Cyber-physical Systems of Systems – Definition and core research and innovation areas

Working Paper of the Support Action CPSoS
Main author: Sebastian Engell

Version October 26, 2014

Preface

This preliminary document is an evolution of the scope document that was distributed before and discussed at the 1st joint meeting of the three CPSoS Working Groups (WG) in Düsseldorf on Jan. 31, 2014. It contains elements that were put forward by the WG members in the meeting , results of interviews with experts in the application fields, and some clarifications on issues that were discussed during the CPSoS 1st WG meeting.

The document will be circulated to the WG members and discussed at the set of 2nd WG meetings/public workshops in September 2014. A prioritization of the research and innovation areas, which is still missing in the current document, will be done within the next months by the CPSoS consortium based on further consultations and the results of the next WG meetings.

1. Definitions: Systems of systems, cyber-physical systems, and cyber-physical systems of systems

Systems of systems (SoS) is a relatively new concept from the domain of systems engineering. Maier[1] stated **five key characteristics of SoS**:

- Operational independence of the components of the overall system
- Managerial independence of the components of the overall system
- Geographical distribution
- Emerging behaviour
- Evolutionary development processes.

Jamshidi[2] provided a somewhat broader definition of SoS: “A SoS is an integration of a finite number of constituent systems which are independent and operable, and which are networked together for a period of time to achieve a

[1] Maier, M.W. "Architecting Principles for System of Systems," Systems Engineering, Vol. 1, No. 4, 1998, pp. 267-284.
[2] Systems of Systems Engineering: principle and applications. Jamshidi, M., ed., CRC Press, 2009.

This project has received funding from the European Union’s Seventh Programme for research, technological development and demonstration under grant agreement No 611115.

certain higher goal." The concept of systems of systems is understood here in this broad and pragmatic sense, comprising systems where most of the components have some managerial and operational independence, but the purpose of the system is to provide a function or service that cannot be provided by the individual systems independently, or cannot be provided in an as efficient manner as by the overall system. As an additional key characteristic, in a system of systems, the structure, the connectivity and the "membership" of the components can change dynamically over time, components can be added or connected or disconnected, and the overall system and the components can be dynamically reconfigured. This evolution of the system happens on different time-scales. On the operational time-scale, components may be switched on or off, enter or leave (as in air traffic or train control), or change their operational regimes. On a longer time-scale, the system undergoes continuous modifications and re-engineering, it may be upgraded, extended in functionality and scope, components may be replaced by similar components with a better performance or components of another type may be added to the system.

Partial autonomy of several components of a system of systems is constitutive for the concept of SoS. Autonomy is understood here as the ability of the subsystems to pursue their own goals, to perform local optimization or to solve tasks without precise directions. It here does not necessarily mean human-free operation. Human supervision and human interventions and utilization are usually an important element of the autonomy of the subsystems as well as of the overall system. From an engineering point of view, this leads to uncertain behaviours but also to the need of making the systems as transparent to the users as possible without overloading the users or operators.

Systems of systems engineering (SOSE) deals with planning, analysing, organising, and integrating the capabilities of a mix of existing and new systems into a system of systems with greater efficiency or additional capabilities compared to the constituent parts. SOSE is a developing multidiscipline, spanning across and drawing from a variety of disciplines to address complex situations characterized by ambiguity, high uncertainty and emergence[3].

Cyber-physical systems are systems where real-time computing and physical systems interact tightly. This is also the case in embedded systems, and sometimes the term cyber-physical systems is used as a synonym for embedded systems, with a stronger emphasis on the interaction with the physical world and on connectivity, e.g. over the internet. The German "Agenda CPS[4]" is an example of this view.

We here take the concept of cyber-physical systems as **meaning *large complex physical systems* that are interacting with a considerable number of distributed computing elements for monitoring, control and management which can exchange information between them and with human users**. The elements of the physical system are connected by the exchange of material, energy, or momentum and/or the use of common resources (roads, rail-tracks, air space, waterways) while the elements of the control and management system are connected by communication networks which sometimes impose restrictions on the amount of exchange of information. Prototype systems are the electrical grid, a power plant, a car, an airplane or a ship, a manufacturing process with many cooperating elements as e.g. robots, machines, warehouses, and conveyer belts, a large processing plant with many process units, a building with advanced distributed HVAC control, combined heat and power generation, etc.

