ISSN 2186-7437

NII Shonan Meeting Report

No. 118

Modelling and Analysing Resilient Cyber-Physical Systems

Amel Bennaceur
Carlo Ghezzi
Kenji Tei

December 17–20, 2018

National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-Ku, Tokyo, Japan

Modelling and Analysing Resilient Cyber-Physical Systems

Organizers:
Amel Bennaceur (The Open University, UK)
Carlo Ghezzi (Politecnico di Milano , Italy)
Kenji Tei (National Institute of Informatics, Japan)

December 17–20, 2018

From smart buildings to medical devices to smart nations, software systems increasingly integrate computation, networking, and interaction with the physical environment. These systems are known as Cyber-Physical Systems (CPS). While these systems open new opportunities to deliver improved quality of life for people and reinvigorate computing, their engineering is a difficult problem given the level of heterogeneity and dynamism they exhibit. While progress has been made, we argue that complexity is now at a level such that existing approaches need a major re-think to define principles and associated techniques for CPS. This seminar aims to reflect on both the theory/formal foundations of resilient CPS and their engineering/implementation. It focuses on identifying research challenges when modelling, analysing and engineering CPS. We focus on three key topics: theoretical foundations of CPS, self-adaptation methods for CPS, and exemplars of CPS serving as a research vehicle shared by a larger community.

This report presents an overview of the talks given at the seminar and summaries of the discussions of the participants.

Overview of Talks

Fundamentals of the Composition of components of CPS

Wolfgang Reisig, Humboldt University Berlin, Germany

This talk focuses in the concept of composition and associativity as desirable property for CPS.

Software foundations for data interoperability in CPS/IoT

Zhenjiang Hu, National Institute of Informatics, Japan

In this talk, Prof. Zhenjiang Hu introduced a new software architecture called Dejima for systematic development of CPS systems where data protection, data sharing, data integration, and data updates can be done in a robust manner. In addition, Prof. Zhenjiang Hu showed that datalog can be used to develop well-behaved bidirectional transformation, the key component in Dejima. In a distributed system, performance properties may determine the architecture to implement, how is this taken into account? As it is a distributed system, the notion of consistency can be defined differently, e.g., the value will be eventually the same? How about when data is not static, e.g., data stream? The view is defined by the context, how is this considered?

Cyberphysical Systems, Laboratories and Industrial IoT

Heinz W. Schmidt, RMIT Australia, Australia

This talk focuses on the design of exemplars and virtual laboratories for CPS. It presents the work done by The Royal Melbourne Institute of Technology (RMIT-Australia) to create a hub for experimenting and demonstrating research in robotic manufacturing, networked control systems, global cloud-enabled automation services.

Resource Matchmaking at Runtime for the Edge-Intensive Internet-of-Things

Christos Tsigkanos, TU Wien, Austria

Internet-enabled things and devices operating in the physical world are increasingly integrated in modern distributed systems; we focus here on spatially-distributed Internet-of-Things systems such as smart environments, where the dynamics of spatial distribution of entities in the system is crucial to requirements satisfaction. Analysis techniques need to be in place while systems operate to ensure that requirements are fulfilled. However, computationally-intensive runtime assurance cannot be supported by resource-constrained devices that populate the space and must be offloaded to the cloud, where challenges arise regarding resource allocation and cost, especially when the workload is unknown at the system's design time. As such, it may be difficult or even impossible to guarantee application service level agreements. To this end, we instantiate

spatial verification processes, integrating them to the service layer of an IoT-cloud architecture based on microservices. We propose several cloud deployments for such an architecture for assurance of spatial requirements and assess their tradeoffs in terms of elasticity, performance and cost by using a workload scenario from a known dataset of taxis roaming in Beijing.

Decentralising the control of distributed cyber-physical systems

Radu Calinescu, University of York, UK

Most CPS are distributed systems that operate in environments characterised by uncertainty, and must continually self-adapt to cope with changes in system goals, workload or available resources. Due to the large size, distributed nature, frequent changes and communication constraints of these CPS, it is often infeasible to maintain accurate global models of entire CPS or to analyse such models efficiently in order to enable timely self-adaptation decisions to be made. When this is the case, the software controllers responsible for these self-adaptation decisions need to be decentralised. This requires individual CPS components to operate autonomously (managed by local controllers) for periods of time, with only infrequent synchronisation for the partition or repartition of the CPS goals and resources.

Designing Resilient Large Scaled CPS: Models, Languages and Tools

Michele Loreti, University of Camerino, Italy

This talk presents a set of formal models and tools for specifying and verifying qualitative and quantitative properties of concurrent and distributed systems with an emphasis on large scaled Cyber Physical Systems.

Synergy between adaptive control methods and MART for CPS

Hausi A Muller, University of Victoria, Canada

This talk focuses on the use of Models at Runtime (MART) to drive the adaptation of CPS.

Applying adaptation to automate the management of IoT

Danny Weyns, Katholieke Universiteit Leuven, Belgium

This talk presents and architecture-based adaptation approach to solve a concrete practical problem of automating the management of Internet-of-Things (IoT). The application comprises a set of IoT devices that communicate sensor data over a time synchronised smart mess network to a central monitoring facility.

