.05065	0.00414	17.61541
	$> 25°C$	0.00267	0.27930	0.02231	0.07030	0.08565	0.00699	
$WL_{1.2}$	$< 25°C$	0.00244	0.16359	0.01400	0.04861	0.05337	0.00436	16.08108
	$> 25°C$	0.00178	0.23166	0.01500	0.05859	0.07342	0.00599	
$WL_{2.1}$	$< 25°C$	0	0	0	0	0	0	10.97640
	$> 25°C$	0.00267	0.29200	0.02486	0.07318	0.08504	0.00694	
$WL_{2.2}$	$< 25°C$	0	0	0	0	0	0	10.02343
	$> 25°C$	0.00200	0.31474	0.02239	0.06682	0.08074	0.00659	

Use Case 1: $SecurityCosts_{CPS_1} = (53.92297 - 53.51435) + 17.61541 = 18.02403 + f_{MT_0}(n)$

Use Case 2: $SecurityCosts_{CPS_1} = (36.15943 - 31.57160) + 10.97640 = 15.56423 + f_{MT_0}(n)$

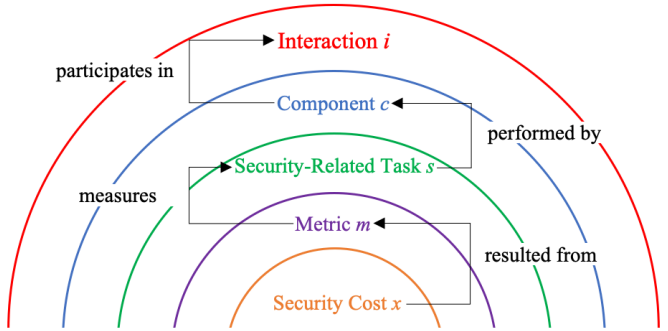
→ Algorithmic Complexity Constants

Summary & Future Work



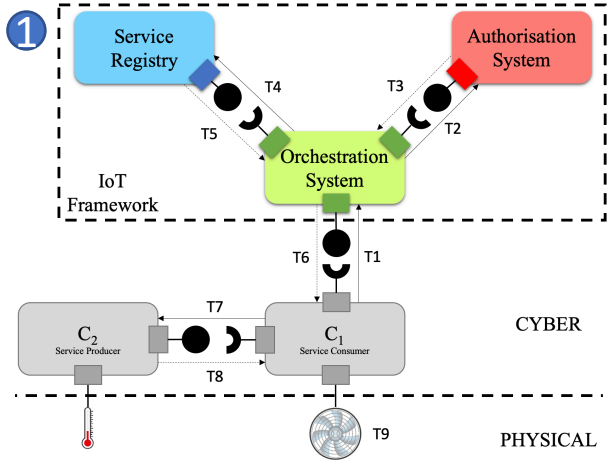
Output 1

normalisation, weighting & aggregation



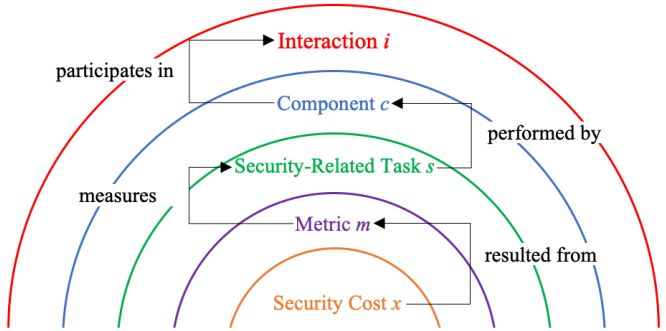
$$SecurityCosts_{CPS_1} = \sum_{i=1}^{\hat{I}_{CPS_1}} \sum_{c=1}^{\hat{C}_i} \sum_{s=1}^{\hat{S}_c} \sum_{m=1}^{\hat{M}_s} \dot{x}_{icsm} * w_{MT_j}$$