Cyber-physical Systems of Systems are cyber-physical systems which exhibit the features of systems of systems:

- Large, often spatially distributed physical systems with complex dynamics
- Distributed control, supervision and management
- Partial autonomy of the subsystems
- Dynamic reconfiguration of the overall system on different time-scales
- Continuous evolution of the overall system during its operation

[3] Sousa-Poza, A., Kovacic, S. and Keating, C. "System of systems engineering: an emerging multidiscipline", Int. J. System of Systems Engineering, Vol. 1, Nos. 1/2, 2008, pp.1–17

[4] Agenda CPS, Intermediate Results, Acatech, 2010

This project has received funding from the European Union's Seventh Programme for research, technological development and demonstration under grant agreement No 611115.

- Possibility of emerging behaviours.

Cyber-physical systems of systems may comprise components which by themselves are not cyber-physical, e.g. computer systems which manage the overall system that consists of coupled cyber-physical subsystems, or a communication infrastructure. Therefore the concept is slightly broader than that of Systems of Cyber-physical Systems which implies that each component of the overall system is a CPS.

2. Explanations and more detailed considerations

On the physical side:

- The system consists of a *significant* number of *interacting* components that are (partially) physically coupled and together fulfill a certain function, provide a service, or generate products. The components can provide services independently but the performance of the overall system depends on the “orchestration” of the components.

The physical size or geographic distribution of the system are not essential factors that make it a system of systems nor not, but rather is its complexity. A factory with many “stations” and materials handling and transportation systems is structurally not much different from a large rail transportation network that extends over several countries and may have a similar number of nodes.

Examples: Rail transport systems, power plants, large production facilities, gas pipeline networks, container terminals, water systems, supply chains.

Counterexample: Washing machine (even with remote control over the internet). Here the components do not provide a useful service independently.

Obviously, it is difficult to draw a line with respect to the degree of complexity that is required for a system of systems. As a distinguishing feature, we propose that (some of) the components provide useful services independently. So a car engine with several controllers that are connected by a communication system is a cyber-physical system, but all components only provide a useful function together with the engine, and there is no local autonomy of the subsystems. Autonomy is not the same as local or distributed control.

Control and management

- Due to the scope and the complexity of the overall system or due to ownership or management structures, the control and management tasks are not performed in a completely centralized or hierarchical top-down manner with one authority tightly constraining the control and management of the constitutive subsystems but there is a significant distribution of authority with partial local autonomy, i.e. partially independent decision making.

The distribution of the management and control structure usually follows the physical distribution of the system elements. Large systems are and probably will almost always be controlled in a hierarchical and distributed fashion where local “uncertainties”, e.g. the effects of non-ideal behaviours of components or of disturbances are reduced by local control. Take as an example a flow controller which makes sure that the flow in a pipe reaches and maintains a desired value despite the nonlinearity and the variation of the valve characteristic and the variation of the pressure in the pipe, so that this flow can be used as a control input for higher level control. In this case, the physical system and the local controller can be replaced by a new deterministic system consisting of pipe, valve, sensor and flow controller. There is no local decision making, the subsystem provides a defined service to the overall system, with a certain accuracy and with the possibility of faults occurring.

This project has received funding from the European Union’s Seventh Programme for research, technological development and demonstration under grant agreement No 611115.

Distribution here refers to the functionality of the control and management system, not to the hardware where the necessary computing resources are provided – it is conceivable that many or all "intelligent" functions are run on a bank of central servers, or in the cloud, but as partly independent, interacting applications. The reason for the distribution of control and management functions can be multifold, from run-time complexity over the difficulty of engineering the control and management system as a single system to distributed ownership or management authority.

