# A Model-based Development, Execution, and Evolution Platform for Dependable Cyber-Physical System-of-Systems

Swedish Workshop on the Engineering of Systems of Systems (SWESoS) 2016

**DEJIU CHEN**
Assoc. Professor, chen@md.kth.se

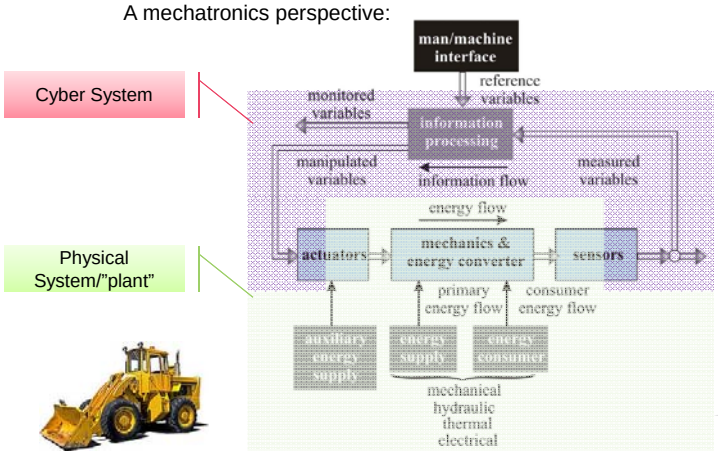
2016-09-09

## Cyber-Physical System - I

A mechatronics perspective:

Cyber System

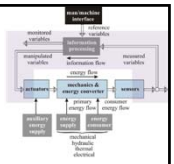
Physical System/"plant"





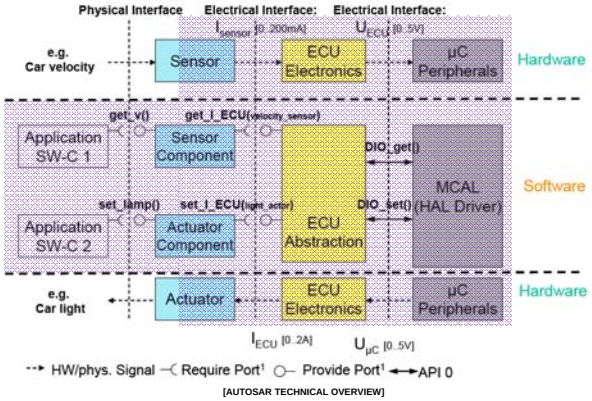

safety

Isermann, R.: Mechatronic design approach, in Bishop, R.H. (Ed.): *The Mechatronics Handbook*, CRC Press, Boca Raton, Section I: Overview of mechatronics, ch. 2, p. 3, 2002.



## Cyber-Physical System – II

An embedded systems perspective:



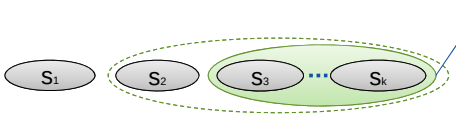

[AUTOSAR TECHNICAL OVERVIEW]

3

## Cyber-Physical System-of-Systems

A system given by some constituent systems that are

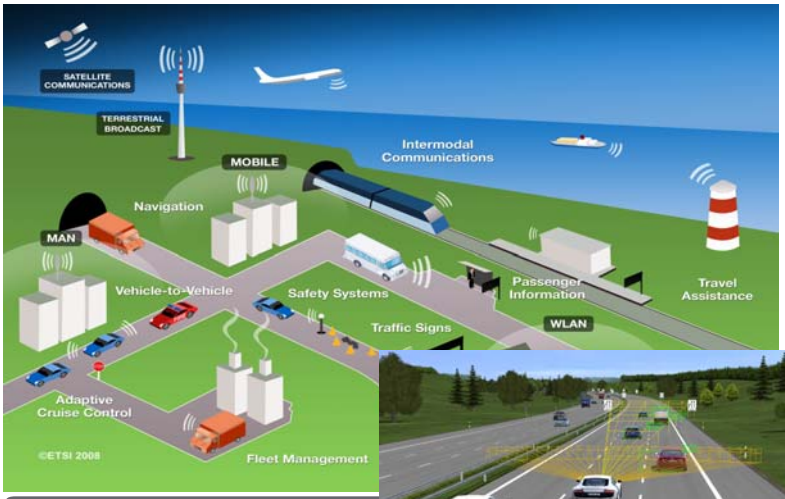
1. Operational and managerial independent,
2. Separate lifecycles (legacy or newly developed)
3. Functional and/or technological heterogeneous
4. Distribution…




- Cooperative vs collaborative
- Open System Boundary,
- Dynamic Configuration,
- Emergent Properties

