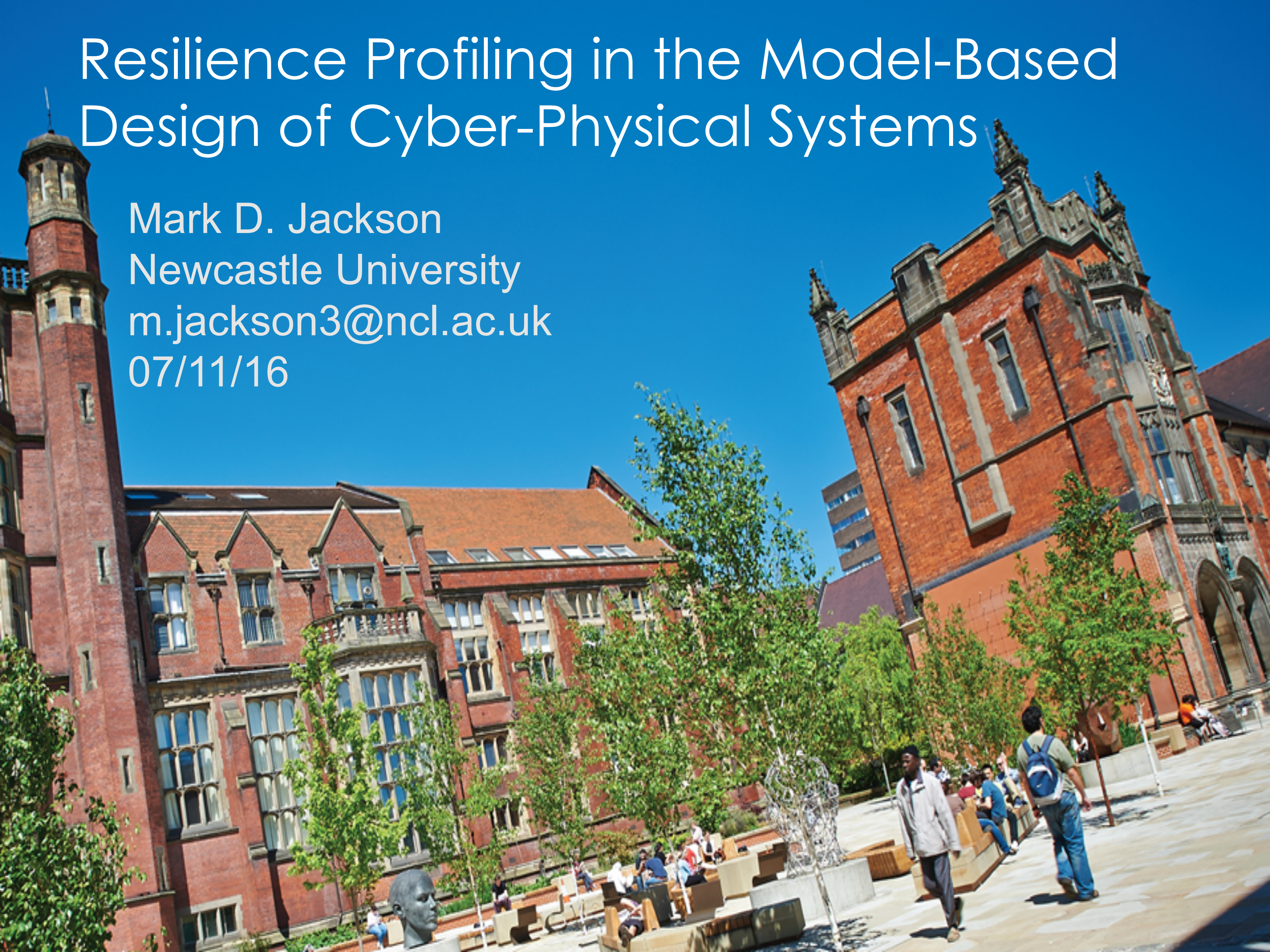
Resilience Profiling in the Model-Based Design of Cyber-Physical Systems

Mark D. Jackson
Newcastle University
m.jackson3@ncl.ac.uk

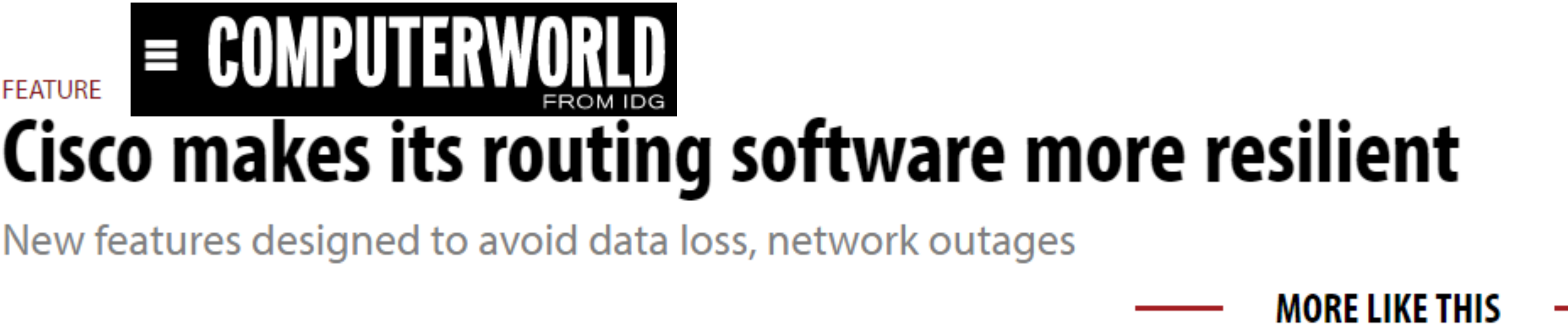
07/11/16



Contents

- Resilience – as a concept, and in Cyber-Physical Systems (CPSs)
- Resilience Analysis
- Integrating Resilience Analysis
- Evaluating Resilience
- Summary