Communication between the physical sub-systems and the control and management of sub-systems happens via sensors and actuators and various types of communication channels, from wires to connections over the internet that may be unreliable or have limited bandwidth. The elements of the management and control systems similarly communicate via suitable channels. Internet communication mechanisms and wireless channels have provided a much greater connectivity of distributed system elements and this trend will continue ("Internet of Things"). CPSoS research and innovation is about how to use this connectivity for better management and control of the overall systems of systems. The increased connectivity is an enabler for better monitoring, management and control. Internet connectivity adds a significant element of vulnerability to technical systems that can have consequences that go far beyond issues of privacy, as potentially large damages (accidents, power outages, standstills) can be caused. Therefore security against unauthorized access is a major system issue and detection of manipulated signals or commands are important aspects of CPSoS design.

For cyber-physical systems of systems, the management of the overall system as well as of its subsystems will usually not only be driven by technical criteria but rather by economic, social, and ecologic performance indicators, e.g. profitability, acceptance and satisfaction of users, and environmental impact. Technical performance criteria usually either constrain the operating range or are intermediates to achieve the real performance goals. CPSoS are managed by humans and many performance criteria concern providing services to human users. Thus cyber-physical systems of systems have to be addressed as socio-technical systems with the specific feature of a large technical/physical structure that determines and constrains the behaviour of the system to a large extent.

Partial autonomy of the subsystems

- Partial autonomy of the subsystems both in terms of their independent ability to provide certain services and of partial autonomy of their control and management systems are essential in the definition of CPSoS. Of particular interest are systems where the subsystems exhibit "selfish" behaviour with local management, goals, and preferences. The autonomy can in particular result from human users or supervisors taking or influencing the local decisions. The decision structures of the overall system can vary largely, from a (possibly multi-layered) hierarchy, where goals for the subsystems are set but the subsystems have degrees of freedom for how to reach their goals, to a fully decentralized structure where only technical constraints and economic incentives provide the "glue" between the subsystems.

The "managerial element" of the components of the management and control systems goes far beyond classical decentralized control as e.g. for an engine of a car or a unit of a chemical plant where many decentralized digital controllers are in place and control certain variables independently and are parameterized by reference values.

Autonomy is understood in this context as the presence of local goals that cannot be fully controlled on the system of systems level. Rather, incentives or constraints are given to the subsystem control in order to make it contribute to the global system targets. An example is the operation of units of a chemical plant that consume and produce steam as a necessary resource or by-product of their main task. Their operators or managers run their processes autonomously to achieve local goals and meet local targets. The site owner/operator sets mechanisms to negotiate about the steam generation/consumption in order to balance the steam network and in addition should provide suitable incentives so that the global profit of the site is maximized.

If a subsystem is controlled by humans, we can always assume a certain degree of autonomy as we assume that humans are autonomous in their decisions. Human behaviour is of course largely determined by predictable responses to certain situations, but humans act following reasons, preferences, and emotions which are external to the technical system and are not controllable, and their actions are not fully predictable. Hence the intervention of humans creates a degree of uncertainty in the predictability of the system.

In contrast, if a system contains 100 “autonomous”, i.e. isolated, PID controllers, each of these controllers has no autonomy at all, it is just a rather simple algorithm and the behaviour of each controller can be predicted exactly if the necessary information about the controller parameters is available. Local or decentralized control is not the same as autonomous decision making.

Besides the possible selfishness of autonomous subsystems, autonomy also describes the ability of a subsystem to cope with certain tasks, disturbances, faults, on its own, without intervention from the system of systems level. Another way of putting this is to say that the autonomous subsystem absorbs variability and to the outside shows a more predictable behaviour than what would result without its ability to regulate, react, and compensate disturbances. Ideally, a subsystem is given a task and fulfills it (“contract”) under any circumstance, and on the higher level one does not have to care and can abstract away from the details of the behaviour of the autonomously controlled subsystem.

From the outside, an autonomously controlled and managed system may to some extent be unpredictable or uncertain, be it because of unknown or only partially known decision mechanisms or because of unknown external influences.

Autonomy can lead to self-organizing systems: Consider the flow of cars in a city when there is a new construction site. Due to their autonomous intelligence the drivers seek new paths, quite predictably, and after a few days each one re-optimizes her or his route to minimize travel time, and a new flow pattern establishes itself. This may not be provably optimal, but the autonomous actions of the “agents” lead to resilience of the overall system.

