COMPUTING SCIENCE

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

Authors: Mark Jackson and John Fitzgerald

TECHNICAL REPORT SERIES

No. CS-TR-1500 September 2016

TECHNICAL REPORT SERIES

No. CS-TR-1500 September, 2016

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

Authors: Mark Jackson and John Fitzgerald

Abstract

We consider the potential to use co-modelling and co-simulation in the design of dependably resilient Cyber-Physical Systems (CPSs). The topic of resilience is widely discussed in the public discourse on CPSs, but is rarely well defined. We propose the description of system resilience in terms of a composite profile which may be used as a basis for assessment and trade-off analysis in CPSs. Our profile has a particular focus on description of system recovery behaviour. As a first evaluation of the concept, we present a case study based on a VDM and 20-sim co-model of a small smart grid illustrating causal chains that cross the cyber-physical boundary. An evaluation of the study leads to suggestions for a further proof-of-concept study that experiments with increasingly challenging CPS architectures.

Printed and published by Newcastle University,
Computing Science, Claremont Tower, Claremont Road,
Newcastle upon Tyne,
NE1 7RU, England.

Bibliographical details

Resilience Profiling in the Model-Based Design of Cyber-Physical Systems
Authors: Mark Jackson and John Fitzgerald

NEWCASTLE UNIVERSITY
Computing Science. Technical Report Series. CS-TR-1500

Abstract

We consider the potential to use co-modelling and co-simulation in the design of dependably resilient Cyber-Physical Systems (CPSs). The topic of resilience is widely discussed in the public discourse on CPSs, but is rarely well defined. We propose the description of system resilience in terms of a composite profile which may be used as a basis for assessment and trade-off analysis in CPSs. Our profile has a particular focus on description of system recovery behaviour. As a first evaluation of the concept, we present a case study based on a VDM and 20-sim co-model of a small smart grid illustrating causal chains that cross the cyber-physical boundary. An evaluation of the study leads to suggestions for a further proof-of-concept study that experiments with increasingly challenging CPS architectures.

About the authors

Mark Jackson is a doctoral candidate in the School of Computing Science at Newcastle University. He gained a first class honours degree in Computer Science from Newcastle University in 2014, then progressed to studying a full time PhD in Computer Science. Mark's research aims to address the challenges of modelling and assuring resilience in cyber-physical systems; and to provide methods for analysing resilience in the model-based development for systems that include both discrete-event and continuous-time components.

John Fitzgerald is a full professor in the School of Computing Science at Newcastle University, where he heads the research group on Advanced Model-based Engineering. With a background in formal validation and verification, he has been working as a researcher and industry practitioner on model-based design since the early 1990s. He led the European Union's COMPASS programme on model-based engineering of systems of systems, and now works on techniques for multidisciplinary design of cyber-physical systems as part of the INTO-CPS and CPSE Labs projects. He plays a leading role in the £56 million Urban Sciences project, creating a campus and laboratory for research, innovation and teaching in computing and urban systems at scale in the heart of the city of Newcastle upon Tyne. He is a Fellow of the British Computer Society, and a member of the ACM, IEEE and INCOSE.

Suggested keywords

Co-Modelling, Co-Simulation, Cyber-Physical Systems, Resilience, Smart Grid, VDM, Overture

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

Mark Jackson and John S. Fitzgerald

Newcastle University, UK
{M.Jackson3, John.Fitzgerald}@newcastle.ac.uk

Abstract. We consider the potential to use co-modelling and co-simulation in the design of dependably resilient Cyber-Physical Systems (CPSs). Resilience is widely discussed in the public discourse on CPSs, but has many definitions. We propose the description of system resilience in terms of a multi-attribute profile which may be used as a basis for assessment and trade-off analysis in CPSs. Our profile has a particular focus on description of system recovery behaviour. As a first evaluation of the concept, we present a case study based on a VDM and 20-sim co-model of a small smart grid illustrating causal chains that cross the cyber-physical boundary. An evaluation of the study leads to suggestions for further proof-of-concept studies that experiment with increasingly challenging CPS architectures.

1 Introduction

> In complex environments, resilience often spells success, while even the most brilliantly engineered fixed solutions are often insufficient or counterproductive.
>
> *McChrystal et al. [1]*

Cyber-Physical Systems (CPSs) formed from the integration of computational and physical processes [2] are a natural evolution of embedded devices in networked environments [3]. Examples range from medical devices and automotive control systems, to "smart" infrastructures in areas such as road traffic management and energy grids [4,5]. In many cases, existing physical infrastructure is overlaid with a computer network that – in principle – offers more efficient and reactive control with greater autonomy than is delivered by individual embedded or centralised architectures. However, computer networks are complex (in the sense that small changes can have remote and large-scale effects), and are vulnerable to failure and attack modes that can be difficult to predict and test. Adding cyber networks to physical infrastructure is therefore a risky business. Controlling this risk requires both design methods that promote detection and avoidance of vulnerabilities, and building-in the capacity to recover from unanticipated faults or attacks.