1



FEATURE

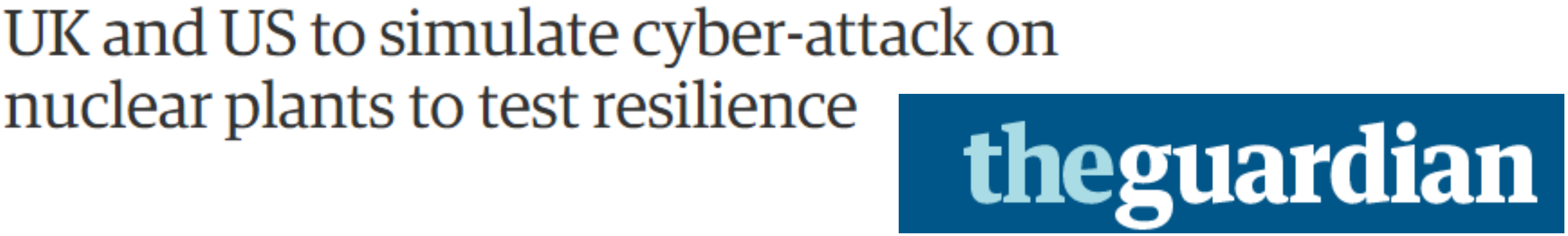
COMPUTERWORLD FROM IDG

Cisco makes its routing software more resilient

New features designed to avoid data loss, network outages

MORE LIKE THIS

2



UK and US to simulate cyber-attack on nuclear plants to test resilience

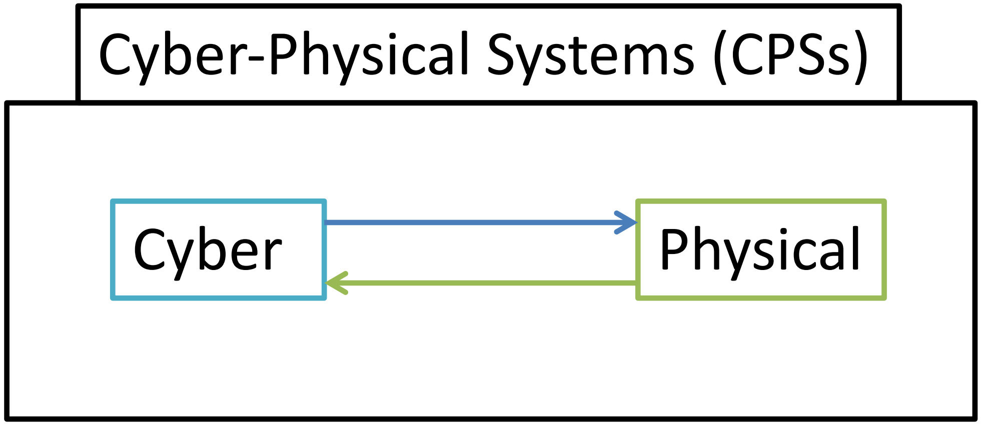
theguardian

[1] http://www.computerworld.com/article/2575855/networking/cisco-makes-its-routing-software-more-resilient.html

[2] https://www.theguardian.com/uk-news/2016/mar/31/uk-us-simulate-cyber-attack-nuclear-plants-test-resilience

Resilience

- Latin *resiliens* – to rebound, recoil

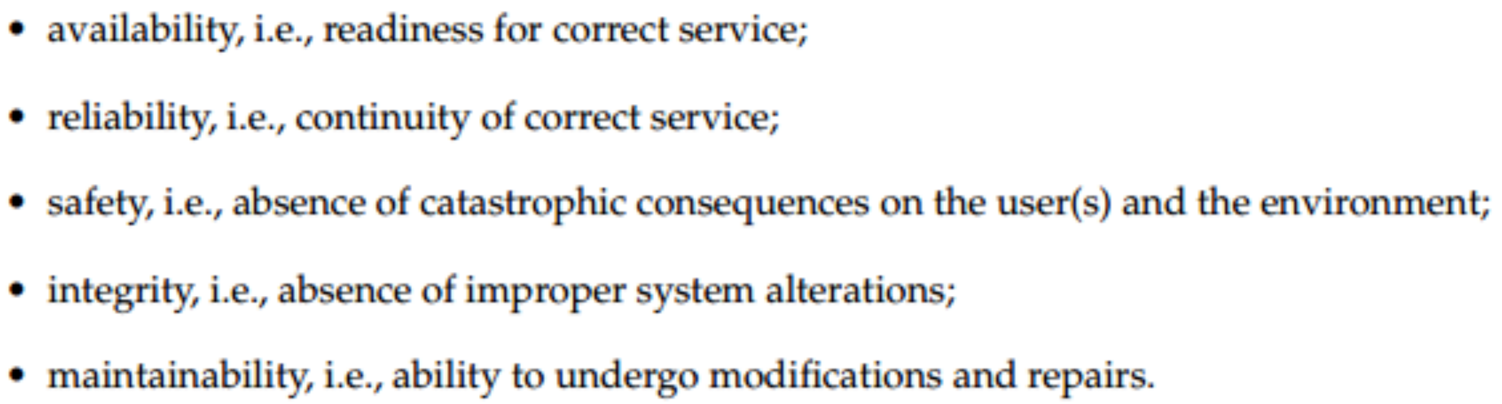


Resilience - Computing

- Dependable Computing[1] – Resilience is fault tolerance.

“The persistence of dependability when facing changes.”

~ *(Jean-Claude Laprie, 2008)*



- availability, i.e., readiness for correct service;
- reliability, i.e., continuity of correct service;
- safety, i.e., absence of catastrophic consequences on the user(s) and the environment;
- integrity, i.e., absence of improper system alterations;
- maintainability, i.e., ability to undergo modifications and repairs.

[1] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” Dependable and Secure Computing, IEEE Transactions on, vol. 1, pp. 11–33, Jan 2004.

Resilience - Systems

- Systems Engineering – INCOSE Resilient Systems Working Group,

[2]Capacity - the ability of a system to absorb or adapt to a disruption without a total loss of performance or structure.