Dynamic reconfiguration of the system

- Dynamic reconfiguration refers to the addition or removal of components on different time scales, depending on the nature of the system and the reasons for the changes of the structure and changes of the way the system is operated. It includes systems where components come and go (like in air traffic control) as well as the handling of faults and the change of system structures and management strategies following changes of demands, supplies or regulations.

Additions and modifications of system components are much facilitated by plug-and-play capabilities of components that are equipped with their own management and control systems.

Fault detection and handling of errors or abnormal behaviours is a key issue in cyber-physical systems of systems. Due to the large scale and the complexity of CPSoS, failures are the norm in CPSoS. The average system performance, as well as the degree of satisfaction of the users, is strongly affected by the impact of rare unforeseen events and outer influences that require non-continuous actions and cannot be compensated on the lower system levels. There is a massive need for detecting such situations quickly and, if possible, preventing them, and for fail-soft mechanisms and resiliency and fault tolerance at the systems level. The handling of faults and abnormal behaviour is challenging from a systems design point of view as in many cases it cannot be done optimally by a design based on separation of concerns but requires a trans-layer design of the reaction to such events.

Living cells with their multiple metabolic pathways are an example of a system that has optimized its ability to reconfigure itself to cope with changing conditions (availability of nutrients and other external factors) by keeping many options (metabolic pathways) intact and being able to switch between them.

For cyber-physical systems of systems that do not operate in a strictly controlled environment, dynamic reconfiguration is a key element.

Continuous evolution

- Cyber-physical systems of systems are large systems that operate and are continuously improved over long periods of time. In many systems, from railways to chemical plants, the hardware (real physical hardware) infrastructure "lives" for 30 or more years, and new functionalities or improved performance have to be realized with only limited changes of many parts of the overall system. Management and control software as well usually has long periods of service, while the computing hardware base and the communication infrastructure change much more rapidly. Components are modified, added, the scope of the system may be extended or its specifications changed. So engineering to a large extent has to be performed at run-time.

The waterfall paradigm "Requirements – modelling – model-based design – verification – commissioning – operation - dismantling" is not applicable to systems of systems where the requirements change during operation.

It was reported from the aerospace industry that systems engineers are often stuck in a "requirements first" clean sheet design paradigm and are used to having a level of control over all system elements that is not available to them in systems of systems engineering. Hence there is a need for a scientific foundation to handle multi-layer operations and multiple life-cycle management.

Specification needs to be thorough in the context of real systems of systems use cases, which should be as simply and clearly articulated as possible. Testing also needs to be thorough in the context of real systems of systems and must include also "mis-use cases". Once rolled out, operating and maintaining a system of systems requires a good knowledge of the "as-deployed-and-configured" system's physical, functional and behavioural configuration. Here the aviation industry has great experience.

When a new system is developed and deployed, the two activities of design and operational management usually can clearly be distinguished and often different groups of people are responsible for them. But later, the distinction is blurred, the experience gained in (day-to-day) management must be taken into account in revisions, extensions etc., and the operational management must also take care of the implementation of engineered changes in a running system. Validation and verification has to be done "on the fly". This integration strengthens the role of models in both engineering processes. Up-to-date (because continuously updated) models of the running operation can be used for both purposes. If they are adapted to the real operational practice, they reflect reality better than the original engineering models and can be used to investigate options for modifications as well as improved operational policies without modifications. System of systems require engineering methods and tools that can be used seamlessly during design as well as operation (design-operations continuum).

Possibility of emerging behaviours

- Emerging behaviours are an issue that is highly disputed. In our view, it is too simple to refer to the fact that the system as a whole is more than its parts and can provide services that the components cannot provide autonomously. Sometimes the term emerging behaviour is used for the consequences of simple dynamic interactions, e.g. that a feedback loop that consists of stable subsystems may become unstable (and vice versa), or of design flaws due to an insufficient consideration of side-effects. The term emerging behaviour however seems more appropriate for the occurrence of patterns, oscillations or instabilities on a system-wide level, as it may occur in large power systems, and to self-organization and the formation of structures in large systems.