4

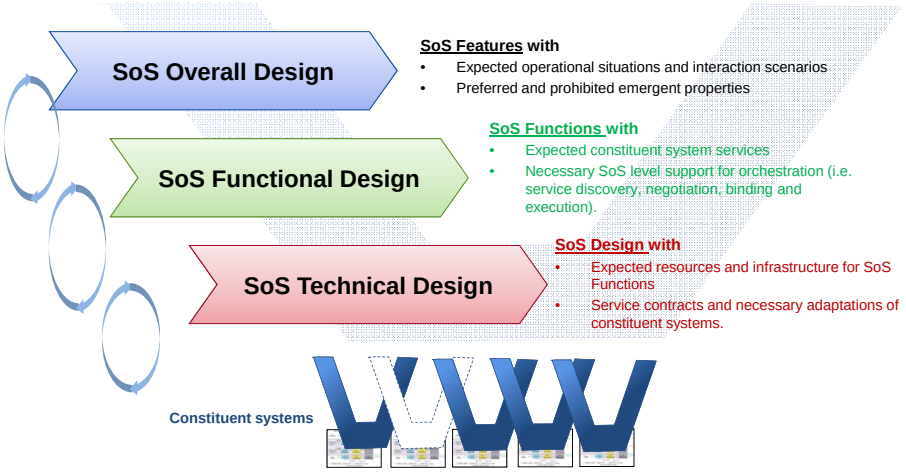
## Example CP SoS






Source: ETSI

## Engineering perspective

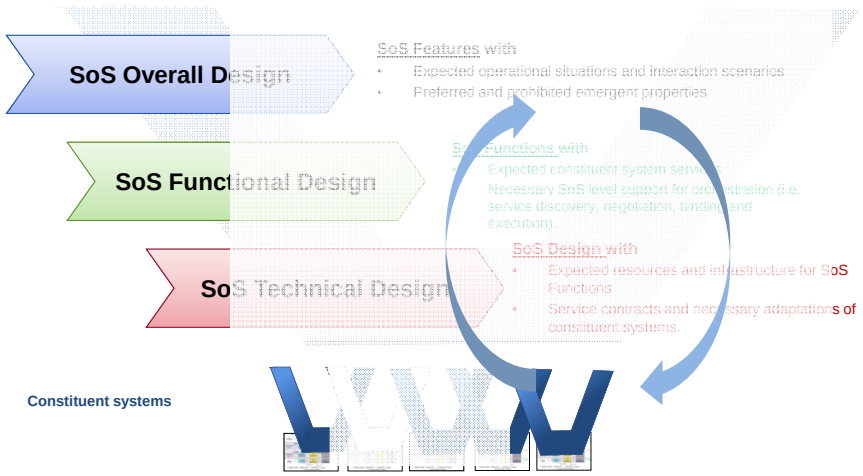



**SoS Features with**
- Expected operational situations and interaction scenarios
- Preferred and prohibited emergent properties

**SoS Functions with**
- Expected constituent system services
- Necessary SoS level support for orchestration (i.e. service discovery, negotiation, binding and execution).

**SoS Design with**
- Expected resources and infrastructure for SoS Functions
- Service contracts and necessary adaptations of constituent systems.

## Bottom-up vs Top-down




- Cooperative or collaborative operation

## Related Concerns

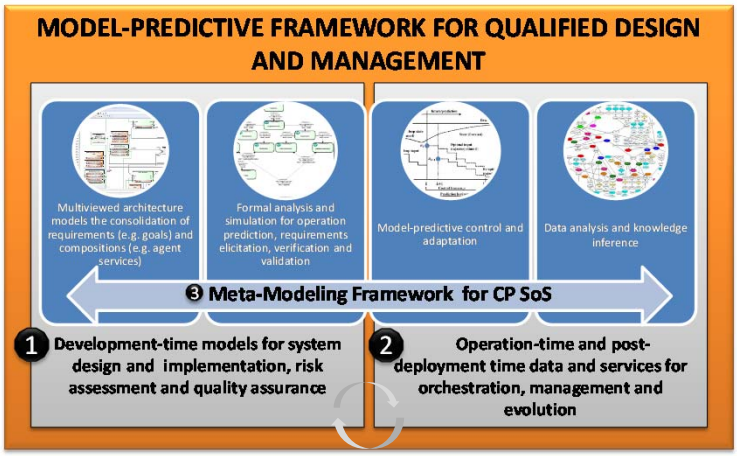
**Qualified treatment of SoS uncertainties:**