Summary & Future Work



Output 1

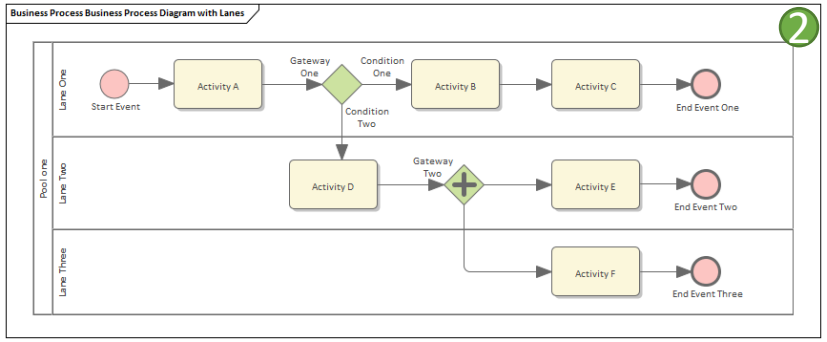
normalisation, weighting & aggregation



$$SecurityCosts_{CPS_1} = \sum_{i=1}^{\hat{I}_{CPS_1}} \sum_{c=1}^{\hat{C}_i} \sum_{s=1}^{\hat{S}_c} \sum_{m=1}^{\hat{M}_s} \dot{x}_{icsm} * w_{MT_j}$$

Interaction Visualisation

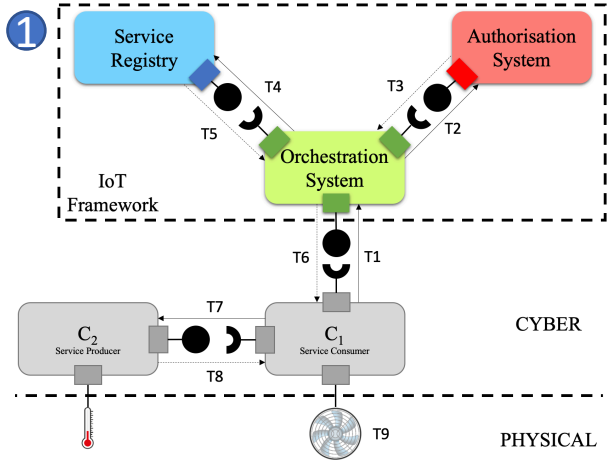
Output 2



incl. comparing the planned and the actual workflow of the CPS
"CPS-as-it-should-be" vs. "CPS-as-it-is"

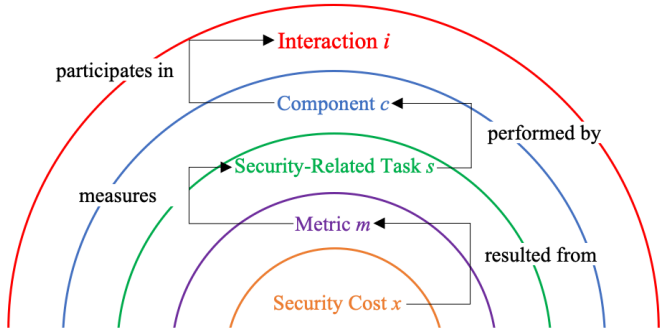
1 2

Summary & Future Work



Output 1

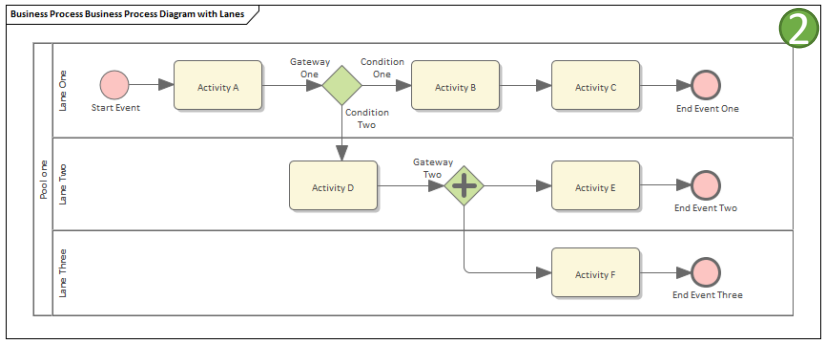
normalisation, weighting & aggregation



$$SecurityCosts_{CPS_1} = \sum_{i=1}^{\hat{I}_{CPS_1}} \sum_{c=1}^{\hat{C}_i} \sum_{s=1}^{\hat{S}_c} \sum_{m=1}^{\hat{M}_s} \dot{x}_{icsm} * w_{MT_j}$$