Much of the public discourse on infrastructure is concerned with *resilience*. Although widely used, the term appears to have a range of meanings in different sectors. The United Kingdom's National Resilience Capabilities programme sees it as "the

ability of assets and networks to anticipate, absorb, adapt to and recover from disruption" [6]. It is open to debate whether this might be defined in terms of properties such as fault avoidance, detection, tolerance and recovery [7], but the term is often used in a broader sense to include adaptive capacity [8]. Given the range of facets of resilience that are important in different application sectors, it is apparent that a nuanced characterisation of resilience is needed to facilitate disciplined engineering.

Engineering dependably resilient CPSs is a demanding goal [9], and many CPSs emerge or are developed without resilience in mind at all. Model-based systems engineering methods offer considerable promise, but are challenged by the independence and heterogeneity of CPS constituents. Several of these challenges are addressed by co-modelling technology such as that explored in INTO-CPS[1]. Predecessor projects such as DESTECS[2] and COMPASS[3] demonstrated model-based engineering for fault tolerance in these settings. It is therefore legitimate to ask whether co-modelling can help to deliver dependably resilient CPSs. This is the subject of our current work.

We discuss background and related work on resilience in Section 2. Given the need for a nuanced characterisation of resilience, we discuss *resilience profiling* (Section 3) and consider how this might be realised in heterogeneous co-models of CPSs. An example based on a simple smart grid is presented (Section 4). Our work is at an early stage; Section 5 describes future directions.

2 Background and Related Work

We aim to provide usable methods and tools for engineering dependably resilient CPSs. In this section, we describe the scope and background to our work. We briefly indicate what we mean by a CPS, explain why we focus on model-based techniques and introduce our baseline tools. We then examine in more detail the existing work on resilience profiling in CPS-related contexts.

Multidisciplinary Model-Based Design for CPSs

A CPS integrates computational and physical processes [2]. CPS engineering therefore should therefore address the integration of methods and tools from different (discrete and continuous) domains and disciplines [10]. The focus of much current work, including our own, is on systems of networked computing elements, including "smart" devices, that together deliver emergent properties on which reliance is placed. This adds to the mix important systems-of-systems (SoS) aspects, including the need to integrate independently owned and managed systems, the ability to reason about the composition of the contractual interfaces between them, and the ability to deal with dynamically evolving structures over the life of the CPS [11, 12].

Collaborative and multi-paradigm Model-Based Design (MBD) techniques have been proposed as a means of evaluating alternative architectures and functionality, and providing early identification of defects in CPSs [13]. Realising the value of such approaches requires a semantic basis for linking models given in diverse notations, the

[1] `http://into-cps.au.dk/`
[2] `http://www.destecs.org/`
[3] `http://www.compass-research.eu/`

ability to compose abstract descriptions of interfaces between system elements, and the ability to describe architectures explicitly.

Much research builds on hybrid systems as a common semantic framework for CPSs [14]. Rather than work with a single formalism, we aim at an extensible framework able to integrate the diverse formalisms used in practice. In the work discussed here, we take Crescendo[4] as a baseline technology. In Crescendo, a model of a CPS is actually a *co-model* with discrete-event (DE) and continuous time (CT) models (in VDM/Overture and 20-sim respectively) as its constituents. Crucially for our work, the approach allows the direct modelling of causal chains across the cyber-physical boundary. A bespoke co-simulation harness implements an operational semantics that manages time and communication between the separate DE and CT models running in their own simulators. The emerging INTO-CPS tool chain promises to extend this to an n-ary multi-modelling approach, allowing co-simulation of executables derived from multiple modelling tools [15]. It leverages Unifying Theories of Programming (UTP) to permit extensible and reusable semantics [16]. At the time of writing, the INTO-CPS framework is not quite able to handle multi-models of the type needed for our smart grid applications, and we remain with Crescendo for the moment.

Resilience

Resilience is important in many fields [17, 18]. In materials science it is "the ability of a material to absorb energy when deformed elastically and to return it when unloaded" [19]. In IT and organisational contexts, a resilient control system has been characterised as "one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature" [20]. In the context of power systems, it is seen as the ability of a system to degrade gracefully under extreme perturbations, and recover quickly after the events have ceased [21]. In socioecological systems Carpenter et al. argue that an assessment of system resilience must be qualified by specifying which system configuration and disturbances are of interest (resilience 'of what, to what, and under what conditions') [22]. Recent European research calls on crisis management see resilience as the ability to reduce the impact of disruptive events and the recovery time [23].

Together, the approaches in the literature reflect the idea that resilience as a composite property: a system cannot simply be said to either be resilient or not, but may be said to show some characteristics of resilience in response to a certain set of faults or attacks under certain circumstances. There is a also a trade space here: for example, a system may be show resilience to a certain set of attacks, but at the expense of becoming less resilient to others, or at the price of slower recovery. Again, being able to trace cause and effect as they go across the cyber-physical boundary is critical to effective model-based engineering of resilience.

Among the few current research projects directly addressing CPS resilience are ADREAM[5], FORCES[6], and SURE[7]. ADREAM aims to investigate and develop core

[4] `http://crescendotool.org/`
[5] `https://www.laas.fr/public/en/adream-project`
[6] `https://www.cps-forces.org/`
[7] `http://cps-vo.org/group/sos/sure/`

technologies, methodologies and components that will enable the successful design of dependable CPSs. FORCES aims to increase the resilience of large-scale networked CPSs in the key areas of energy delivery, transportation, and energy management in buildings. SURE will develop foundations and tools for designing, building, and assuring CPSs that can maintain essential system properties in the presence of adversaries. Although few outputs are available from these projects at this time, there is an emerging body of work aiming to address CPS resilience.