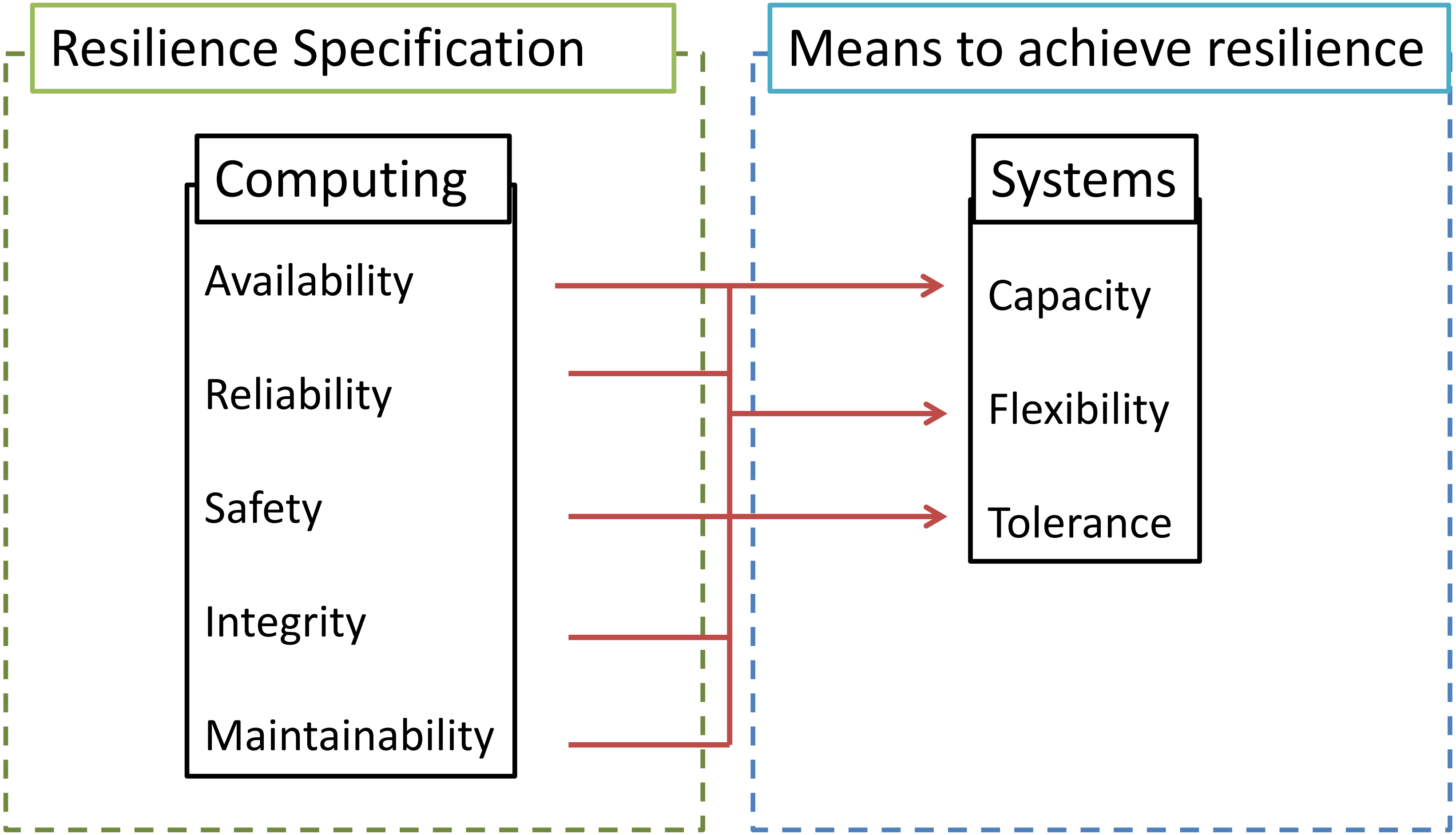
Flexibility - the ability of a system to restructure itself in response to disruptions.

Tolerance - the ability of a system to be tolerant to disruptions.

[2] S. Jackson, Architecting resilient systems: Accident avoidance and survival and recovery from disruptions, vol. 66. John Wiley & Sons, 2009.

Resilience - CPSs

There is no standard definition of resilience in CPSs.



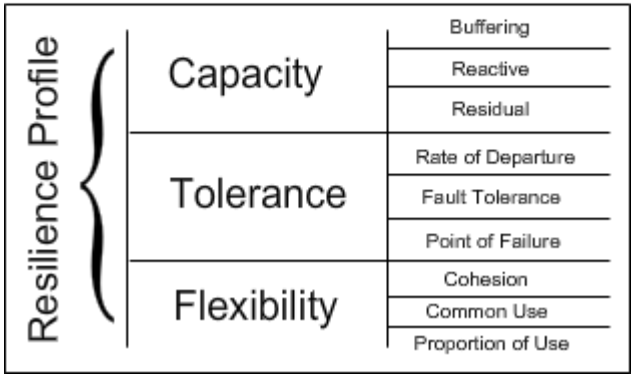
Objectives of work

- Characterise Resilience – Bridge the gap between public notion of resilience, and resilience in CPSs.
- Analyse & Evaluate Resilience in a model-based engineering approach.

Characterisig Resilience

Quantifying Resilience

- Pflanz provided extended methods for quantifying resilience.



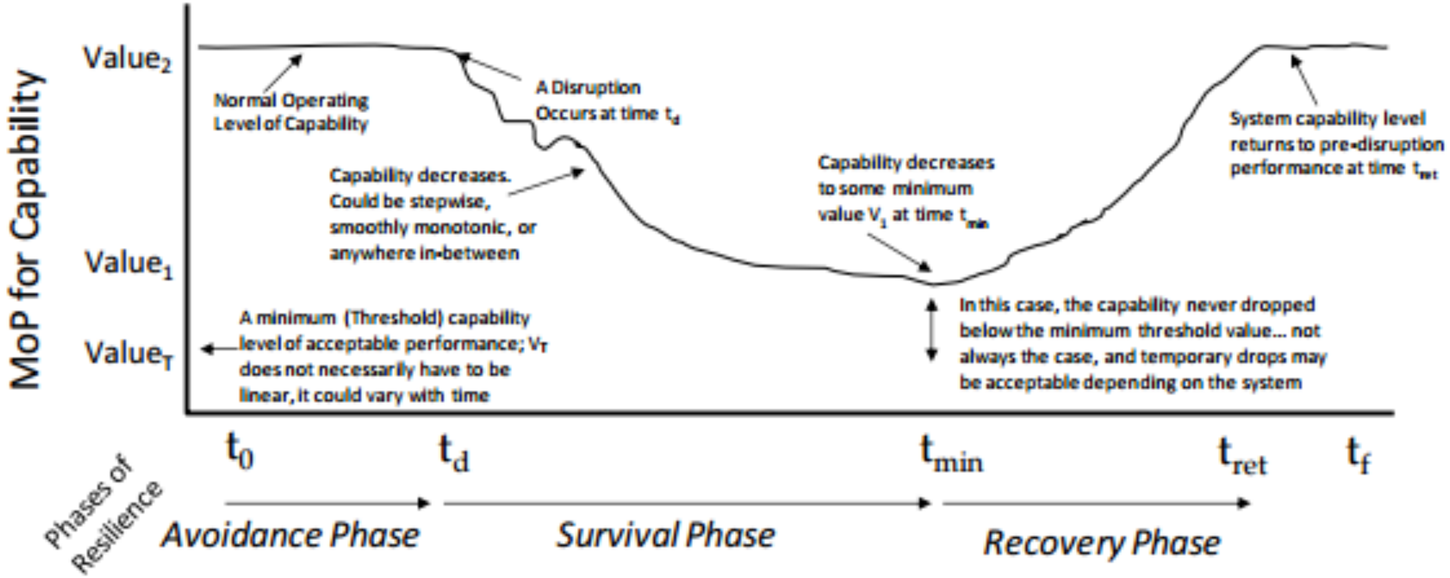
Resilience Profile

Resilience Profile	Capacity	Buffering
		Reactive
		Residual
	Tolerance	Rate of Departure
		Fault Tolerance
		Point of Failure
	Flexibility	Cohesion
		Common Use
		Proportion of Use

Characterising Resilience

Quantifying Resilience

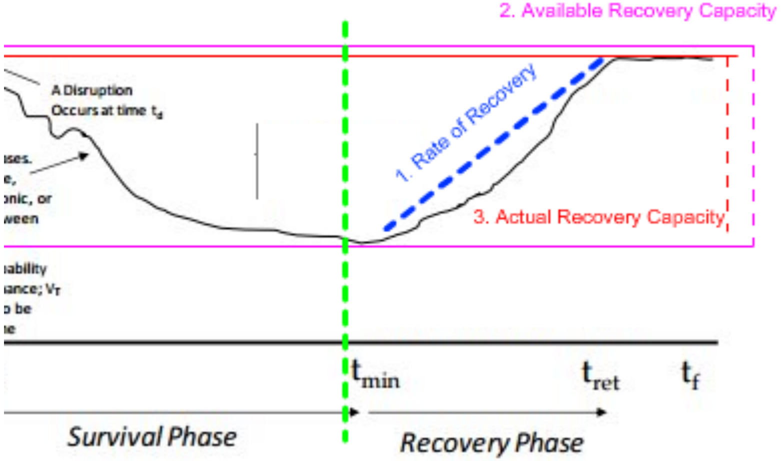
- Pflanz provided extended methods for quantifying resilience.