Interaction Visualisation

Output 2



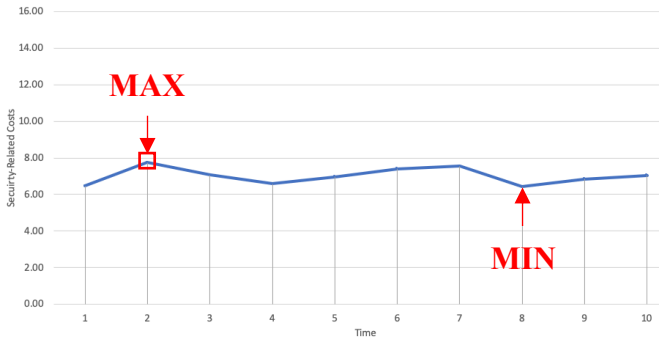
incl. comparing the planned and the actual workflow of the CPS
"CPS-as-it-should-be" vs. "CPS-as-it-is"

1 2

Monitoring the Security Costs over time

Output 3

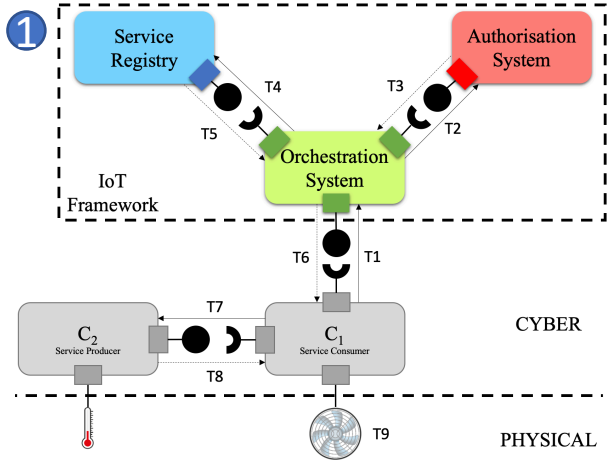
direct relation



know the "nature" of security costs of a CPS
in case security costs rise above MAX or drop below MIN:
-) identify affected/responsible components

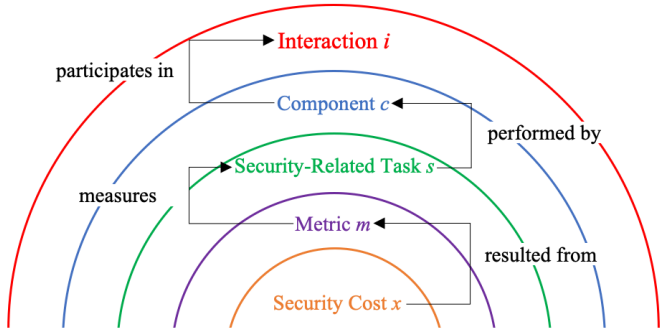
Summary & Future Work

Lancaster University



Output 1

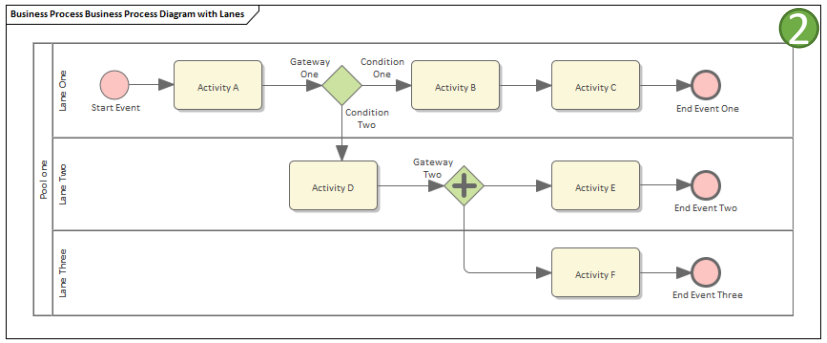
normalisation, weighting & aggregation



$$SecurityCosts_{CPS_1} = \sum_{i=1}^{\hat{I}_{CPS_1}} \sum_{c=1}^{\hat{C}_i} \sum_{s=1}^{\hat{S}_c} \sum_{m=1}^{\hat{M}_s} \dot{x}_{icsm} * w_{MT_j}$$