Emerging behaviour should be distinguished from cascades of failures, like if a traffic jam on one motorway leads to one on the alternative route. However, if faults lead to instabilities and possible breakdowns of a large system due to "long-range interactions" in the system, like in power blackouts, then this can be called emerging behaviour. In technical systems, emerging behaviours usually are seen as problematic as a predictable behaviour of the system is preferred. On the other hand, in large systems with subsystems that show significant diversity in their behaviours, the formation of stable structures on a higher level due to the interactions between the subsystems despite their local diversity is very important and enables the design and management of the overall system without precise knowledge of all its elements. Emerging behaviour should be addressed both from the side of system analysis – under which conditions does emerging behaviour occur – and from the side of systems design – how can sufficient resiliency be built into the system that local variations, faults, and problems can be absorbed by the system or be confined to the subsystem affected and its neighbors and do not trigger cascades or waves of problems in the overall system. Formal verification (e.g. assume/guarantee reasoning) as well as dynamic stability analysis for large-scale systems are possible approaches to prove the non-existence of unwanted emerging behaviours.

3. Enabling CPSoS technologies and methodologies

The scope of cyber-physical systems of systems technology is the engineering and operation of cyber-physical systems of systems defined as described above.

In order to engineer and to operate cyber-physical systems of systems, knowledge and technologies from many domains are needed. We distinguish between enabling technologies that are required to realize cyber-physical systems of systems but are developed independently and for a broad range of purposes, and core technologies that are specific and have to be specifically developed for cyber-physical systems of systems.

Examples of enabling technologies and methodologies:

- Communication technologies and communication engineering. Standardized protocols, exploiting the Internet of Things, e.g. interactions between phone and car, to provide new functionality/services, LiFi – light communications.
- Computing technologies, high-performance and distributed computing. Multicore computing and new computer architectures to deal with more data and provide localised processing, low power processing for ubiquitous installation (with energy harvesting supplies), ability to implement mixed criticality on multicores.
- Sensors, e.g. energy harvesting, Nano NEMs sensors - the next generation beyond MEMs.
- Management and analysis of huge amounts of data (“big data”).
- Human-machine interfaces, e.g. head up displays, display glasses, polymer electronics and organic LEDs to display information.
- Dependable computing and communications.
- Security of distributed/cloud computing and of communication systems.

Research and innovation in these areas contributes strongly to the ability to develop and operate cyber-physical systems of systems more efficiently and more reliably, but is of a broader nature. CPSoS research and innovation includes to investigate how to best make use of these technologies and to trigger and jointly perform specific CPSoS-related developments.

4. Core CPSoS technologies and methodologies and areas for future research and innovation

Requirements engineering and model-based systems engineering and validation and verification over the system’s full life-cycle

New approaches are needed for dynamic requirements management during the operation of a cyber-physical system of systems, ensuring correctness by design during its evolution, and for verification especially on the system of systems level. This includes formal languages and verification techniques for heterogeneous distributed hybrid systems including communication systems, theory for successive refinements and abstractions of continuous and discrete systems so that validation and verification at different levels of abstraction are correlated, and the joint use of simulation-based (Monte Carlo) and exhaustive (model checking) verification techniques. A model-based approach should support the exploration of the design space in a relatively fast way in order to see which designs are feasible or infeasible, and a model-based approach for early integration and testing. The decision between the use of cross-layer and separation-of-concern based designs must be understood better.

A key requirement in systems of systems engineering is to re-use existing systems, to integrate them in an operational environment with new ones and to obtain the benefits of the resulting synergy. The challenges in rolling out systems of systems are the asynchronous lifecycles of the constituent parts and also the fact that many components are developed independently and that legacy systems may only be described insufficiently. The key is to make sure that the integration is loosely coupled so that integration can happen in any order, or at least such that useful capability is achieved by many different partial system of systems configurations. To support this, the interfaces must be simple and easy to test. An important research area is the interaction between new components and those they are meant to replace as during a staged roll out they need to co-exist with existing components.