Specification and Monitoring of spatio-temporal properties

Laura Nenzi, University of Trieste, Italy

Cyber-Physical Systems (CPSs) consist of collaborative, networked and tightly intertwined computational (logical) and physical components, each operating at different spatial and temporal scales. Hence, spatial along with the temporal requirements play an essential role for their correct and safe execution. However, the local interactions among the system components result in global spatio-temporal emergent behaviours often impossible to predict at the design time. In this talk, we present a number of spatio-temporal logics to describe interesting behaviours of CPS with a spatio-temporal dynamics. We show how to specify and verify such properties in a number of case studies and we discuss the current challenges using them.

Forensic Readiness in Cyber-Physical Systems

Liliana Pasquale, University College Dublin/Lero, Ireland

Cyber-physical systems (CPSs) are part of most critical infrastructures such as industrial automation and transportation systems. Thus, security incidents targeting CPSs can have disruptive consequences to assets and people. As prior incidents tend to re-occur, sharing knowledge about these incidents can help organisations being more prepared to prevent, mitigate or investigate future incidents. This paper proposes an approach to enable representation and sharing of knowledge about CPS incidents across different organisations. To support sharing, we represent incident knowledge (incident patterns) capturing incident characteristics that can manifest again, such as incident activities or vulnerabilities exploited by offenders. Incident patterns are a more abstract representation of specific incident instances and, thus, are general enough to be applicable to various systems - different than the one in which the incident occurred. They can also avoid disclosing potentially sensitive information about an organisation's assets and resources. We provide an automated technique to extract an incident pattern from a specific incident instance. To understand how an incident pattern can manifest again in other cyber-physical systems, we also provide an automated technique to instantiate incident patterns to specific systems.

Cyber-Physical-Human Systems

Schahram Dustdar, TU Wien, Austria

This talk addresses the core technologies and technological enablers for managing the human and social components of CPS.

Breakout Groups

1 Group 1: Foundation

1.1 Motivation

Resilient CPS involve rethinking design and engineering with a major focus on composition and dynamic environments. One possible way to capture those aspects is considering *ecosystems* that compose software platforms as well as communities of users [11].

The rigorous analysis of CPS requires models that represent heterogeneous aspects of CPS across different layers of the technology stack—from the physical, sensor and actuator layer, to communication and middleware, up to application layer. Models may be required across tiers of the CPS, to represent heterogeneous types of software, from user applications to supporting services and back-end storage. These are inherently multi-faceted and typically belong to different disciplines (e.g., physical, communication, software, social). An important challenge is then how to align the abstractions of these heterogeneous models into a unified representation that allows for reasoning and supporting adaptation decisions.

While rigorously representing CPS is difficult, their composition, analysis, and adaptive control are even more challenging [32]. In particular adaptive control of CPS is challenging due to their inherent hybrid nature. On the one hand, discrete-time control focuses on functional requirements, deals with composition but require complete knowledge of the environment. On the other hand, continuous-time control focuses on quantitative requirements, adapt to perturbations in the environment but does not support composition and concurrency. Defining appropriate *assurance* properties and methods for CPS is essential.

Given the diversity of techniques and methods that are foundational for modelling and analysing CPS, curricula that prepare and train a skilled workforce should reflect this diversity and multidisciplinarity.

1.2 Ecosystems

The choice of the environment depends on the scale of the system at hand: how a CPS is defined depends on the scope and the context. Figure 1 gives an example on how we can model an automotive system at four different levels of granularity. For each level of granularity, the notion of environment is defined with respect to the chosen system. For example, while modelling the engine, the environment is made up of the other components of the car. When modelling a car, then other cars compose the environment. When designing a platoon, then the transport infrastructure can represent the environment. Finally, when considering a smart city as a CPS, then the environment may include other cities.

The scope and goals of those ecosystems need to be well understood in order for the impact of collaboration and interconnection to be specified rather than just incurred. Understanding, yet alone controlling, emergent collaborations between communities of users and CPS, and the theory and processes for understanding them are still to be defined.