Resilience Profiling

To analyse resilience in model-based CPS design, we need a working intuitive characterisation of resilience. We adopt some of the terminology of faults, errors and failures [7] in that we regard a failure as the deviation of a delivered service from correct service. An error occurs when the state of the system deviates from those required to deliver a correct service. A fault is the adjudged or hypothesized cause of an error. An error does not necessarily cause a failure, but it is possible one or more errors may. Throughout this report we describe a specific fault–error–failure casual chain as a *resilience scenario*.

Rather than identify a single resilience metric, we treat it as a multi-attribute property defined in what we will call a *resilience profile*. The idea of a multifaceted definition of resilience is not new. Jackson [24] proposes a representation of resilience composed of four attributes:

Capacity: the ability of a system to absorb or adapt to a disturbance without a total loss of performance or structure.
Tolerance: the exhibition of graceful degradation near the boundary of a system's performance.
Flexibility: the systems ability to restructure itself in response to disruptions.
Inter-element Collaboration: collaborations, or communication and cooperation between human elements of a system.

A resilience scenario is divided into three aspects:

Avoidance: the preventive aspects of system resilience in response to a disruption, either internal or external.
Survival: implies that the system has not been destroyed or totally incapacitated and continues to function when experiencing a disturbance.
Recovery: the capability of surviving a major disturbance with reduced performance. This capability is a focus of system resilience.

Pflanz [25] extends Jackson's characterisation, applying it to command and control systems. Although Pflanz does not consider inter-element collaboration, he subdivides the first three of Jackson's attributes into the constituent facets listed in Figure 1. Jackson's resilience scenarios were then implemented by Pflanz as temporal phases, as shown in Figure 2.

Pflanz's work focuses on the survival phase, where capacity, tolerance and flexibility provide means of analysing resilience in this phase alone. However, there is only limited further discussion of ways in which to characterise recovery.

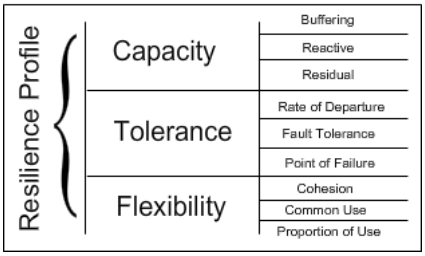

Fig. 1. Outline of Pflanz's Resilience Profile.

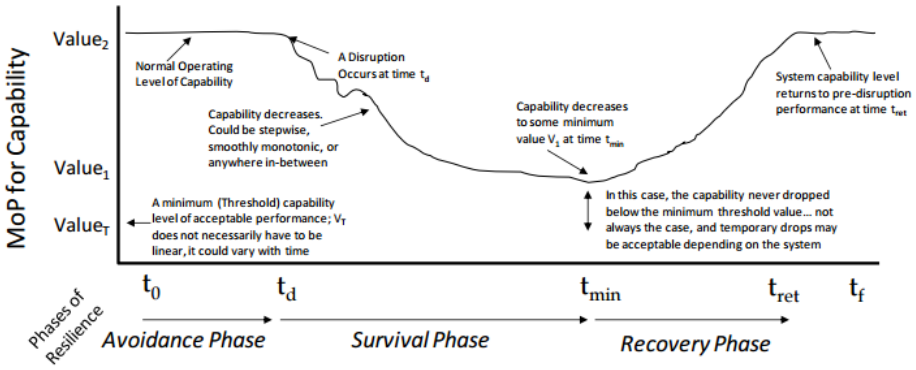

Fig. 2. Avoidance, Survival and Recovery as temporal phases, from [25].

Research Landscape

Although increasing importance is attached to the resilience of the CPSs on which we depend, there is no widely accepted definition of the concept, still less methods and tools for he lack of a coherent definition of resilience in the field, and a lack of methods for analysing resilience as a profile, especially in the recovery phase. In our current work, we therefore have two main goals. First, to deliver a resilience profile that describes resilience in the context of CPS, specifically characterising the recovery phase. Secondly we will provide methods for analysing co-models in the MBD of CPS.

3 Resilience Profiling

In this section we describe our approach to delivering the two goals mentioned at the end of Section 2. We extend the resilience profile described with new attributes which elaborate the **recovery phase**. We initially present one new attribute 'Recovery' with three facets described below and indicated in Figure 3:

Rate of Recovery: the rate at which system performance returns to an acceptable level.

Available Recovery Capacity: the available performance margin from the current operating levels to the expected recovery operating level.

Actual Recovery Capacity: the actual performance margin from the current operating levels to the recovery operating levels.

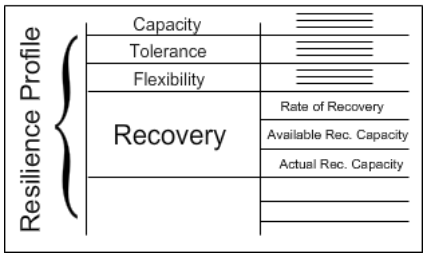

Fig. 3. Extending the resilience profile to characterise recovery.