Modelling and large-scale simulation of heterogeneous systems of systems

Modelling and simulation are key to improved design, operation and continuous improvement of cyber-physical systems of systems. The design of complex systems is increasingly built upon models, but building reliable and sufficiently precise models of a system often requires significant efforts. The challenges in modelling include the high cost for building and maintaining models and the difficulty of model re-use, modelling, simulation and analysis of stochastic behaviour, coupling tools of different strengths without the need for re-modelling, the consistency of detailed and abstract models, and the effort needed for setting up models that include failure states and the reaction to abnormal situations for validation and verification purposes. Different levels and types of models must be provided for different steps in the design process and for fault detection and operations support. Keeping these models up to date and consistent (model management) is a major issue as well as reducing the effort and cost of modeling by model re-use (object-oriented or modular modelling) and predefined and adaptable standard models. New business models may lead to a situation where for potential system components simulation models are delivered such that the overall system can be designed on these models. Modelling of the behaviour of users or operators of systems of systems or of their components and the structure formation among users also is an important future research topic.

Challenges in simulation include large-scale simulation of heterogeneous systems, efficient hybrid (continuous-discrete) simulation, simulation of systems with many different time scales, and integrated simulation of the physical part of the system and the management strategies for performance analysis including abnormal situations. Efficient simulation of complex systems with reconfiguration and switching behaviours requires dynamic on the fly reconfiguration of simulation models, including switching between models of different level of detail according to the required accuracy and the operating conditions as well as high performance numerical algorithms.

The model-based development of systems of systems necessitates collaborative environments for competing companies and the integration of legacy system simulation as well as open approaches for tight and efficient integration and consolidation of data, models, engineering tools, and other information across different platforms.

Models are the basis for the optimization of the design of systems of systems and for the use of optimization methods in their management and control. Usually the design optimization will lead to multi-criterial optimization problems for which techniques that are efficient for large heterogeneous non-convex system models must be developed.

Partially autonomous decision making and system-wide control and coordination

The interaction and coordination of dynamic systems with partial autonomy in systems of systems, possibly with dynamic membership, must be studied broadly. Examples of applicable methods are population dynamics and control and market-based mechanisms for the stimulation of the production and for the distribution of constraining resources. As discussed above, the partial autonomy of the components from the system of systems perspective leads to uncertainty about the behaviour of the subsystems. Therefore the system-wide coordination must take into account uncertain behaviour and should nonetheless guarantee an acceptable performance of the overall system. Stochastic optimization and risk management should be developed for CPSoS. It must be understood better how the type of control (centralized, hierarchical, distributed, clustered) influences system performance.

Collaborative decision making by computer systems and humans

Filtering and appropriate presentation of information to human users is an important research topic, as well as the identification of the capabilities of humans and machines in real-time monitoring and decision making and the investigation of how to combine them optimally by human-machine cooperation. HMI concepts are crucial for the acceptance of advanced computer-based solutions by human users or operators. If systems are sold in large numbers, like cars, a high development effort can be invested to make them completely automatic and/or robust against wrong behaviours of the human users and operators. This is not possible in domains where solutions are one of a kind and human intervention is needed to react to unforeseen situations and faults and to monitor the behaviour of the overall system. Humans may introduce an additional nonlinearity and uncertainty in the system. Interesting research issues in collaboration with other communities are the human capacity of attention and how to provide motivation for sufficient attention and consistent decision making. Future research on the monitoring of the actions of the users and anticipating their behaviours and modelling their situation awareness is a promising direction of progress. The distribution of responsibility between automated components manufacturers and the users is a crucial question in some application domains, e.g. road traffic. Social phenomena (e.g. the dynamics of user groups) must also be taken into account.

Fault detection, resilience, reconfiguration, and integration of new components

Due to the large scale and the complexity of systems of systems, failures are the norm in CPSoS, hence there is a strong need for the detection of abnormal states and for fail-soft mechanisms and fault tolerance by suitable mechanisms at the systems level. Advanced monitoring of the state of the system and triggering of preventive maintenance based on its results can make a major contribution to the reduction of the number of unexpected faults and to the reduction of maintenance costs and downtimes. The availability of cheap and easily interfaced sensors will contribute significantly to better fault detection and fault prevention. The effect of faults on the performance of the system must be predicted reliably to decide on the required degree of redundancy. Many real-world SoS experience cascading effects of failures of components. Faults may propagate over the different layers of the management and automation hierarchy. The response to these abnormal events should be designed systematically across the layers and be verified rigorously.