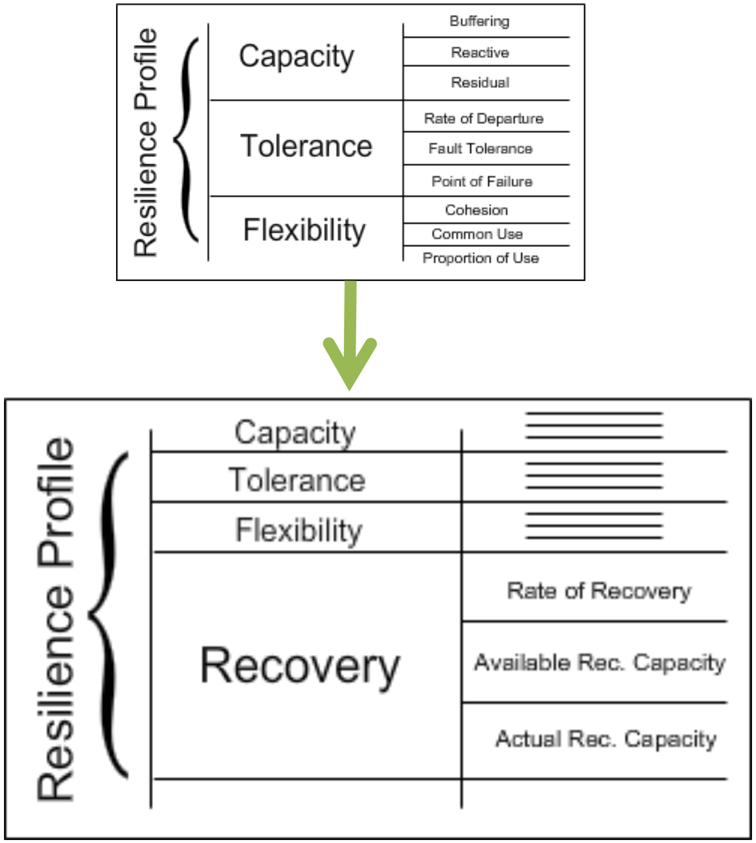

MoP for Capability
Value₂
Value₁
Value_T
Normal Operating Level of Capability
A Disruption Occurs at time t_d
Capability decreases. Could be stepwise, smoothly monotonic, or anywhere in-between
Capability decreases to some minimum value V₁ at time t_min
System capability level returns to pre-disruption performance at time t_ret
A minimum (Threshold) capability level of acceptable performance; V_T does not necessarily have to be linear, it could vary with time
In this case, the capability never dropped below the minimum threshold value… not always the case, and temporary drops may be acceptable depending on the system
t₀
t_d
t_min
t_ret
t_f
Phases of Resilience
Avoidance Phase
Survival Phase
Recovery Phase

CharactersingResilience

Quantifying Resilience

- Pflanz provided extended methods for quantifying resilience.