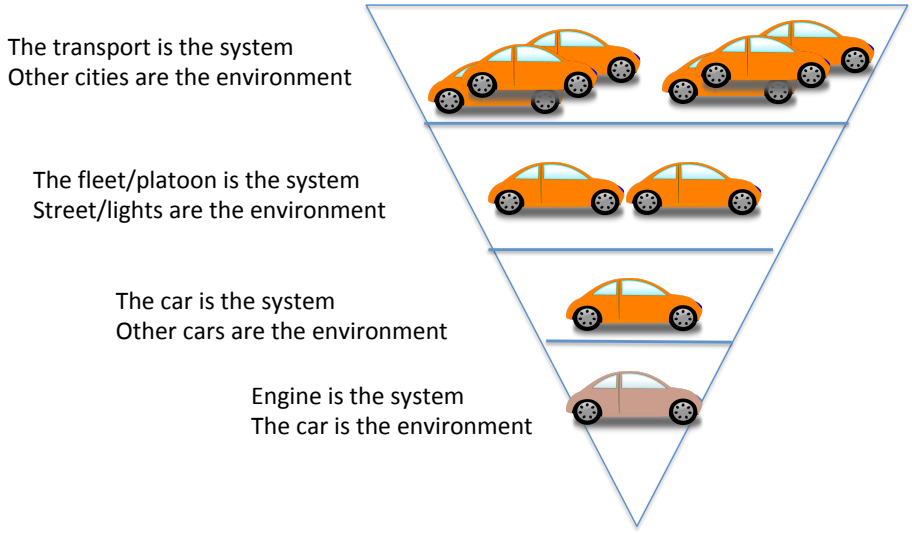

Figure 1: Illustrating CPS ecosystems on transport

1.3 Assurance

Resilience has been defined as the persistence of dependability while facing change [23], and often understood as the ability of the system to return to a viable zone/stability [5] while avoiding Zeno behaviour, i.e. the system undergoing an unbounded number of discrete transitions in a finite and bounded length of time. The classic notion of satisfaction is insufficient to describe properties of such behaviour. Therefore, we consider the notion of *equilibrium* as a new form of satisfaction. The idea is that the system maintains a behaviour within its multidimensional viability zone rather than satisfy a property in the case of perturbations. Moreover, the system actively monitors whether it is in its normal viability zone and is able to bring it back within if it ventures outside. After returning or healing, the system can potentially be stronger and so even the bounds can change leading to contextual viability zones [16]. Different definitions of this notion can lead to different interpretations and requirements.

For self-adaptive CPS, assurances must also consist of *comprehensive evidence* (obtained through modelling and simulation, testing, formal verification, compliance with established practices, etc.) that the CPS can safely achieve the goals of their intended application in the physical environment in which they operate. Given the heterogeneity and distributed nature of many CPS and the complexity of their goals, devising this comprehensive body of evidence represents a major challenge that is not fully addressed by existing approaches.

A further challenge in the provision of assurances for CPS self-adaptation is the need to *integrate assurance evidence* from all stages of the CPS lifecycle. Assurance cases for CPS must combine development-time evidence from the CPS design, implementation and verification with runtime evidence that they continue to safely achieve their goals during self-adaptation. Dynamic safety cases have been used to tackle this challenge for self-adaptive software [13], but extending their applicability to CPS requires significant additional research due to the physical aspects of these systems and of their goals.

Modelling and reasoning about spatio-temporal properties is also important. *Cyber-physical spaces* [34] are composite models integrating human agents, computational and physical aspects of systems. Formal languages such as spatio-temporal logics [6,20] can be used to describe, verify, and test complex properties where the spatial and temporal part are intrinsically connected and influence each other. Furthermore, they provide efficient monitoring procedures to verify the property and they deal with changes in spatial configuration.

1.4 Education

The multifaceted nature of designing and engineering CPS raises multiple questions on how to educate students with those foundational concepts in CPS in order to create and maintain a skilled workforce to support the design, engineering, deployment, and operation of future CPS. CPS engineers, scientists and developers not only need strong backgrounds in CPS foundations, but also significant knowledge in relevant application domains. The cross-cutting and rapidly evolving application of sensing, actuation, control, communication and computing presents significant challenges for industry, academia and governments. Existing engineering and computer science programs are challenged in teaching the comprehensive skill set required for a successful career in the CPS realm [27]. The software engineering community has made tremendous strides in designing and operating highly dynamical software systems by developing methods and techniques to deal with CPS uncertainty and resilience at runtime as well as standardise and distribute CPS components and services effectively. It is high time to inject these innovations into computing and software curricula which still largely concentrate on design-time aspects of, for example, requirements, models and V&V (Verification and Validation). Digital control, which integrates discrete and continuous mathematics, is central to CPS. On the one hand, computer science and software engineering programs need digital control courses; on the other hand, traditional engineering programs need to include software engineering courses. Designing CPS contents involves a careful balancing of physical and cyber aspects as well as CPS application knowledge [33]. While adding CPS courses, options or degree programs is extremely challenging due to the many competing forces, trained CPS students are needed in industry to harvest CPS rich economic opportunities.

2 Group 2: Engineering Self-Adaptation for Resilient CPS

2.1 Motivation

CPS must handle high levels of dynamicity and uncertainty. This is due to factors that include workload variation, interactions with human users and operators, regular goal changes, and components joining and leaving the CPS. As such, the software controlling the CPS operation must manage its dynamicity and uncertainty, using self-adaptation to ensure that the system behaviour stays within the bounds defined by its goals. For CPS used in safety-critical applications, these goals often specify strict safety, dependability and performance requirements. Accordingly, the CPS control software must also provide assurances guaranteeing

the system compliance with these requirements. While the features we mentioned so far are common to most types of self-adaptive systems, several distinguishing characteristics of CPS further increase the challenges associated with the engineering of their control software. First, the heterogeneity of the CPS components and of their sensors and actuators (vertically across the technology stack, and horizontally across different components and subsystems) greatly increases the complexity of the control software. Second, the distributed deployment of most CPS, often with only unreliable, high-latency or low-bandwidth communication affordable between components, precludes the maintenance of up-to-date global system models. Third, even when such global models can be assembled and kept up to date, they are typically too large to be analysed efficiently and to support timely reasoning about the CPS. Fourth, many CPS are assembled through the integration of components owned by different organisations. Last but not least, the constraints and optimisation criteria specified by CPS goals refer not only to computational aspects such as throughput and task ordering, but also to physical aspects of the system components.

This unique combination of characteristics is responsible for multiple open challenges in developing self-adaptation methods and software for resilient CPS. In the remainder of this section, we summarise four of these open challenges that we expect to drive future research in this area.