Methods for verification and validation when components are added or modified are needed, as well as methods for the design of systems that can be safely integrated during operations (“plug and play”).

Another issue in the context of reconfiguration is to move functionality around a system in order to make the best possible use of the computational resources.

Large-scale online data analysis and feature extraction (“artificial cognition”) for the analysis and the dynamic management of systems of systems

During the operation of cyber-physical systems of systems, huge amounts of heterogeneous data are generated, transmitted and stored. There is a huge potential in using this data in combination with other data (e.g. weather data) for better system understanding, optimization, condition monitoring and detection of abnormal situations, e.g. based

This project has received funding from the European Union’s Seventh Programme for research, technological development and demonstration under grant agreement No 611115.

upon pattern recognition. This requires real-world real-time data analysis based upon data integration, synchronization, and feature extraction, merging operational and maintenance and diagnostic data, dealing with heterogeneous data with respect to data type, reliability and quality, and designing for resilience against missing and erroneous data. Also pattern recognition in historical data could provide fast hints on the current state of the system and possible paths of action.

Trust in large distributed systems

Cyber-security is a very important element in cyber-physical systems of systems. Maintaining privacy is an important issue here but this is addressed in other parts of the HORIZON 2020 Work Programme. A specific CPSoS topic is the recognition of obstructive injections of signals or takeovers of components in order to cause malfunctions, suboptimal performance, shutdowns or accidents which needs to be specifically addressed for CPSoS because the detection (and the planning) of such attacks requires to take into account both the behaviour of the physical elements and the computerized monitoring, control and management systems. In the case of the detection of unsecure states, suitable isolation procedures must be designed and soft (partial) shut-down strategies.

Stability, structure formation and emergent behaviour in cyber-physical systems of systems

The prediction of emergent behaviour is an open challenge at the moment. It is not clear how distributed management and control methods can be designed such that CPSoS do not show undesired emerging behaviour or how this can be verified for a given design. Inputs from the field of dynamic structure or pattern formation in large systems with uncertain elements are needed.

5. Need of an interdisciplinary approach

Cyber-physical systems of systems cannot be designed and managed using theories and tools from only one single domain. The behaviour of the large coupled physical part of the system must be modelled, simulated and analysed using methods from continuous systems theory, e.g. large-scale simulation, stability analysis, and design of stabilizing control laws. An impressive example of the strength of this approach is the analysis, detection and damping of large power oscillations across the European power grid[5], another one is the management and stabilization of wind farms. On the other hand, methods and tools from computer science for the modelling of distributed discrete systems, for verification and testing, assume-guarantee methods, contract-based assertions etc. are indispensable to capture both the behaviour on the low level (discrete control logic, communication, effects of distributed computing) and global effects, in the latter case based on abstract models of complete subsystems. Logistic models as well as models and tools for performance analysis of discrete systems will be useful for system-wide performance analysis. Finally, theories from physics, e.g. structure formation in large systems, and from economics and social science (market mechanisms, evolution of beliefs and activity in large groups) may also prove to be useful.

The size of cyber-physical systems of systems and their “multimodality” or hybrid nature consisting of physical elements as well as quasi-continuous and discrete controls, communication channels, and local and system-wide optimization algorithms and management systems, implies that hierarchical and multi-domain approaches to their simulation, analysis and design are needed that are currently not available. Scalability of the methods is a crucial issue. In the individual domains, e.g. dynamic modelling and simulation, verification of discrete systems, design of controllers for guaranteed system stability on different system levels, and optimization of flows across the system, further progress can be expected that will have a high impact on the engineering of systems of systems. However, the simultaneous use and the integration of heterogeneous models and tools to capture system-wide properties reliably

[5] Mats Larsson (ABB Corporate Research): Wide-area Monitoring in Control for Electric Power Systems. Presentation at the HYCON II Workshop on Energy, Brussels, September 4, 2012.

and with firm guarantees are currently completely open issues. The critical properties of cyber-physical systems of systems go beyond what can be analysed and designed systematically today: dynamic reconfiguration of complex systems, large-scale dynamics, waves of events or alarms, interaction of autonomous, selfish systems, and coupling of physical and computational elements via communication channels.