Interaction Visualisation

Output 2



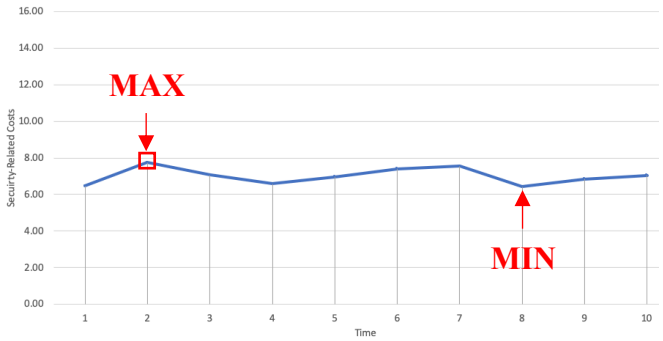
incl. comparing the planned and the actual workflow of the CPS
"CPS-as-it-should-be" vs. "CPS-as-it-is"

1 2

direct relation

Monitoring the Security Costs over time

Output 3

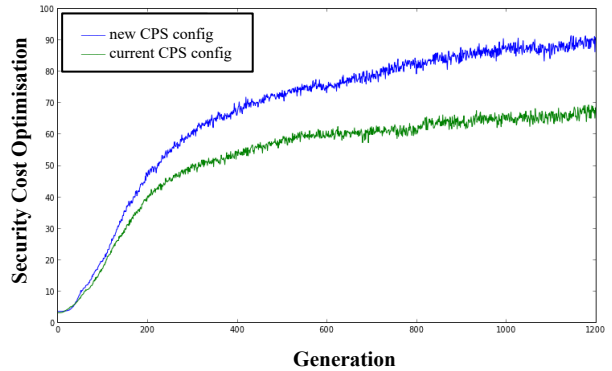


know the "nature" of security costs of a CPS
in case security costs rise above MAX or drop below MIN:
-) identify affected/responsible components

direct relation

Output 4

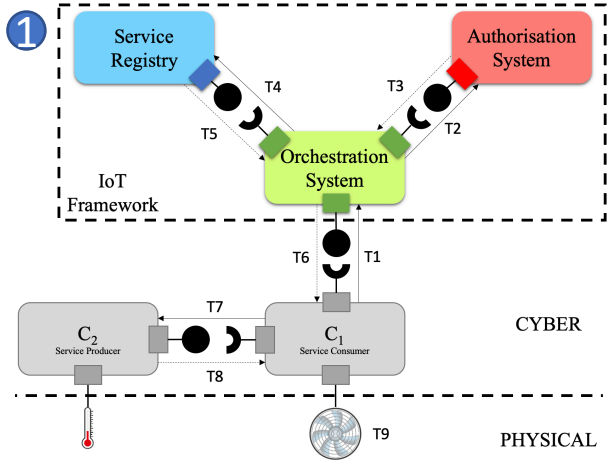
Simulation & Optimisation



usage of genetic and selective algorithms to simulate possible interaction configurations (e.g. protocols) and measure their resulting security costs