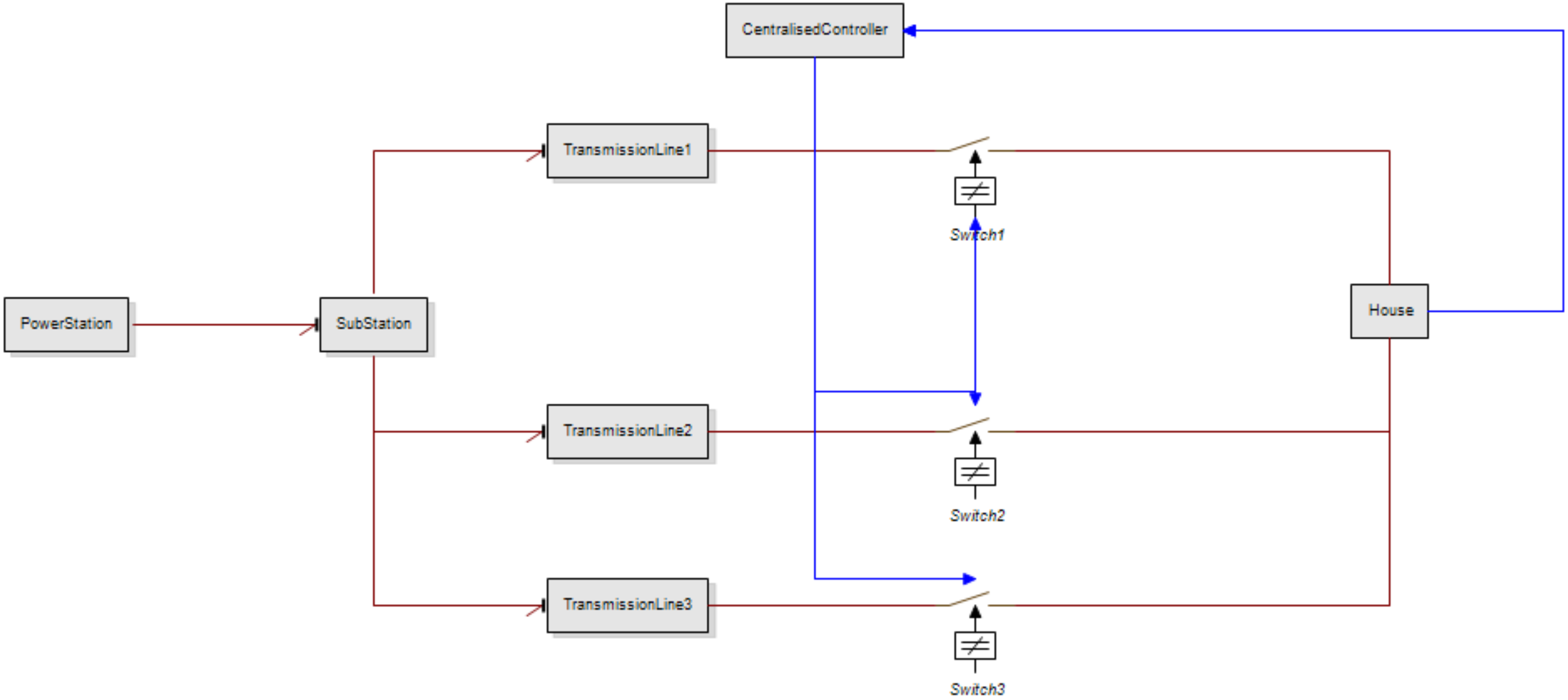




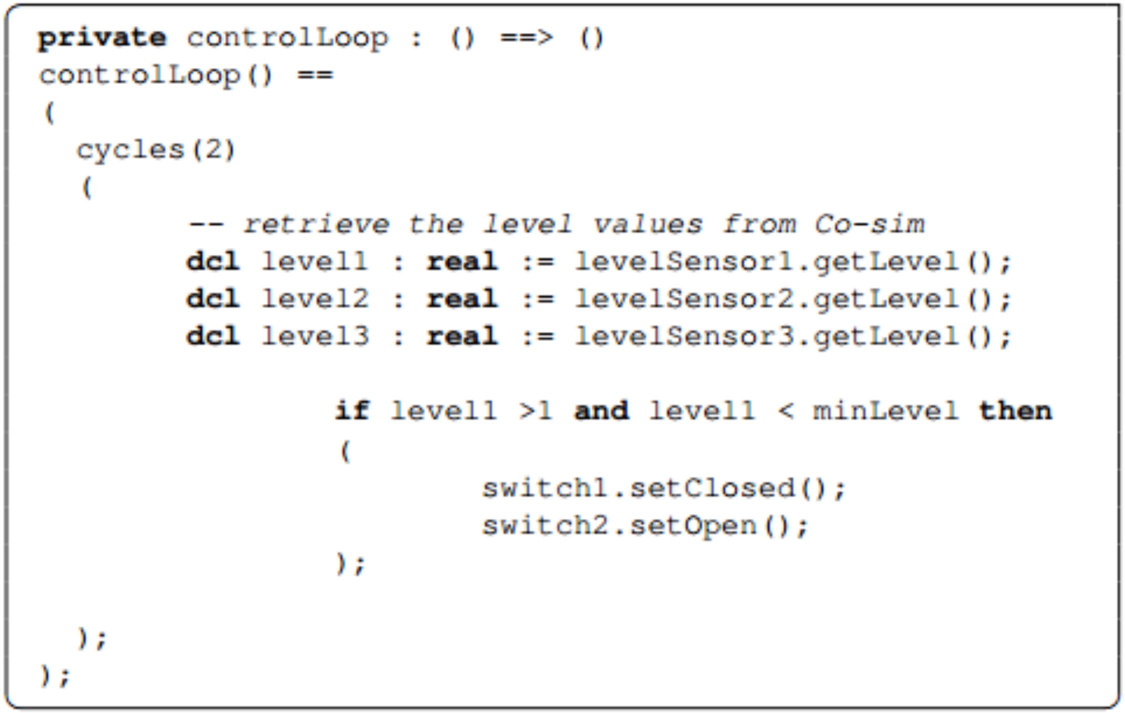
Resilience Profile	Capacity	Buffering Reactive Residual
	Tolerance	Rate of Departure Fault Tolerance Point of Failure
	Flexibility	Cohesion Common Use Proportion of Use

Resilience Profile	Capacity	
	Tolerance	
	Flexibility	
	Recovery	Rate of Recovery Available Rec. Capacity Actual Rec. Capacity