As shown in Figure 4, the (average) Rate of Recovery (in blue) is measured by the Measure of Performance Capability (y-axis) divided by time (x-axis). The Actual Recovery Capacity (in red) is measured from the point in which the performance value settles within a range of acceptable levels, however never reaches the Available Recovery Capacity (purple) which we assume is higher. Further analysis of resilience lies in the ability to compare our attributes in our profile (as shown in Section 4).

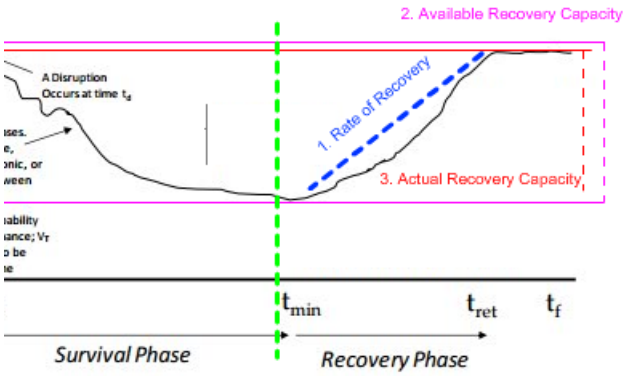

Fig. 4. Recovery Attributes: Rate of Recovery, Available Recovery Capacity and Actual Recovery Capacity.

Given a co-model that can co-simulate a resilience scenario, how can we assess the resilience of the system of interest according to our extended profile? First, we must

ensure that the co-model is *competent* in the sense that it incorporates sufficient features to allow resilience attributes to be assessed; this amount to ensuring we can observe the properties needed for the y-axis of the graphs shown in Figures 2 and 4. This could potentially involve instrumenting the constituent models by adding, e.g. methods in Overture or 20-sim. Second, we can visualise or post-process co-simulation output data to generate the elements needed for analysis against our resilience profile. in either case, the key question lies with the CPS design engineer on exactly what properties need to be measured. In some cases the y-axis measure may be composed of properties both cyber and physical in nature.

4 Example

In this section we describe an example co-model from the smart grids domain. We first explain why we have chosen this application area to evaluate our extended resilience profile. Second we demonstrate how we can use our co-model to produce sufficient data so that we are be able to analyse the resilience of an example grid.

Smart Grids

In seeking to extend the resilience profile so as to better incorporate recovery, we need to validate the approach with example studies. In order to be credible, these should be in a well established and accepted CPS domain [4, 5]. In order to test the capabilities of formalisms, they should be capable of incorporating a series of increasingly demanding architectures, including centralised, distributed, and modular control. Finally, the resilience of the systems of interest should be both desirable to have, and challenging to deliver.

Smart power grids present one such area. Such a grid is a complex ecosystem of heterogeneous (co-operating) entities that interact in order to deliver specific functionality related to the generation, transmission, storage and consumption of (usually electrical) energy [4]. It is an archetypal example of a CPS, in which the power network is overlaid with a computing and communication network, and the two are coupled together into what is generally perceived as a single system of interest [5,26]. CPS technology is seen as an integral part of the smart grid concept and resilience in smart grids is identified as a key challenge [9, 27]. There is interest in increasing local control and autonomy to better match supply and demand in smart grids, and the idea of a local microgrid provides a modular control concept. Finally, significant reliance is placed on the energy supply, even in the face of natural or human-made disruptions. Together these factors make smart grids a suitable example domain for our work.

Co-model Example

To demonstrate our approach to analyse our resilience profile, we have created an example co-model of a Smart Grid with a centralised controller in Crescendo. In our example, we model the physical environment in 20-sim which includes a physical description of

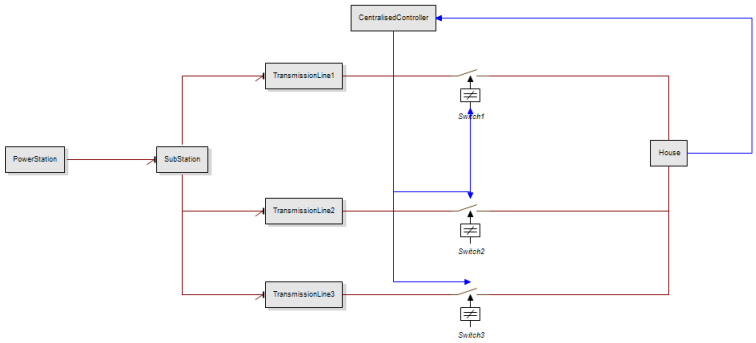

Fig. 5. 20-sim CT model: An example smart grid.

the grid's components ranging from power stations and transmission lines, to sensors and actuators.

Figure 5 is a representation of the CT model in our co-model example in 20-sim. This gives us an overview of our physical system, in which we include 1 PowerStation, 1 SubStation, 3 TransmissionLines, 3 Switches and 1 House. To give context, Figure 6 shows us the CT logic for Switch1. This is an example of the types of CT equations present in our physical model in 20-sim.

```
parameters
   real Ron = 0.00001 {ohm};     // Resistance when switched on
   real Roff = 100000.0 {ohm};      // Resistance when switched off
   real vt = 0.5; //threshold value, switch = on when abs(input)>vt
variables
   real R {ohm};
equations
   R = if input > vt then Roff else Ron end;
   p.u = R * p.i;
```

Fig. 6. A code snippet from within Switch1.