2.2 Control software decentralisation

For the numerous CPS for which system-level modelling and analysis are unfeasible, or the system components are owned by multiple organisations, the control software needs to be decentralised. Examples of such CPS include many Internet of Things (IoT) systems, unmanned-vehicle CPS, and smart e-health CPS. For instance, to support multiple tenants and increase the scale of the IoT system presented in [39], the control software necessarily needs to be decentralised to enable local decision-making while keeping the energy consumption of battery-powered modes within bounds. As another example, consider the CPS of unmanned underwater vehicles from [12], the driving factors for decentralising the control software are the efficiency of modelling and analysis, and ensuring the mission goals regardless of the inherent restrictions of communication under water. Finally, in a smart e-health CPS as the one presented in [25], different parts of the systems have different owners that may be unable to share all information (e.g., for security or privacy reasons); hence, autonomy of subsystems and decentralising the control software is imperative.

In summary, decentralising self-adaptation enables dealing with multiple owners and autonomy of CPS components, and inherent distribution and restrictions of resources. However, successfully decentralising the CPS control software is neither a panacea nor without its costs. We highlight four implications or potential drawbacks, together with their associated challenges and starting points for addressing them.

As CPS are often long-living systems that organically grow, decentralisation of control software can serve as an enabler to support robust and scalable system evolution. However, this raises the challenge of suitable coordination capabilities for entities to join and leave the CPS ecosystem. Agent coordination and protocols [21] could be a starting point for tackling this challenge.

Decentralisation of the CPS control software requires adaptation decisions

to be made based on locally available information that are not necessarily altruistic. Consequently, the decisions may be sub-optimal compared to global decision-making. The challenges are then how to measure and quantify the cost of decentralising the control software in terms of loss of decision-making optimality. This cost may then be traded against the degree of decentralisation, e.g., by structuring decision-making for adaptation hierarchically. One source of inspiration to study these challenges is "Price of anarchy" [30], which is a concept from economics and game theory that allows measuring how a system's efficiency degrades as a result of distributed competitive decision making.

Decentralisation of control software may raise trust issues as well. In a decentralised setting, the subsystems of a CPS may be unwilling or unable to share all the information needed for local decisions, e.g., on how to perform reconfigurations. A challenge is then how to ensure sufficient trust in the system and how to ensure that no undesired effects emerge from local decisions? Interesting approaches to start tackling this challenge are computational mechanism design and game theory [15].

An important aspect of CPS is incident handling, e.g., due to security or privacy events. An important challenge is then to understand the impact of decentralisation of control software on incident handling. This impact can be considered from two perspectives: on the one hand, detecting incidents may be more difficult due to locality of activities; on the other hand, the effects may be localised, reducing the harm caused by incidents.

2.3 Adaptive Security for CPS

As CPS span cyber and physical spaces, they are more vulnerable than conventional software systems to attacks [28]. Malicious actors can exploit cyber accessibility to a digital network to gain access to the physical devices connected to the network (e.g., German Still Mill Attack [24]). Malicious actors can also exploit vulnerabilities of physical devices to control them remotely and orchestrate attacks against third party systems and services (e.g., Mirai Attack [9]).

So far security risks arising from the cyber and physical spaces have been assessed separately [36], leading to gaps and vulnerabilities for parts of the system. Thus, traditional risk assessment methods (e.g., CORAS [17]) need to be revised and should consider the extended attack surface brought by the interplay between cyber and physical components in CPS.

Unpredictability, heterogeneity, and scale make it difficult to anticipate how security threats can materialise and what security countermeasures to apply to prevent them. To protect todays CPS, designing static and rigid security solutions is no longer sufficient. CPS should be designed with the capability to self-protect [8, 41], especially when security threats may arise from different spaces.

Existing approaches proposed to develop self-protecting software systems (e.g., [35]) usually can only react to a set of changes (in the system or its operating environment) that are known at design time by enacting a set of pre-defined countermeasures. This would still leave the sub-system to be protected exposed, for example, to attacks targeting new assets or exploiting vulnerabilities brought by changes in the topology (structure and connectivity) of cyber and physical components. Thus it is necessary to develop novel threat analysis and planning techniques to reason about changing security threats and selecting a set of coun-

termeasures that could guarantee assets protection. These techniques should scale by adaptively focusing on the aspects of the CPS that require protection.

2.4 Models at runtime

The self-adaptation methods used by CPS must efficiently and coherently leverage multiple types of models at runtime. Models used for self-adaptation often capture uncertainties (e.g., in terms of probabilities of properties in the environment), or the models themselves may have uncertainty (e.g., due to sensor noise). Given the heterogeneity of CPS, a challenge is then how to ensure that the runtime models are sufficiently accurate to make timely adaptation decisions. Rephrased from a models@runtime perspective, the question raised by this challenge is: what does causal connection[1] mean for runtime models of CPS, and how can this causality be realised?

As CPS are often large-scale systems and the control software for self-adaptation is decentralised, an important challenge is to decide what information is collected where, what and how is this information shared, and how to ensure that the distributed models used to support decision making for self-adaptation are consistent across the CPS components.