Analysing Resilience



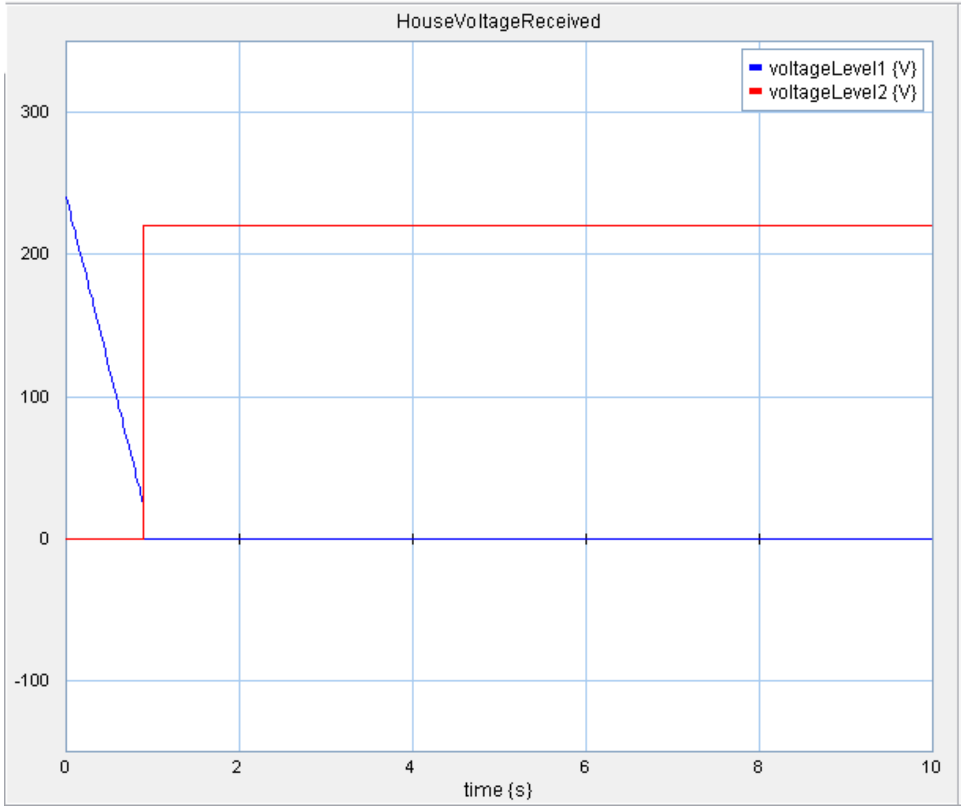
Analysing Resilience



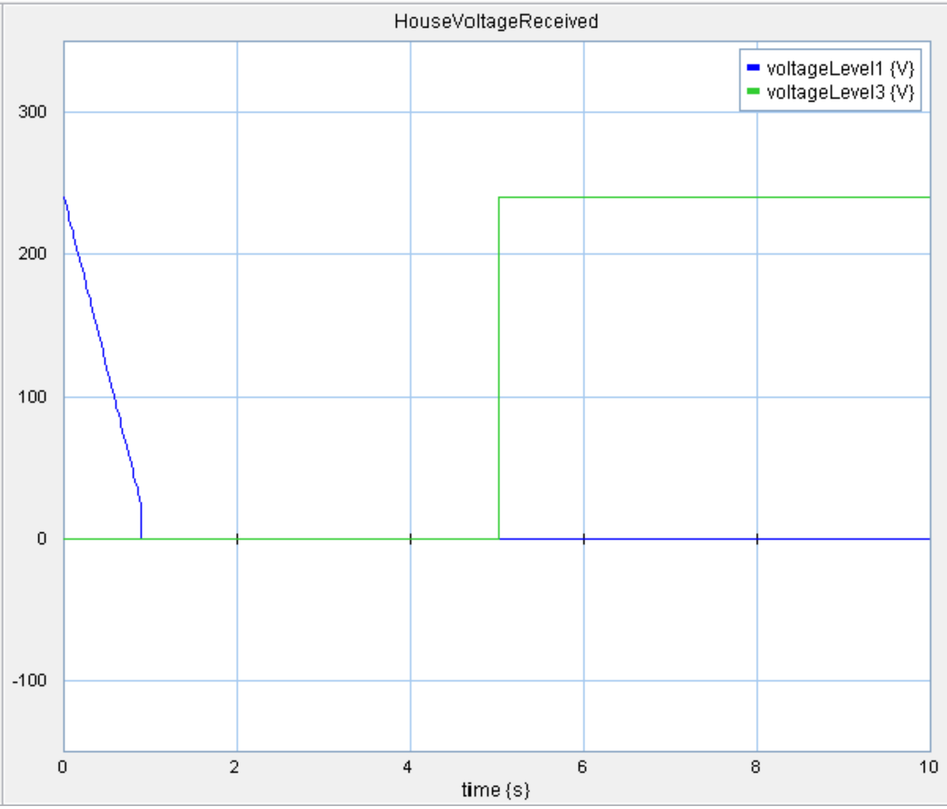
```
private controlLoop : () ==> ()
controlLoop() ==
(
  cycles(2)
  (
        -- retrieve the level values from Co-sim
        dcl level1 : real := levelSensor1.getLevel();
        dcl level2 : real := levelSensor2.getLevel();
        dcl level3 : real := levelSensor3.getLevel();

                if level1 >1 and level1 < minLevel then
                (
                        switch1.setClosed();
                        switch2.setOpen();
                );

  );
);
```