Our DE model is written using VDM-RT. This is where we write our controller logic and any other cyber functionality present in our CPS. Figure 7 shows the controller logic used in our co-model when deciding to switch transmission lines. The logic changes switch state if the voltage level falls below a 'minLevel' threshold (minLevel is a shared parameter between CT and DE models).

Cross-Domain Resilience Scenarios

Cross-domain resilience scenarios are those in which the causal chain transits the boundary between cyber and physical elements. We look at how cyber faults can lead to physical failures. An example of a cyber fault is a digital controller that fails to execute its

```
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.setOpen();
                        switch2.setClosed();
                );

  );
);
```

Fig. 7. A code snippet of controller logic

control logic even though it is receiving signal data. We model this in Overture by creating a subclass of our centralised controller class. Before we co-simulate, we initialise a faulty version (subclass) of our controller class. This is in line with the fault modelling mechanisms demonstrated in [28]. The fault would cause the switches in our Smart Grid to remain in their initial state. Our controller would never switch to a different transmission line and thus may lead to the propagation of physical failures within the system.

We can also characterise physical faults leading to cyber failures. For example, we may consider a faulty voltage sensor in the house. This sends only the first voltage value. We can model this in 20-sim by creating a second (faulty) implementation of the equation model of our house. Before we co-simulate we can switch to the faulty implementation. The value sent to the centralised controller would be an outdated value, and so the controller cannot switch transmission lines if the voltage level falls below the minimum threshold (shown in Figure 7).

Resilience Profiling

To allow for the analysis of resilience, we must be able to evaluate our resilience profile against data produced from our co-models. To test our scenario, we run our co-model through a co-simulation in Crescendo. The PowerStation in our study provides power to the SubStation. The SubStation uses a step-down transformer to reduce the voltage to 240Volts(V). This power is then split across 3 transmission lines. The first source

is sent across TransmissionLine1, where it passes a closed switch to get to the house. The second and third sources of power are sent across TransmissionLine2 and TransmissionLine3 respectively, where they encounter open switches and do not reach the house. The power from TransmissionLine2 and TransmissionLine3 are considered as contingencies in the case TransmissionLine1 fails to provide adequate service.

In our scenario, TransmissionLine1 is faulty, which has lead to a steady decrease in voltage output. Our centralised controller checks the voltage level the house receives. If this level falls below a threshold, the centralised controller opens the switch to TransmissionLine1 and closes the switch to TransmissionLine2.

From Figure 8 we see a significant voltage drop from TransmissionLine1 (blue) until around 1 second into the simulation. This is when the controller has opened the switch from TransmissionLine1.

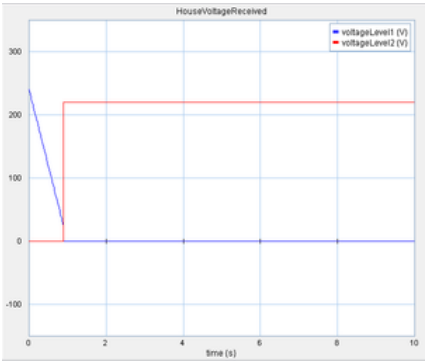

Fig. 8. A comparison of the output voltage from TransmissionLine1 and TranmissionLine2.

Figure 8 shows us the comparison between the voltage received by the house from TransmissionLine1 (blue) and TransmissionLine2 (red). The cyber controller in our DE model recognises when the voltage from TransmissionLine1 falls below our threshold and switches to TransmissionLine2. The house now receives power once again - although at a reduced voltage (220V).

With this data we demonstrate how we can analyse the resilience of our example using our resilience profile. As shown in Figure 9, from our co-model output we can analyse the three facets of our recovery phase.

1. **Rate of Recovery** - In Figure 9 we can see the gradient of the voltage increase is our Rate of Recovery (blue). In our example the switch in our transmission lines happens almost instantaneously which results in a vertical line on our graph. In this case we would have an undefined gradient. From our analysis perspective in the recovery phase this is the optimal rate at which our line can reach its Available and Actual Recovery Capacity.
2. **Available Recovery Capacity** - The Available Recovery Capacity is shown in purple in Figure 9. This is the maximum potential in which our system may recover

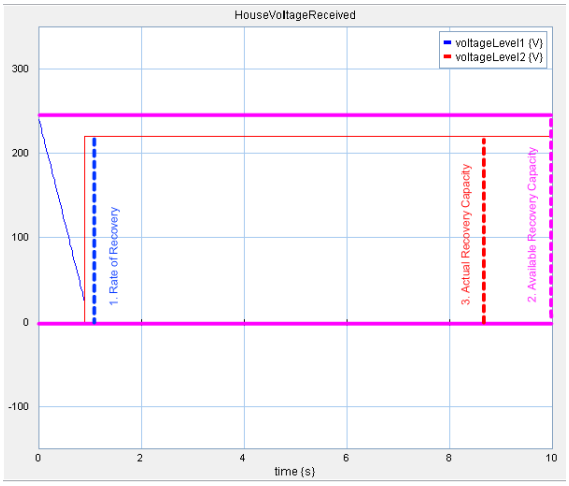

Fig. 9. An analysis of the recovery phase from a Smart Grid co-model with a centralised controller.

to. In our case TransmissionLine1's voltage dropped to 0, and the maximum difference the house can receive is the limit of our initial transmission line which is 240V. This follows that our Available Recovery Capacity is 240V.