2.5 Human stakeholders

The self-adaptation methods employed by CPS must provide *relevant and comprehensible information to stakeholders* ranging from users and operators to regulators and the general public [18]. This includes information about the rationale underpinning self-adaptation decisions (e.g., to gain the trust of users, and to enable CPS certification by regulators), and information supporting users and operators in their regular interactions with the system.The adoption and success of many envisaged CPS depend on this challenge being addressed by the research community.

Numerous CPS used in smart cities, e-health, smart transportation and similar applications are complex socio-technical systems. Humans who interact with these CPS are not merely providers of system input and consumers of artefacts produced by the system. They are first-class *participants in the CPS*, whom the system relies upon for contributions to decision making, to the execution of these decisions, etc. This means that the self-adaptation methods employed by these CPS must consider human participants in all their steps—from the monitoring and analysis of the system and its environment, to the synthesis of adaptation plans and the execution of these plans. While preliminary work and thoughts on self-adaptive systems with "humans in the loop" (e.g., [14, 38]) provide a starting point for tackling this challenge, further research is needed to apply these concepts to CPS with human participants.

Research has emphasised the need for social adaptation, where the software system analyses users' feedback and updates its behaviour to best satisfy the requirements in the given context [4]. In fact with the prevalence of mobile and

[1] Recall that a causal connection refers to the link between the managed system and the model representing it such that whenever a change is made to the model, this change is reified in the system and whenever the system changes, this change is reflected in the corresponding model

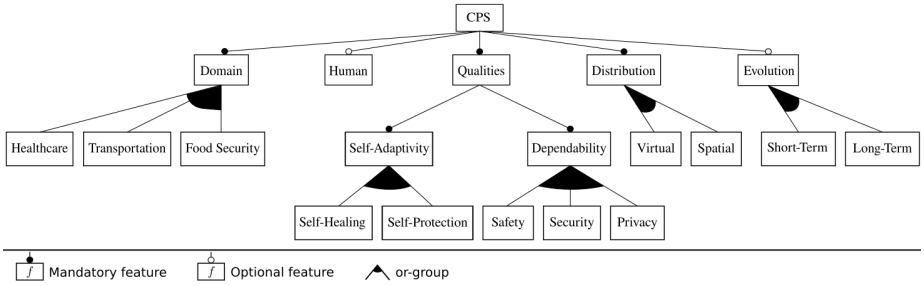

Figure 2: Excerpt of an early version of our feature-based classification scheme for characterising the general kind of CPS represented by an exemplar.

ubiquitous technology, it is becoming easier to have a better understanding of user preferences, and one can aim to compose both digital and social services [29].

3 Group 3: Exemplars

3.1 Motivation

Good (software) engineering research not only requires methodological, technical and theoretical results, but also convincing evidence that these results are sound [31]. Exemplars are well-suited for validation, studying relevant problems, and as a medium for education. Exemplars have been collected and established in various areas of engineering software-intensive systems, e.g., in requirements engineering [19], software and system evolution [37], software product-line engineering [26], and self-adaptive and self-managing systems [3]. However, to the best of our knowledge there is no structured catalogue or repository of exemplars specifically addressing CPS.

Therefore, our goal is to provide comprehensive information about CPS exemplars that would be otherwise scattered in the literature or restricted to local usage in dedicated laboratories, such as the *Cyber-Physical Systems Laboratory* at the HPI [2] or the *Virtual Experiences Laboratory (VXLab)* at the Royal Melbourne Institute of Technology [1, 10]. The primary target group comprises researchers and educators who can use the collection as a source of information to find the exemplars which fit to their individual needs. We focus on a common classification scheme for characterising the exemplars and a technical infrastructure for collecting these exemplars.

3.2 Classification Scheme

As mentioned above, collections of exemplars have been established by several research communities. The SEAMS community maintains a catalogue of exemplars for self-adaptive systems, ranging from generic artefacts to specific model problems [3]. Some of these exemplars are specifically addressing CPS and represent a good starting point for our classification scheme. Yet, our goal is to address CPS from a broader perspective, including further qualities besides self-adaptation and -management.

Moreover, exemplars in the SEAMS catalogue are mainly described in an unstructured way using natural language. While this has the advantage that

providing new exemplars is easy, searching for an exemplar offering specific characteristics can be difficult and tedious. Therefore, we propose a more detailed classification scheme that enables structured descriptions of CPS exemplars amenable to (semi-)automated search. This scheme should allow one to a) characterise the general kind of CPS represented by an exemplar as well as b) characterise a specific exemplar itself.

Characterising the kind of CPS represented by an exemplar To characterise the general kind of CPS represented by an exemplar, we rely on techniques that are primarily known from the field of software product-line engineering, particularly the use of feature models [22]. These have proven well-suited for structuring a domain of interest. The idea is that the features including their inter-relations formally capture the variation points of the set of conceivable exemplars, while the kind of system represented by a specific exemplar is precisely characterised by a valid configuration of the feature model. Besides formally documenting the main variation points of a CPS, such a feature model also provides a common yet high-level terminology for CPS, which is of increasing importance given its interdisciplinary nature. Our aim is not to come up with an exhaustive taxonomy or ontology, but with a feature model which is generic enough to classify any kind of CPS of interest and specifically tailored for our purpose of describing exemplars. An excerpt of an early version of our feature model is shown in Figure 2.