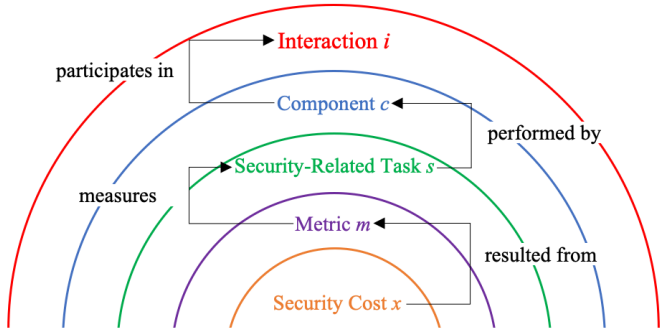
Summary & Future Work

Lancaster University



Output 1

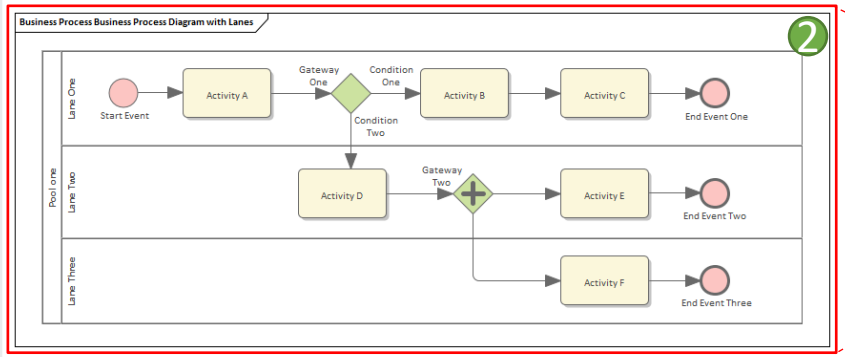
normalisation, weighting & aggregation



$$SecurityCosts_{CPS_1} = \sum_{i=1}^{\hat{I}_{CPS_1}} \sum_{c=1}^{\hat{C}_i} \sum_{s=1}^{\hat{S}_c} \sum_{m=1}^{\hat{M}_s} \dot{x}_{icsm} * w_{MT_j}$$

Interaction Visualisation

Output 2



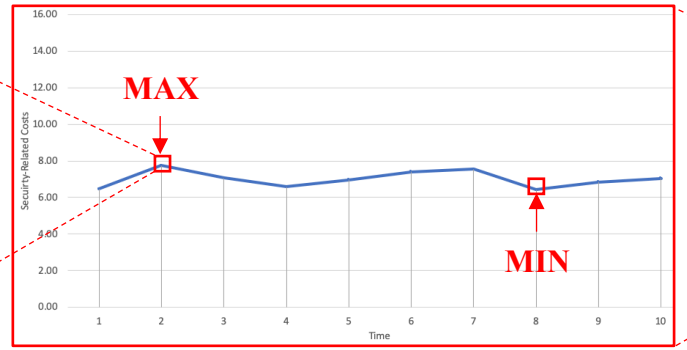
incl. comparing the planned and the actual workflow of the CPS
"CPS-as-it-should-be" vs. "CPS-as-it-is"

1 2

direct relation

Monitoring the Security Costs over time

Output 3

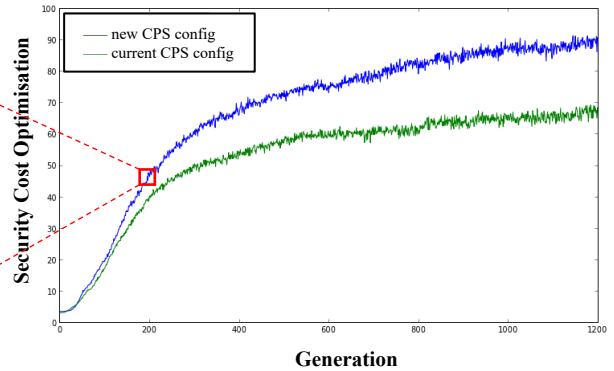


know the "nature" of security costs of a CPS
in case security costs rise above MAX or drop below MIN:
-) identify affected/responsible components

direct relation

Output 4

Simulation & Optimisation



usage of genetic and selective algorithms to simulate possible interaction configurations (e.g. protocols) and measure their resulting security costs

Lancaster University

Thank you for your attention

ORCID iD
https://orcid.org/0000-0003-3037-7813

Google Scholar
https://scholar.google.at/citations?user=eWmRzy0AAAAJ&hl=de&oi=ao

arXiv
https://arxiv.org/search/cs?searchtype=author&query=Ivkic%2C+I