3. **Actual Recovery Capacity** - The Actual Recovery Capacity is shown in red. In this case TransmissionLine2 is a line operating at 220V as opposed to 240V. Therefore the Actual Recovery Capacity is 220V. This is not always the case, as performance may be recovered fully, to the Available Recovery Capacity.

Resilience Trade-Off

Crescendo allows us to model resilience scenarios across both cyber and physical domains. We present a resilience scenario in which we can perform resilience profiling and trade-off analysis of our Smart Grid co-model. To perform trade-off analysis we consider two resilience scenarios:

1. **TransmissionLine1 - TransmissionLine2** - TransmissionLine2 produces power almost instantly but at a reduced voltage (220V).
2. **TransmissionLine1 - TransmissionLine3** - TransmissionLine3 produces a higher voltage (240V), but at the expense of time.

In our example we have modelled each scenario, and analysed the results. Figure 10 shows us a comparison between scenario 1 (left) and scenario 2 (right). In scenario 1 we can clearly see that TransmissionLine2 switches almost instantly and provides power to the house at a voltage of 220V. In scenario 2 the house receives power from TransmissionLine3 at around 5 seconds, this is approximately a 4 second delay from when TransmissionLine1 is switched off. It is here a CPS design engineer must consider which is more important, the Actual Recovery Capacity, or the Rate of Recovery.

Figure 11 shows the analysis of the Recovery attribute in our resilience profile. It is shown that the Available Recovery Capacity (purple) is the same in both scenarios (240V), as this is the maximum potential voltage our house can receive under normal operation. The Actual Recovery Capacity (red) for scenario 1 is 220V, whereas in scenario 2 it is 240V. The Rate of Recovery in scenario 1 is a vertical line and so we have an undefined gradient as the switch is almost instantaneous. However due to the delay of switching in scenario 2, our (average) Rate of Recovery becomes 240V divided by 4 seconds, this gives us a Recovery Rate of 60V/s. With this data a CPS design engineer can assess the trade-off between the Actual Recovery Capacity and the Rate of Recovery facets, in the Recovery Attribute of our resilience profile.

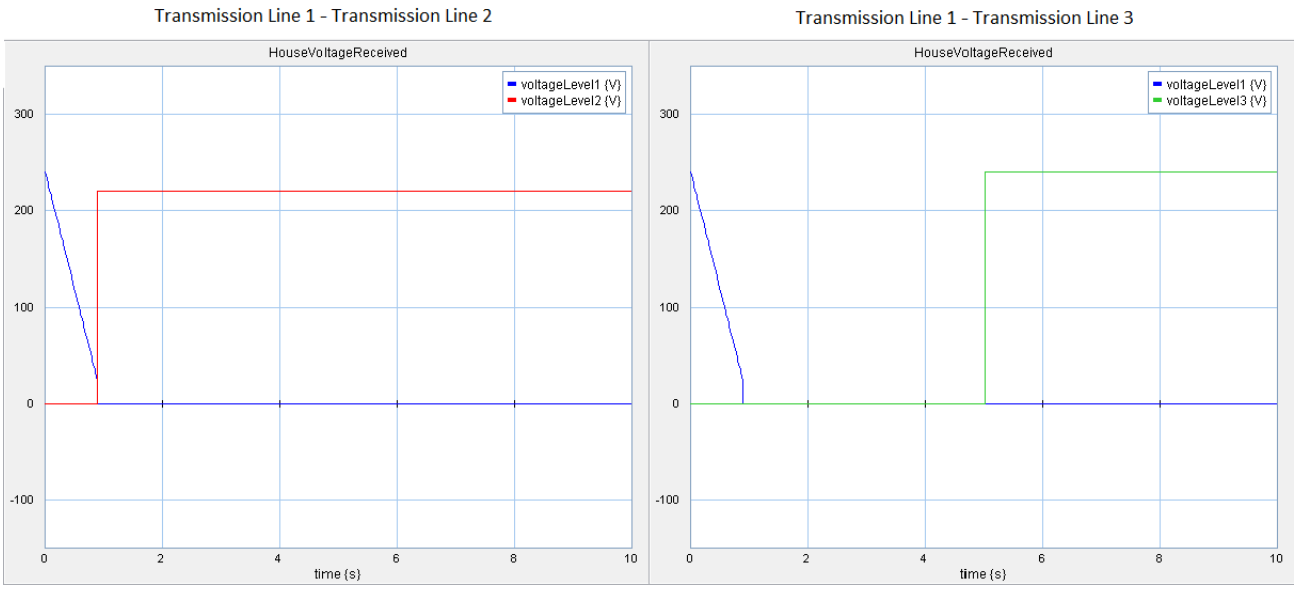

Fig. 10. A comparison of resilience scenarios.