Analysing Resilience

Transmission Line 1 - Transmission Line 2

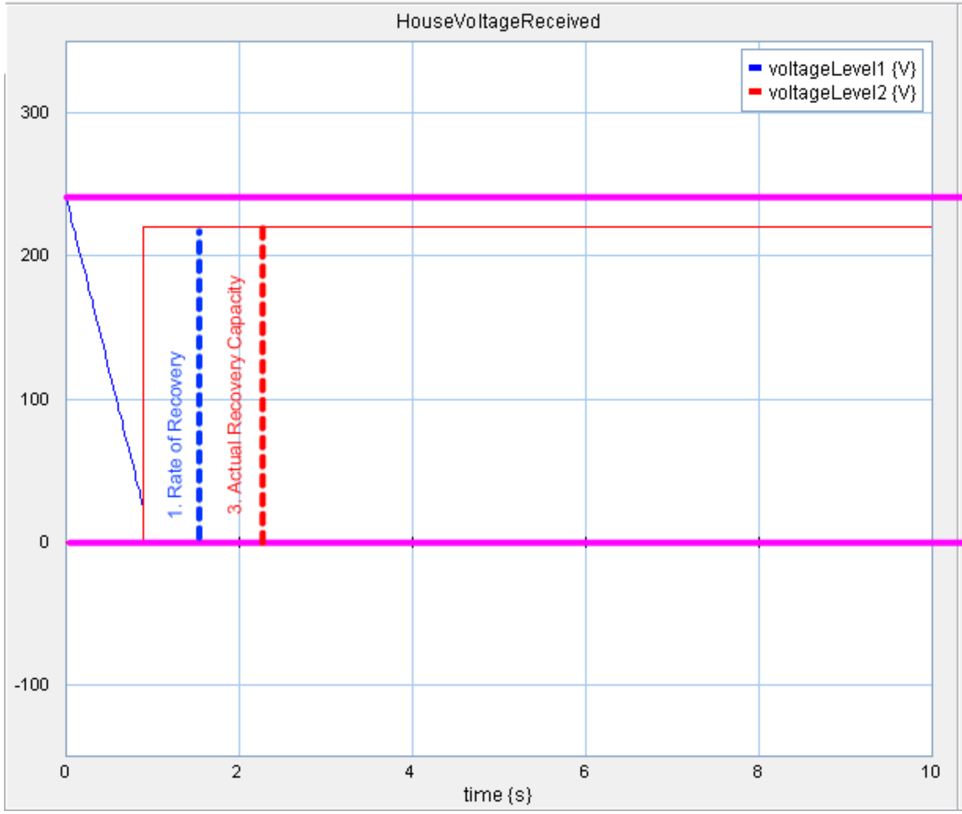


Transmission Line 1 - Transmission Line 3

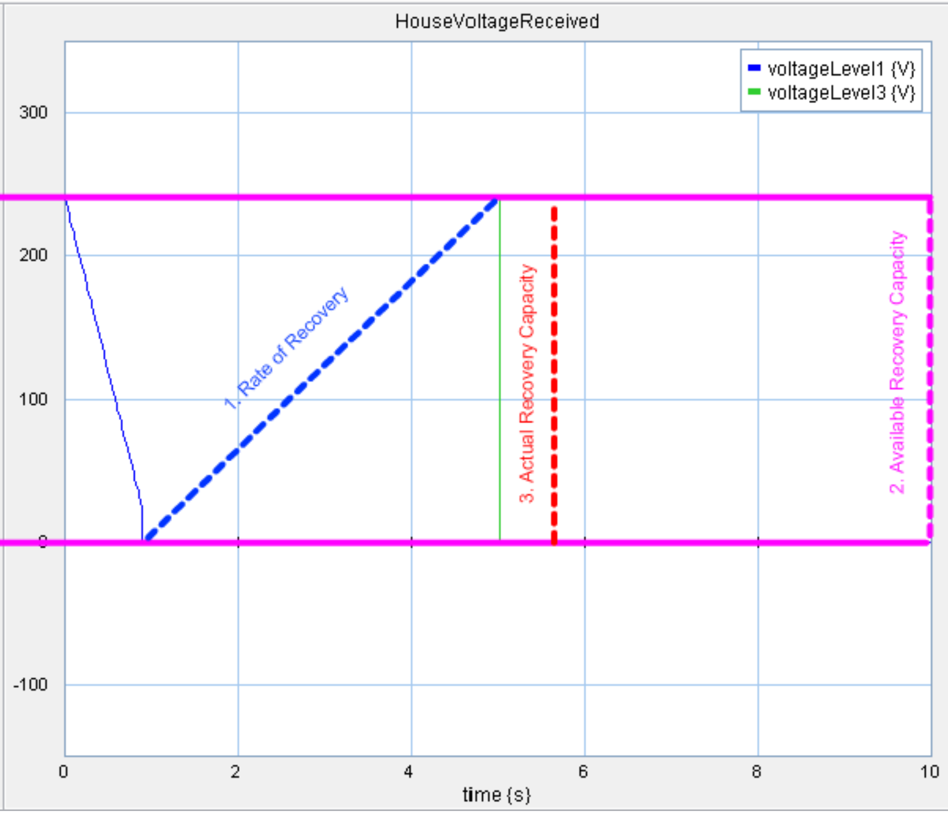


Analysing Resilience

Transmission Line 1 - Transmission Line 2

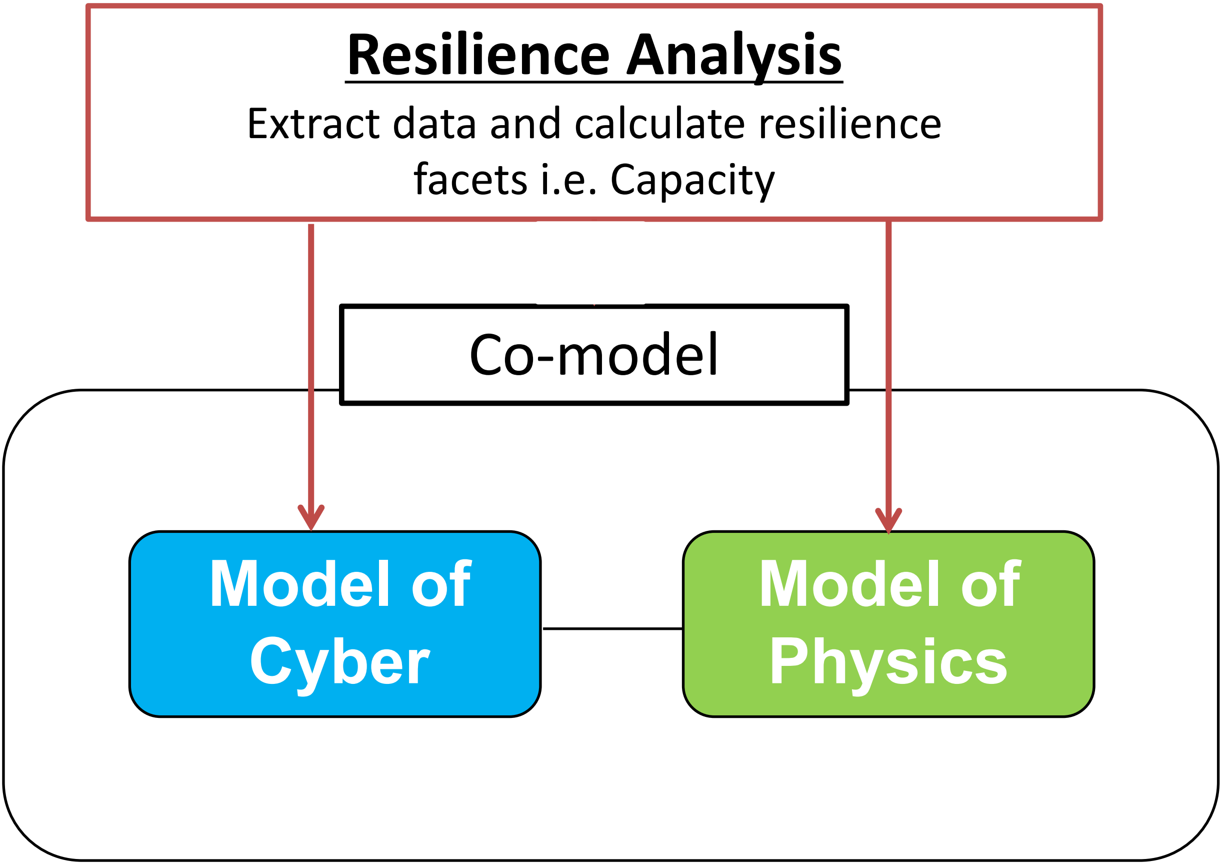


Transmission Line 1 - Transmission Line 3

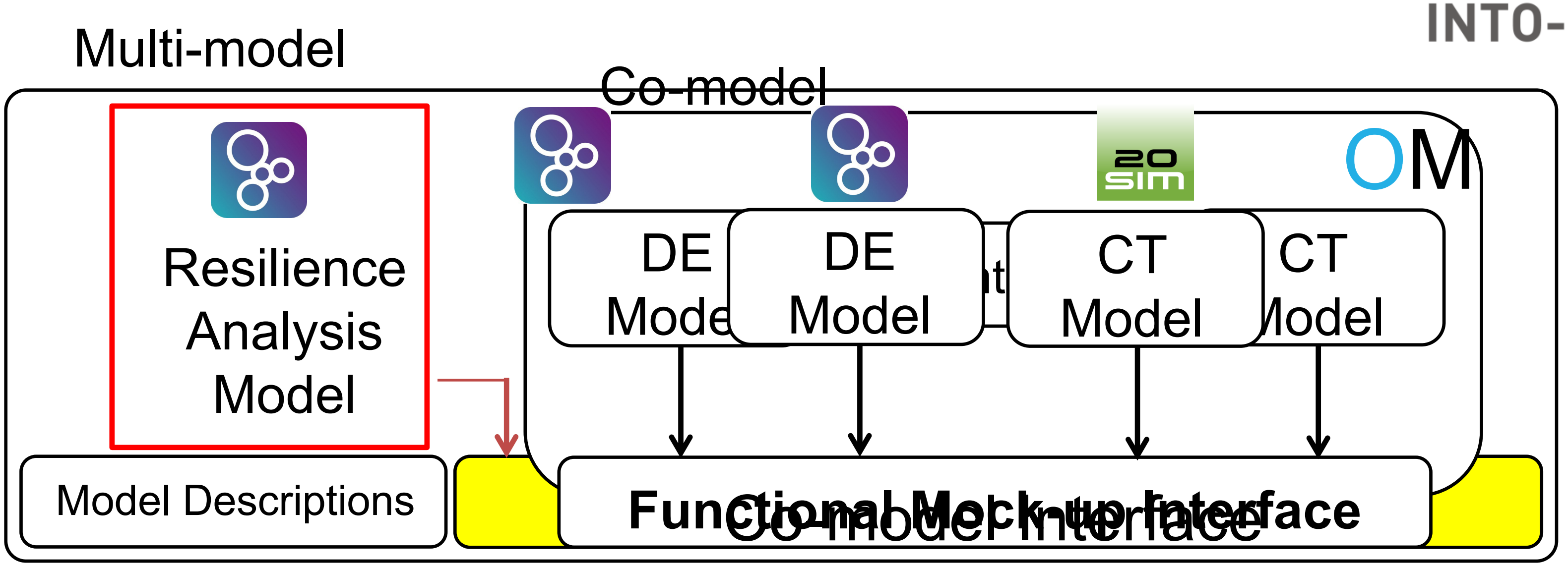


Integrating Resilience Analysis

- Resilience is often a collection of non-functional requirements.