A first variation point to do a high-level characterisation is the *Domain* in which a CPS is intended to operate. Some typical domains are *Healthcare*, *Transportation* or *Food Security*. Another high-level yet distinguishing feature is whether a CPS emphasises the role of the *Human* interacting with the system or not.

In addition, there are a number of cross-cutting features which, regardless of the particular domain and regardless of whether the CPS emphasises human interaction, are interesting for validating a broad range of generic methods as:

Qualities. Since we are specifically addressing the analysis of CPS, one important variation point pertains the *Qualities* which we expect to be exposed by a particular kind of CPS. Qualities of interest include *Dependability* properties such as *Safety*, *Security* and *Privacy*. *Self-Adaptivity* leads to improvements in dependability. Specifically, considering our example dependability properties, *Self-Healing* and *Self-Protection* refer to the automatic detection of failures and attacks as well as their subsequent correction and suppression, respectively.

Distribution. CPS are highly distributed systems by definition. However, we may distinguish whether *Distribution* is only *Virtual* or also *Spatial*. The former reflects the classical notion of a distributed system where computational entities are distributed and connected over some network structure, while the latter applies to CPS which are designated to be operated in a larger spatial environment such as smart buildings or cities.

Evolution. Another aspect which is of particular interest for various analysis methods is *Evolution*, where we distinguish among *Short-Term* evolution and *Long-Term evolution*. Short-term evolution means that the system operates in a highly dynamic environment undergoing continuous changes, while long-term evolution stresses the fact that a system is intended to be operated for a long

period of time.

For example, let us consider two concrete CPS exemplars from the SEAMS catalogue: The Automated Traffic Routing Problem (ATRP) [40] and an IoT-based ecosystem to support nutrition called "Feed me, Feed me" (FmFm) [7]. According to our feature-based classification, both systems have a set of common and individual features. While stemming from different domains, namely *Transportation* and *Food Security*, both systems share a highly dynamic nature (*Short-Term*) and must deal with frequent changes and uncertainty (*Adaptivity*). Concerning further qualities, FmFm produces vast quantities of personal data which demands for robust protection mechanisms (*Security* and *Privacy*), while *Safety* is one of the primary concerns for ATRP. Moreover, ATRP clearly operates in a *Spatial* environment, while this dimension of distribution is of minor importance for FmFm. However, in contrast to ATRP, FmFm puts forward the shared control and partial automation between the software system and its users in the social dimension (*Human*).

Characterisation of a specific exemplar In addition to the characterisation of the kinds of systems represented by an exemplar, exemplars shall be further characterised by collecting meta-data that are specific to an exemplar instance.

Generic Meta-data include but are not limited to, e.g., literature references where the exemplar has been used, which kinds of artefacts are available for the exemplar, and, if available, a literature reference to where the exemplar has been originally published as well as further pointers where to find more detailed information about the exemplar.

In order to evaluate the scalability of a method, researchers might also be interested in the *Size* of an exemplar. For our classification scheme, we propose to use a purely qualitative classification into *Small-*, *Medium-* and *Large*-scaled exemplars.

Optionally, an exemplar may also be intended for serving a particular *Purpose*. Typical purposes are to drive and communicate individual research advances, to compare and contrast alternative approaches, to establish research agendas, and, ultimately, to lead to advances in practices of developing and operating certain kinds of CPSs. This characterisation can be useful since, as argued in [19], there are interferences between these different purposes of exemplars, and an exemplar suited to serve one purpose is not necessarily suited to serve another.

References

[1] *Virtual Experiences Laboratory (VXLab)* at the Royal Melbourne Institute of Technology. `http://rmit.edu.au/vxlab`. visited on 15 March 2019.

[2] *Cyber-Physiscal Systems Laboratory* at the Hasso Plattner Institute Potsdam. `https://www.hpi.uni-potsdam.de/giese/public/cpslab`, 2019.

[3] Software Engineering for Self-Adaptive Systems Exemplars. `https://www.hpi.uni-potsdam.de/giese/public/selfadapt/exemplars/`, 2019.

[4] M. Almaliki, F. Faniyi, R. Bahsoon, K. Phalp, and R. Ali. Requirements-driven social adaptation: Expert survey. In *Requirements Engineering:*

Foundation for Software Quality - 20th International Working Conference, REFSQ, pages 72–87, 2014.

[5] J.-P. Aubin, A. M. Bayen, and P. Saint-Pierre. *Viability Theory: New Directions*. Springer, 2011.

[6] E. Bartocci, L. Bortolussi, M. Loreti, and L. Nenzi. Monitoring mobile and spatially distributed cyber-physical systems. In *Proc. of MEMOCODE*, pages 146–155, 2017.

[7] A. Bennaceur, C. McCormick, J. García-Galán, C. Perera, A. Smith, A. Zisman, and B. Nuseibeh. Feed me, feed me: an exemplar for engineering adaptive software. In *Proc. of SEAMS*, pages 89–95, 2016.

[8] A. Bennaceur, T. T. Tun, A. K. Bandara, Y. Yu, and B. Nuseibeh. Feature-driven mediator synthesis: Supporting collaborative security in the internet of things. *TCPS*, 2(3):21:1–21:25, 2018.

[9] E. Bertino and N. Islam. Botnets and Internet of Things Security. *Computer*, (2):76–79, 2017.