- ❑ Emergent properties
- ❑ *a priori* unknown operation situation
- ❑ Stochasticity/plausibility in perception
- ❑ Nondeterministic decision-making
- ❑ Inherent incompleteness of V&V

safety

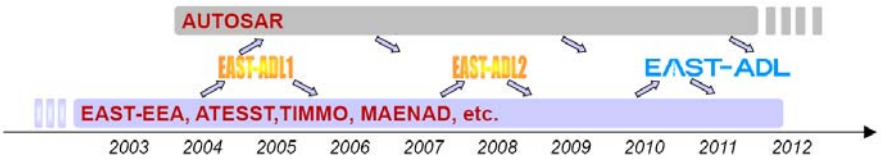
1. **How to formally specify and manage the SoS uncertainties** for
   - ❑ requirements engineering,
   - ❑ SoS development and
   - ❑ Safety engineering
   - ❑ Lifecycle management and evolution
2. **How to support effective V&V of SoS as well as related constituent systems** using
   - ❑ Well-defined contracts
   - ❑ Composable V&V cases
   - ❑ Services for run-time knowledge inference, risk asessment and behavior adaptation

**A Model-based Development, Execution, and Evolution Platform for Dependable Cyber-Physical System-of-Systems**




## One base technology: EAST-ADL

- A common **ontology** for improved engineering methods and tools



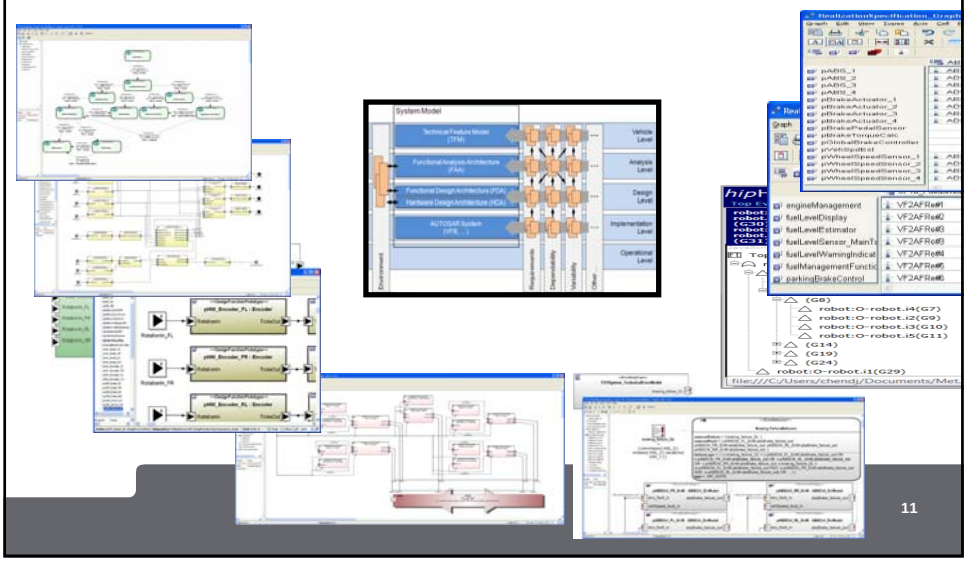

- AUDI AG
- BMW AG
- Carmeq GmbH
- CRF
- Daimler AG
- ETAS GmbH
- **Mecel AB**
- **Mentor Graphics**
- OPEL GmbH
- PSA
- Renault
- Robert Bosch GmbH
- Siemens, Continental
- Valeo
- Vector
- **Volvo Car Corporation**
- **Volvo Technology AB**
- ZF
- CEA-LIST
- INRIA
- LORIA
- Paderborn Univerisity-C-LAB
- Technical University of Darmstadt
- Technische Universität Berlin
- **The Royal Institute of Technology**
- The University of Hull
- …

**http://www.east-adl.info/**

10

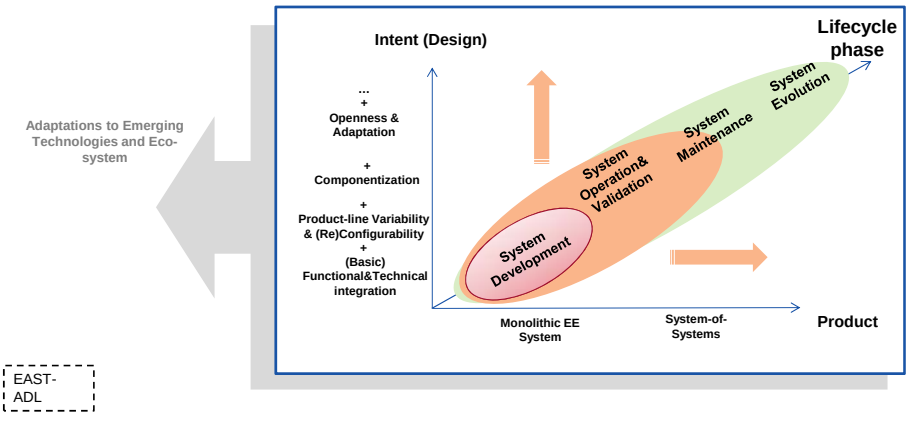
## Current EAST-ADL Support

Focused on EE system and the architecture development:



11

## EAST-ADL Evolution




13

## Direction I - Model-based SoS development and management with an additional SoS Modeling Layer

**SoS Overall Design**

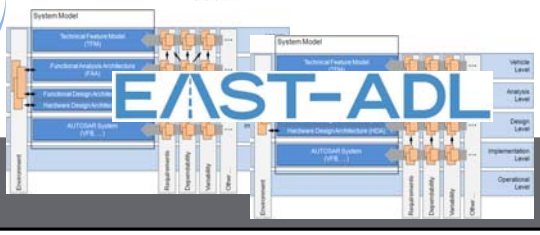
**SoS Features with**
- Expected operational situations and interaction scenarios
- Preferred and prohibited emergent properties

**SoS Functional Design**

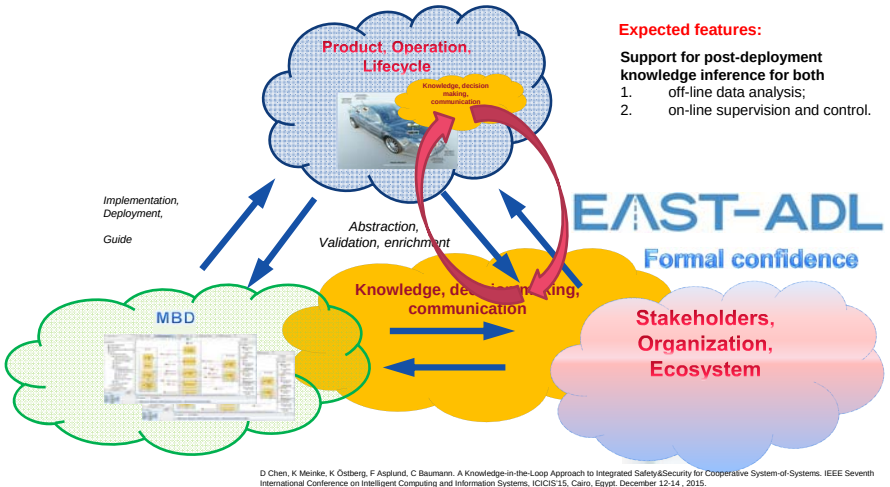
**SoS Functions with**
- Expected constituent system services
- Necessary SoS level support for orchestration (i.e. service discovery, negotiation, binding and execution).

**SoS Technical Design**

**SoS Design with**
- Expected resources and infrastructure for SoS Functions
- Service contracts and necessary adaptations of constituent systems.




## Direction II - "Knowledge-in-the-Loop"

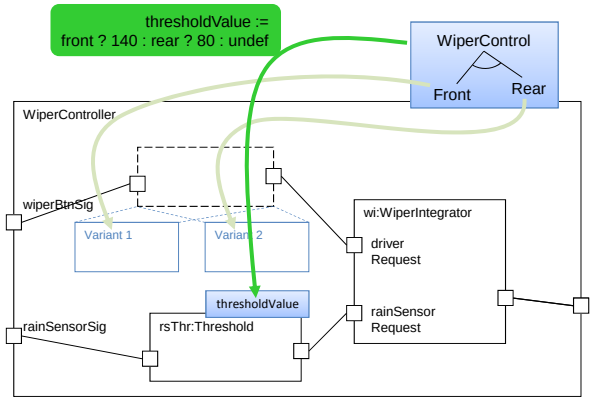



**Expected features:**

**Support for post-deployment knowledge inference for both**
1. off-line data analysis;
2. on-line supervision and control.

D Chen, K Meinke, K Östberg, F Asplund, C Baumann. A Knowledge-in-the-Loop Approach to Integrated Safety&Security for Cooperative System-of-Systems. IEEE Seventh International Conference on Intelligent Computing and Information Systems, ICICIS'15, Cairo, Egypt. December 12-14 , 2015.

## Example of system variability




EU FP7 ATESST2

19

## Conclusion

- CP SoS implies a rich set of functional and extra-functional challenges
  - Multidisciplinarity
  - Heterogeneousity
  - Uncertainties
- "Knowledge-in-the-loop" for a seamless interplay of
  - MBD with Correct-by-construction
  - Advanced services for self-awareness, control and validation.