An important note to make about our trade-off analysis example as seen in Figure 11, resides in the fact that our Rate of Recovery facet (blue) is compromised of our voltage level and time. The Rate of Recovery facet will always rely on the relation and importance of the y-axis and the x-axis on our graph. We calculated the (average) Rate of Recovery in Figure 11 for scenario 2 as 60V/s, however we can see from the graph that there is no voltage supplied at all until 5 seconds. This is due to the discrete nature of switching transmission lines in our model. This information may be of interest to a CPS design engineer. For other resilience scenarios, the engineer may wish to have some values of performance available leading up to the Actual Recovery Capacity, as opposed to our co-model example, in which the transmission line is either switched on or off. In this case we can analyse our recovery phase further at more time steps. It is for reasons like this that we seek to extend our resilience profile to a more refined

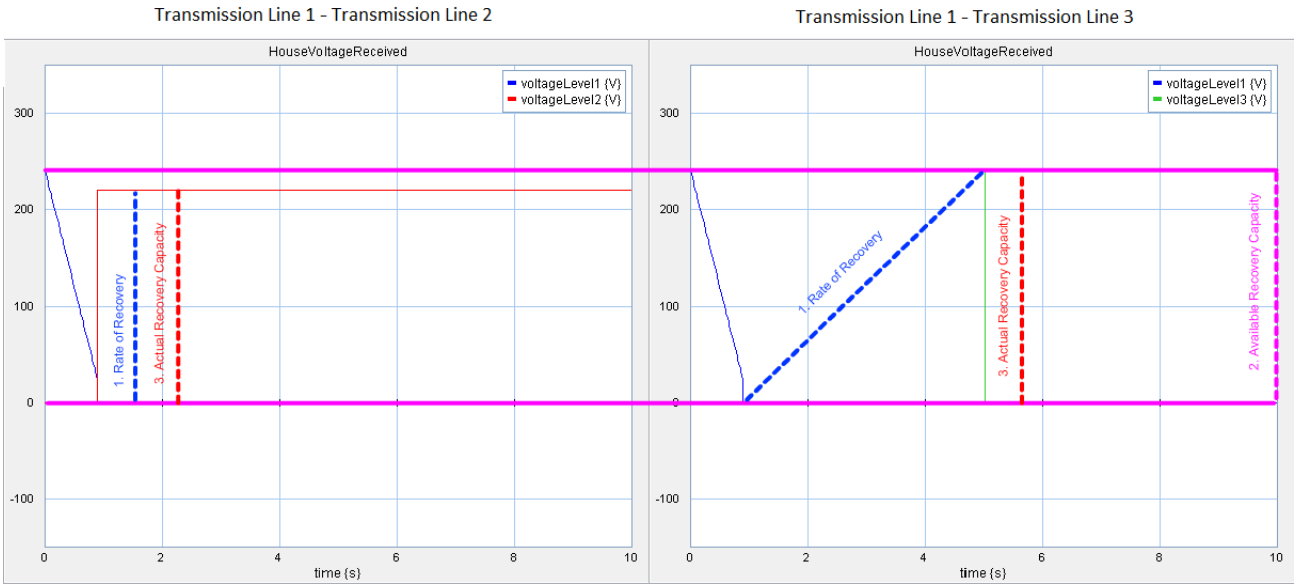

Fig. 11. An analysis of trade-off.

and sophisticated version. Although this is somewhat a trivial example, it describes the basis of our resilience profile and demonstrates how we can perform trade-off analysis between attributes and facets.

5 Evaluation and Further Work

We have provided motivation for being interested in resilience as a property of cyber-physical systems. Recognising that it is a multi-faceted property, we have extended an existing resilience profile with additional features that characterise recovery phases, and demonstrated that it is possible to assess this aspect of resilience on CPS co-models using Crescendo by means of a simple example from the domain of smart grids. We have illustrated resilience scenarios that cross the cyber-physical boundary and have demonstrated the potential to assess trade-offs.

Our work is at a preliminary stage, but we believe that there is potential to build useful methods for CPS resilience engineering on top of co-modelling technology of the kind pioneered by Overture, 20-sim, Crescendo and INTO-CPS. We naturally expect to progress from the Crescendo framework to INTO-CPS, exploiting the nascent SysML architectural modelling methods developed in that context as well as the improving performance of tools. We hope to take advantage of order of magnitude improvements in co-simulation and design space exploration performance that will allow us to evaluate our resilience profile on system architectures that reflect the potential complexity of emerging CPSs. These will include decentralisation of control, and eventually increased localised responsibility and autonomy in smart grids. Modular architectures such as

microgrids (in which local smart grids negotiate with one another to trade energy) may serve to improve or impede facets of resilience, for example. We will assess the extent to which the abstractions currently available in VDM-RT help or hinder the modelling of such structures.

As discussed at the end of Section 4, we seek to extend our profile in order to better encapsulate the interesting design decisions that a CPS design engineer may face when considering the resilience of a system. In the future we look towards generating data using the INTO-CPS tool chain described in Section 1. This would allow us to profile the resilience of models of CPSs that have been generated with different semantics across a variety of simulation tools.