[10] J. O. Blech, M. Spichkova, I. D. Peake, and H. W. Schmidt. Cyber-virtual systems - simulation, validation & visualization. In *Proc. of ENASE*, pages 218–225, 2014.

[11] J. Bosch. Speed, data, and ecosystems: The future of software engineering. *IEEE Software*, 33(1):82–88, 2016.

[12] R. Calinescu, S. Gerasimou, and A. Banks. Self-adaptive software with decentralised control loops. In A. Egyed and I. Schaefer, editors, *Fundamental Approaches to Software Engineering*, pages 235–251, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[13] R. Calinescu, D. Weyns, S. Gerasimou, M. U. Iftikhar, I. Habli, and T. Kelly. Engineering trustworthy self-adaptive software with dynamic assurance cases. *IEEE Trans. on Soft. Eng.*, 44(11), 2018.

[14] J. Cámara, G. A. Moreno, and D. Garlan. Reasoning about human participation in self-adaptive systems. In *Proceedings of the 10th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*, pages 146–156. IEEE Press, 2015.

[15] R. K. Dash, N. R. Jennings, and D. C. Parkes. Computational-mechanism design: a call to arms. *IEEE Intelligent Systems*, 18(6):40–47, Nov 2003.

[16] R. e. a. de Lemos. Software engineering for self-adaptive systems: Research challenges in the provision of assurances. In *Software Engineering for Self-Adaptive Systems III. Assurances*, pages 3–30. Springer, 2017.

[17] F. Den Braber, I. Hogganvik, M. S. Lund, K. Stølen, and F. Vraalsen. Model-Based Security Analysis in Seven StepsA Guided Tour to the CORAS Method. *BT Technology Journal*, 25(1):101–117, 2007.

[18] S. Dustdar. Towards building cyber-physical ecosystems of people, processes, and things. In *Proc. of the 1st International Conference on Complex Information Systems, COMPLEXIS*, page 11, 2016.

[19] M. S. Feather, S. Fickas, A. Finkelstein, and A. Van Lamsweerde. Requirements and specification exemplars. *Automated Software Engineering*, 4(4):419–438, 1997.

[20] P. Herrmann, J. O. Blech, F. Han, and H. W. Schmidt. A model-based toolchain to verify spatial behavior of cyber-physical systems. *Int. J. Web Service Res.*, 13(1):40–52, 2016.

[21] M. N. Huhns and L. M. Stephens. In G. Weiss, editor, *Multiagent Systems*, chapter Multiagent Systems and Societies of Agents, pages 79–120. MIT Press, Cambridge, MA, USA, 1999.

[22] K. C. Kang, S. G. Cohen, J. A. Hess, W. E. Novak, and A. S. Peterson. Feature-oriented domain analysis (foda) feasibility study. Technical report, Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, 1990.

[23] J.-C. Laprie. From dependability to resilience. In *Proc. of the 38th IEEE/IFIP Int. Conf. On Dependable Systems and Networks*, 2008.

[24] R. M. Lee, M. J. Assante, and T. Conway. German Steel Mill Cyber Attack. *Industrial Control Systems*, 30:62, 2014.

[25] N. Li, C. Tsigkanos, Z. Jin, S. Dustdar, Z. Hu, and C. Ghezzi. Poet: Privacy on the edge with bidirectional data transformations. In *International Conference on Pervasive Computing and Communications*. IEEE Press, 2019.

[26] J. Martinez, W. K. Assunção, and T. Ziadi. Espla: A catalog of extractive spl adoption case studies. In *21st International Systems and Software Product Line Conference*, pages 38–41. ACM, 2017.

[27] H. A. Müller. The rise of intelligent cyber-physical systems. *IEEE Computer*, 50(12):7–9, 2017.

[28] L. Pasquale, C. Ghezzi, C. Menghi, C. Tsigkanos, and B. Nuseibeh. Topology aware adaptive security. In *Proc. of SEAMS*, pages 43–48, 2014.

[29] W. Qian, X. Peng, J. Sun, Y. Yu, B. Nuseibeh, and W. Zhao. O2O service composition with social collaboration. In *Proc. of the 32nd IEEE/ACM International Conference on Automated Software Engineering, ASE*, pages 451–461, 2017.

[30] T. Roughgarden. Selfish routing and the price of anarchy. *MIT Press*, 2005.

[31] M. Shaw. What makes good research in software engineering? *International Journal on Software Tools for Technology Transfer*, 4(1):1–7, 2002.

[32] J. Sifakis. System design in the era of iot - meeting the autonomy challenge. In *Proc. of MeTRiD@ETAPS 2018*, pages 1–22, 2018.

[33] J. A. Stankovic, J. W. Sturges, and J. Eisenberg. A 21st century cyber-physical systems education. *IEEE Computer*, 50(12), 2017.

[34] C. Tsigkanos, T. Kehrer, and C. Ghezzi. Modeling and verification of evolving cyber-physical spaces. In *Proc. of ESEC/FSE*, pages 38–48, 2017.

[35] C. Tsigkanos, L. Pasquale, C. Ghezzi, and B. Nuseibeh. On the Interplay Between Cyber and Physical Spaces for Adaptive Security. *IEEE Transactions on Dependable and Secure Computing*, 15(3):466–480, 2018.

