Towards a European Roadmap on Research and Innovation in Engineering and Management of Cyber-Physical Systems of Systems

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

Presented by Prof. Sebastian Engell / TU Dortmund

at the first Meeting of the European Systems of Systems Research Cluster on July 9th, 2014 in Sophia Antipolis

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

Systems of Systems

Standard Definition (Maier)

- 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

Systems of Systems

Pragmatic Definition

- 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.

Additional key characteristics

- The structure, the connectivity and the “membership” of the components can change dynamically over time, components can be added or connected and disconnected and be dynamically reconfigured.
- The system evolves continuously, components are added, modified while the system is in operation.

Cyber-physical Systems

Standard definition

- Tight interaction of physical systems and real-time computing
- **More than embedded – connectivity, larger scale**
- Computer science: Cyber-physical systems are about control

Our definition

- ***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 other CPS and with human users
- Physical connections between the subsystems
- Exchange of information can be subject to failures or be restricted by bandwidth limitations.

Cyber-physical Systems of Systems

Cyber-physical systems of systems are CPS with these features:

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

Physical System Elements

- *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.
- After a removal of some components, the overall system can still fulfill its function, with reduced performance.
- The physical size or geographic distribution of the system is not essential but its complexity and the partial autonomy of the components.
- **Examples*:***
  - Rail transport systems, power plants, production facilities, gas pipeline networks, container terminals, road transport, supply chains ...

Control and Management

- Not performed in a completely centralized or top-down manner with one “authority” providing all the necessary control signals but with distributed decision power
- Drivers are economic, social and ecologic.

Partial Autonomy

- Independent ability of the components to provide certain services
- Partial autonomy of the control and management systems of the components
- Subsystems can exhibit “selfish” behaviour with local management, goals, and preferences.
- Autonomy can result from human users or supervisors taking or influencing the local decisions.
- Ranges from a (possibly multi-layered) hierarchy to a fully decentralized structure where only technical constraints and economic incentives connect the subsystems.
- The “managerial element” of the components goes beyond classical decentralized control.

Dynamic Reconfiguration

- Addition or removal of components on different time scales, depending on the nature of the system
- Changes of the way the system is operated
- 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.

Emerging Behaviour

- Occurrence of pattern formation, oscillations and instabilities on the system level
- Not anticipated in the design
- Usually not intended in technical systems
- Simple feedback phenomena and design flaws should not be mixed up with emerging behaviour.
- Analysis of the possibility of emerging behaviours is a challenge.

Continuous Evolution

- Systems operate and are continuously improved and modified over long periods of time.
- The 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 has long periods of service, while the computing hardware base and the communication infrastructure change much more rapidly.
- Engineering is re-engineering and takes place at run time.

Challenges of CPSoS

- The size of the system and the “ownership structure” do not permit a “top-down-only” control and management structure.
- Partial autonomy of (some) system elements
  - Local optimization rather than local reference tracking
  - Possibly erratic behaviours due to human intervention
  - From an outside view, autonomy and uncertainty cannot be distinguished → distributed control and optimization under uncertainty

- Full scale “flat” verification or proof of stability impossible
  - Layered approaches
  - Assume/guarantee or contracts
  - Abstractions – well understood for discrete systems but not for continuous ones

Challenges of CPSoS

- Systems of systems operate and are continuously improved and modified over long periods of time
  - No clear sequence design – operation
  - Continuous engineering at runtime
  - Waterfall “Requirements – modelling – model-based design – verification – commissioning” not applicable
  - Legacy elements may be insufficiently described
  - Dynamic requirements management needed
  - Need for “Plug and play” – complex interfaces
  - Verification and validation when components are added / modified

Challenges of CPSoS

- Handling faults and abnormal situations
  - Average system performance and user satisfaction are strongly determined by the effect of faults and abnormal situations on the system
    - Failures and degradation of components
    - Human errors or lack of compliance or performance
    - Extreme conditions
    - Accidents
  - Due to the size of the system, fault-free behaviour is rare.
  - Error handling is a multi-layer phenomenon → trans-layer design
  - Early detection is crucial → data analysis, e.g. in road traffic
  - Enormous challenge in modelling and simulation and design

Challenges of CPSoS

- Multi-scale multi-domain multi-system simulation needed
  - Object-oriented “plug and play” modular modelling
  - Dynamic reconfiguration (cf. flare system)
  - Reconfiguration of the level of detail to reduce the computational load
  - High performance numerics
  - Co-simulation

- CPSoS are human controlled
  - Humans are an important (dynamic and uncertain) element of the system
  - Interaction of physical systems, algorithms, and humans
  - Social phenomena have to be considered
  - Division of tasks, synergetic collaboration, MMI

Challenges of CPSoS

- "Cognitive" CPSoS
  - Enormous amounts of data available in Systems of Systems
  - How can it be used during operation?
    - State monitoring and early fault detection
    - Detecting similar patterns and identifying "good" reactions
- Emerging behaviours
  - How to predict system-wide effects like event cascades or system-wide oscillations?

Enabling Technologies

- Communication technologies and communication engineering → where is co-design needed?
- Computing technologies, high-performance and distributed computing
- Human-machine interfaces
- Dependable computing and communications
- Security of distributed and “open” systems

Research Areas

TOOLS

- Requirements engineering and model-based engineering over the system's full life-cycle
- Modelling and large-scale faithful simulation
  - Integration of highly accurate models from different domains
  - Global high-level modelling including stochastic phenomena
  - Integrated models that include the behavior of communication systems
  - Modelling of the behavior of the users and supervisors
  - Model reconfiguration, model consistency and model integration
- Validation and verification of key properties of heterogeneous cyber-physical systems of systems
- Productive integrated development environments

Research Areas

MANAGEMENT AND CONTROL METHODS

- Distributed ("agent-based") autonomous decision making and control and coordination of independently controlled uncertain subsystems
  - Population control, coalition games, market-based methods, …
- Adaptation, plug-and-play
- State monitoring, maintenance planning and fault detection
- Exception handling /fault mitigation on the system level
- Collaborative, possibly multi-objective decision making by computer systems and humans, including filtering and appropriate presentation of information to human users

Research Areas

SYSTEM-WIDE PROPERTIES

- Stability, structure formation and emergent behaviour in large distributed systems
- Reconfiguration, replacement of components and integration of new elements
- Verification and validation of dynamically changing systems
- Large-scale online data analysis and feature extraction (“artificial cognition”) for the analysis and the dynamic management of systems of systems
- Trust in large distributed systems, detection of manipulated signals

Interdisciplinary Approach

- **Cyber-physical systems of systems require a multi-disciplinary approach!**
- The behaviour of the physical part of the system must be modelled, simulated and analysed using methods from **continuous systems theory**, e.g. large-scale simulation, stability analysis, design of stabilizing controls
- 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 are needed for system-wide performance analysis.
- **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.

Next steps

- Discussion at the cluster meeting
- Distribution of the extended draft of the "CPSoS scope and research needs" paper to the Working Group members
- Discussion at the public WG workshops in September
- Prioritization of the research challenges
- Discussions with experts
- Discussion with the Commission
- Collection of technical papers on the research challenges