Finally, we note that there are – at least at a certain abstraction level – significant similarities between CPSs in different infrastructure domains. We might expect that some modelling patterns might be shared between, say, negotiating microgrids, and negotiating traffic flow systems. There is therefore significant potential in identifying and exploiting those patterns as a means of sharing experience between otherwise quite separate application domains.

As societal and business dependence on cyber-physical systems grows, we believe that the need to take a systematic view of resilience – and in particular recovery – will only grow. Through their support for varied levels of abstraction, and their capacity to integrate with hitherto isolated tools, Overture and VDM have a vital role to play in addressing this requirement in the future.

References

1. S. McChrystal, T. Collins, D. Silverman, and C. Fussell, *Team of Teams: New Rules of Engagement for a Complex World*. Portfolio Penguin, October 2015.
2. E. A. Lee, "CPS foundations," in *Proceedings of the 47th Design Automation Conference*, DAC '10, (New York, NY, USA), pp. 737–742, ACM, 2010.
3. M. Broy, "Engineering cyber-physical systems: Challenges and foundations," pp. 1–13, 2013.
4. S. Karnouskos, "Cyber-physical systems in the smartgrid," in *Industrial Informatics (INDIN), 2011 9th IEEE International Conference on*, pp. 20–23, July 2011.
5. J. Taneja, R. Katz, and D. Culler, "Defining cps challenges in a sustainable electricity grid," in *Cyber-Physical Systems (ICCPS), 2012 IEEE/ACM Third International Conference on*, pp. 119–128, April 2012.
6. "Summary of the 2015-16 sector resilience plans." United Kingdom Cabinet Office, April 2016.
7. 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.
8. "Keeping the country running; natural hazards and infrastructure." United Kingdom Cabinet Office, October 2011.
9. Q. Zhu and T. Basar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, pp. 4066–4071, Dec 2011.
10. M. Broy, "Engineering cyber-physical systems: Challenges and foundations," pp. 1–13, 2013.

11. L. Zhang, "Modeling large scale complex cyber physical control systems based on system of systems engineering approach," in *Automation and Computing (ICAC), 2014 20th International Conference on*, pp. 55–60, Sept 2014.
12. A. Hellinger and S. Heinrich, "Cyber-physical systems driving force for innovation in mobility, health , energy and production," tech. rep., acatech - National Academy of Science and Engineering, 2011.
13. C. Brooks, C. P. Cheng, T. H. Feng, E. A. Lee, and R. Von Hanxleden, "Model engineering using multimodeling," tech. rep., DTIC Document, 2008.
14. R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine, "The algorithmic analysis of hybrid systems," *Theoretical computer science*, vol. 138, no. 1, pp. 3–34, 1995.
15. P. G. Larsen, J. Fitzgerald, J. Woodcock, P. Fritzson, J. Brauer, C. Kleijn, T. Lecomte, M. Pfeil, O. Green, S. Basagiannis, and A. Sadovykh, "Integrated tool chain for model-based design of cyber-physical systems: The into-cps project," in *2016 2nd International Workshop on Modelling, Analysis, and Control of Complex CPS (CPS Data)*, pp. 1–6, April 2016.
16. P. G. Larsen, J. Fitzgerald, J. Woodcock, R. Nilsson, C. Gamble, and S. Foster, "Towards semantically integrated models and tools for cyber-physical systems design," in *Proc. 7TH Intl. Conf. on Leveraging Applications of Formal Methods, Verlification and Validation (ISoLA 2016)*, Springer, in press, 2016.
17. E. Hollnagel, D. D. Woods, and N. Leveson, *Resilience engineering: Concepts and precepts*. Ashgate Publishing, Ltd., 2007.
18. E. Hollnagel, J. Paries, D. W. David, and J. Wreathall, *Resilience engineering in practice: A guidebook*. Ashgate Publishing, 2010.
19. S. M. Mitchell, *Resilient engineered systems: the development of an inherent system property*. PhD thesis, Texas A&M University, 2007.
20. C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient control systems: next generation design research," in *Human System Interactions, 2009. HSI'09. 2nd Conference on*, pp. 632–636, IEEE, 2009.
21. L. Mili and N. V. Center, "Taxonomy of the characteristics of power system operating states," in *Taxonomy of the characteristics of power system operating states*, 2011.
22. S. Carpenter, B. Walker, J. Anderies, and N. Abel, "From metaphor to measurement: Resilience of what to what?," *Ecosystems*, vol. 4, no. 8, pp. 765–781, 2001.
23. C. of the European Communities, "Disaster resilience: Safeguarding and securing society, including adapting to climate change."
24. S. Jackson, *Architecting resilient systems: Accident avoidance and survival and recovery from disruptions*, vol. 66. John Wiley & Sons, 2009.
25. M. Pflanz, *On the Resilience of Command and Control Architectures*. PhD thesis, George Mason University, 2011.
26. O. Yagan, D. Qian, J. Zhang, and D. Cochran, "Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 9, pp. 1708–1720, 2012.
27. P. Smith and A. Schaeffer-Filho, "Management patterns for smart grid resilience," in *Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on*, pp. 415–416, IEEE, 2014.
28. J. Fitzgerald, K. Pierce, B. Bos, and C. Gamble, "Co-modelling of faults and fault tolerance mechanisms," in *Collaborative Design for Embedded Systems*, ch. 9, pp. 185–198, Springer, 2014.