Integrating Resilience Analysis



Modelio **Overture** **20-sim** **OpenModelica** **Crescendo** **TWT Engine** **RT-Tester**

SysML modelling

Discrete-event modelling

Continuous-time and physical-systems modelling

Co-simulation solutions

Test automation / model checking

Evaluating Resilience

Architectural Model

- Architectural Description Language such as **SysML**
- Define system components and information paths

Formal Model

- Formalise resilience profile and represent it in a formal modelling language such as **VDM**

Data Outputs

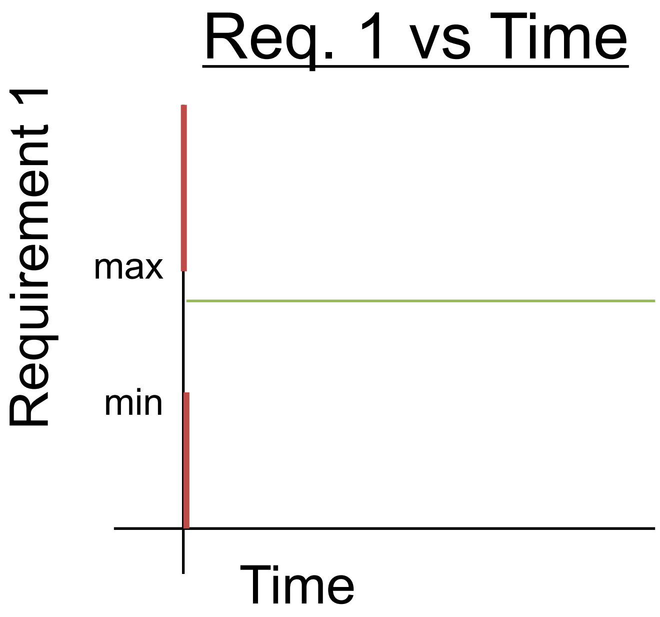
- Analyse data in graphs from the output of simulations

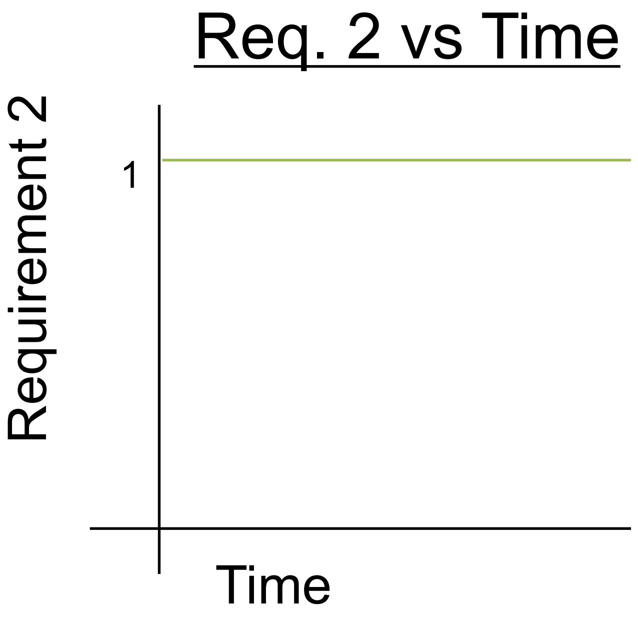
Evaluating Resilience

System Performance: At what rate does a system meet its requirements

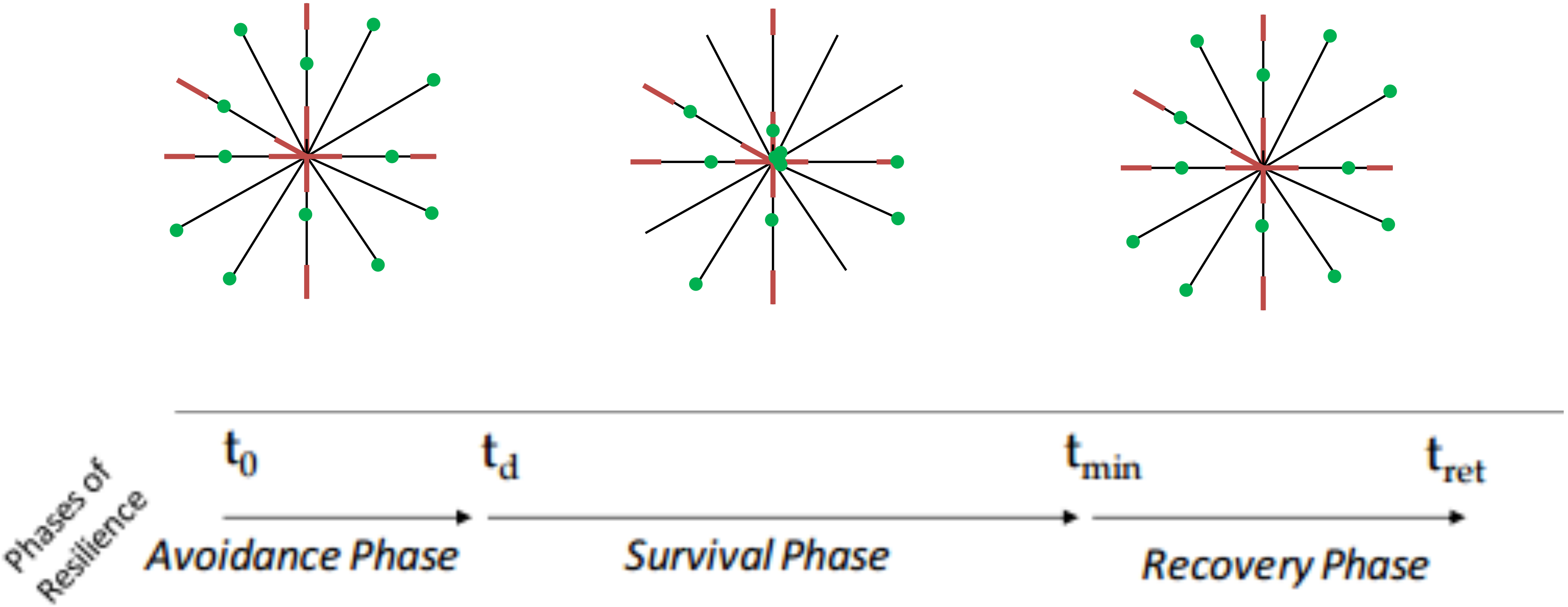
Requirement 1: Power received must be within bounds min and max at all times.

Requirement 2: The house must receive power within 3 hours after a power outage.





Evaluating Resilience



Phases of Resilience

t_0 t_d t_{min} t_{ret}

Avoidance Phase

Survival Phase

Recovery Phase

Summary & Future Work

- Characterise Resilience – Bridge the gap between public notion of resilience, and resilience in CPSs.
- Analyse & Evaluate Resilience in a model-based engineering approach - formalise profile and integrate into a model-based engineering approach.

Thank you for listening!

m.jackson3@ncl.ac.uk