[36] A. van Cleeff, W. Pieters, R. Wieringa, and F. van Tiel. Integrated Assessment and Mitigation of Physical and Digital Security Threats: Case Studies on Virtualization. *Information security technical report*, 16(3-4):142–149, 2011.

[37] B. Vogel-Heuser, S. Feldmann, J. Folmer, J. Ladiges, A. Fay, S. Lity, M. Tichy, M. Kowal, I. Schaefer, C. Haubeck, et al. Selected challenges of software evolution for automated production systems. In *13th International Conference on Industrial Informatics*, pages 314–321. IEEE, 2015.

[38] D. Weyns, N. Bencomo, R. Calinescu, J. Camara, C. Ghezzi, V. Grassi, L. Grunske, P. Inverardi, J.-M. Jezequel, S. Malek, R. Mirandola, M. Mori, and G. Tamburrelli. Perpetual assurances for self-adaptive systems. In R. de Lemos, D. Garlan, C. Ghezzi, and H. Giese, editors, *Software Engineering for Self-Adaptive Systems III. Assurances*, pages 31–63. Springer, 2017.

[39] D. Weyns, M. U. Iftikhar, D. Hughes, and N. Matthys. Applying architecture-based adaptation to automate the management of internet-of-things. In *Proc. of the 12th European Conference on Software Architecture, ECSA*, pages 49–67, 2018.

[40] J. Wuttke, Y. Brun, A. Gorla, and J. Ramaswamy. Traffic routing for evaluating self-adaptation. In *Proc. of SEAMS*, pages 27–32, 2012.

[41] E. Yuan, N. Esfahani, and S. Malek. A Systematic Survey of Self-Protecting Software Systems. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 8(4):17, 2014.

List of Participants

- Dr. Liliana Pasquale, University College Dublin/Lero, Ireland
- Dr. Michele Loreti, University of Camerino, Italy
- Prof. Heinz Schmidt, RMIT Australia, Australia
- Dr. Timo Kehrer, Humboldt-University of Berlin, Germany
- Dr. Laura Nenzi, University of Trieste, Italy
- Dr. Gabriel Moreno, Software Engineering Institute/CMU, USA
- Prof. Jeffrey Kramer, Imperial College London, UK
- Prof. Fuyuki Ishikawa, National Institute of Informatics, Japan
- Prof. Hausi A. Muller, University of Victoria, Canada
- Mr. Paul Piho, University of Edinburgh, UK
- Dr. Haiyan Zhao, Peking University, China
- Dr. Christos Tsigkanos, Technical University of Vienna, Austria
- Prof. Zhi Jin, Peking University, China
- Prof. Bashar Nuseibeh, The Open University & Lero, UK
- Dr. Marin Litoiu, York University , Canada
- Prof. Schahram Dustdar, TU Wien, Austria
- Prof. Wolfgang Reisig, Humboldt University Berlin, Germany
- Dr. Radu Calinescu, University of York, UK
- Prof. Zhenjiang Hu, National Institute of Informatics, Japan
- Prof. Shinichi Honiden, Waseda University, Japan
- Prof. Danny Weyns, Katholieke Universiteit Leuven, Belgium

Meeting Schedule

Sunday

19-21:30	Welcome Reception

Monday

9-9:30	Welcome
9:30-10:30	Introductions (12*5min)
Break	
10:50-12	Introductions (12*5min)
Lunch	
14-15:30	**Foundations of CPS** (Chair: Jeff Kramer) · Fundamentals of the Composition of components of CPS – Wolfgang Reisig · Software foundations for data interoperability in CPS/IoT – Zhenjiang Hu · Discussion
Break	
16:00 – 17:30	**CPS and IoT** (Chair: Hausi A. Muller) · Cyberphysical Systems, Laboratories and Industrial IoT – Heinz W. Schmidt · Resource Matchmaking at Runtime for the Edge-Intensive Internet-of-Things – Christos · Discussion
Dinner	

Tuesday

9-10:20	**Designing and Engineering CPS** (Chair: Wolfgang Reisig) · Decentralising the control of distributed cyber-physical systems – Radu Calinescu · Designing Resilient Large Scaled CPS: Models, Languages and Tools – Michele Loreti · Discussion
Break	
10:40-12	**Adaptive methods for CPS** (Chair: Heinz Schmidt) · Synergy between adaptive control methods and MART for CPS – Hausi A Muller · Applying adaptation to automate the management of IoT – Danny Weyns · Discussion
Lunch	
14-15:30	**CPS properties** (Chair: Fuyuki Ishikawa) · Specification and Monitoring of spatio-temporal properties – Laura Nenzi · Forensic Readiness in Cyber-Physical Systems – Liliana Pasquale · Discussion
Break	
16:00 – 16:30	**CPS and Human Behaviour** (Chair: Carlo Ghezzi) · Cyber-Physical-Human Systems – Schahram Dustdar
16:30-17:30	Discussion and Group Forming
Dinner	

Wednesday

9-10	Group Breakout
Break	
10:30-11:15	Group Breakout
11:15-12	Intermediary group presentations and feedback
Lunch	
Excursion/Social Event	
Visiting Jomyoji temple with Japanese Tea ceremony (**Tour Description**)	

Thursday

9-10:00	Group Breakout
Break	
10:30-12	Final group presentations Discussion and action plan
Lunch	