Beyond Crystal –
A Metamodel for Systems of Cyber Physical Systems

Werner Damm
Director,
Interdisciplinary Research Center on Critital Systems Engineering,
Carl von Ossietzky University Oldenburg
Chairman, OFFIS Transportation
Chairman, SafeTRANS
Member acatech

joint work with Alberto Sangiovanni-Vincentelli, UCB
WHY WE NEED THIS
SmartRoads

The status quo:

Complex and interconnected road networks

Emergency vehicles delayed due to traffic

World’s largest traffic jam: 100+ Km/10+ days

Communication and Control:

FHWA IT Connections

Global web of critical IT infrastructure

The Smart Roads testbed/system integrates advanced control algorithms (CC) and high-fidelity simulation software (C2WT) with real-time data to predict and manage traffic flows to support the realization of resilience to cyber attacks.

The CC project will provide a next generation decision support system for the Greater Los Angeles area by 2016, soon to be deployed in 50 corridors in California.

Additional tests will involve DOT’s Southeast Michigan Testbed.

Picture Source: Smart America, http://smartamerica.org/privacy-policy/
Smart water
Apply monitoring and management technologies to help optimize the availability, delivery, use, and quality of water as well as related systems including energy and chemical treatment.

Smart energy
Analyze customer usage and provide customized products and services that help to boost efficiency from the source through the grid to the end user.

Future challenges
Managing Systems of Cyber Physical Systems
Self Learning Systems

Picture Source: A. Sangiovanni Vincentelli
http://www.safetrans-de.org
The need for Cross-domain Platforms
The need for a cross-domain cross instruments platform strategy

- Europe has so far no instruments to enforce cross domain platform building across different CPS related funding instruments, resulting in
  - barriers in creating cross-domain solutions due to lack of interoperability and shared standards (such as in smart cities)
  - re-inventing the wheel
  - impossibility to make end-to-end quality assurance, vulnerability
  - fragmented eco systems
Challenges

- Optimization applications rely on crowd sourcing of individual behaviours for optimizing overall system utilization – such as smart grid, traffic flow optimization, ...

- Commodity equipment used for lowest level of measuring individual activities

- Yet planting a virus in these can cause complete system crash with immense consequences
The need

• Cross domain standard for quality assurance attributes of systems
• For ALL non-functional parameters relevant for the highest criticality level of integrated systems:
  – resilience
  – reliability
  – time
  – ....
A key observation

• This does NOT entail that all such systems are developed to ensure high levels of
  – reliability
  – resilience
  – timing predictability
  – ....

• BUT that characterizations of such systems wrt to what levels are achieved ARE A MUST

• We can not provide Assurance Facets for CPS without this
A platform strategy for Systems of CPS

- Combined top-down / bottom up approach
  - complement existing instruments by light-weight structure / industry association (IA) fostering identification of potentials cross-domain solutions and cross domain platforms and cross domain interoperability reflected in shared strategy
  - Dedicated funding program for cross-domain solutions (harmonized EU-US funding)
  - Dedicated funding for cross-instrument cross-domain platform building
A METAMODEL FOR SYSTEMS OF CPS
Objectives

To provide a Reference Meta Model for Systems of Systems (including human actors) as a basis for

– formal operational semantics enabling formal analysis (of risks, failures, threats, emergent behaviour)
– designing hierarchical multi-level decentralised control
– lifelong adaptability to changing objectives, changing actors, changing capabilities of actors, changing regulatory settings
A running Example
Causes of Failures of SoS: what must be addressed by the blueprint
Overarching Challenges

• anticipating unknown deployment contexts
  – changing environments
  – changing capabilities
  – changing regulations

• from off-line assessment to on-line assessments

• from off-line design to on-line synthesis

• integrating complex physical environments

• integrating the cyber world
Coping with changing environments

• The blueprint demands for each actor to explicate its beliefs about its environment
  – health state, location, current and expected dynamics of actors (human and technical) in its proximity
  – introspection into the beliefs and plans of other agents in same “coalition”
  – dynamics of physical environment (forces acting on actor, prevailing weather conditions, disturbances, ...)
  – possibly aggregated beliefs about the environment beyond its proximity

as perceived through sensors or via information sharing with other actors
1. Maintain safety
2. Drive to exit 42
3. Minimize travel time
4. Minimize fuel consumption

Available capabilities:
1. Keep distance
2. Maintain speed
3. Video
4. Lidar
5. Radar
6. C2I comm
7. Change lane
8. Accelerate

Role: Highway
Health State: all
Environment mode: sunny

Goals:
1. Maintain safety
2. Drive to exit 42
3. Minimize travel time
4. Minimize fuel consumption

Available capabilities:
1. Keep distance
2. Maintain speed
3. Video
4. Lidar
5. Radar
6. C2I comm
7. Change lane
8. Accelerate

Environment beliefs:
- my_id
- my_loc
- my_v
- 60
- c5, c3, c1
- c1
- HwyCtr_c2

I know:
- c

I partner with:
- c

I receive orders from:
- (c,c5)
- (c,c3)
- (c,c1)
- (c,HwyCtr_c2)

Available capabilities:
- Video
- Lidar
- Radar
- Acceleration

my state

Environment mode: sunny
Challenge

• How can we assure, that an actors belief about its environment is “sufficiently precise” for achieving its services?
  – can we observe all relevant artefacts of the environment?
  – can we provide confidence guarantees for artefact identification along the sensor chain?
  – even in the presence of failures of relevant subsystems?
  – can we ensure bounds on jitter?
  – can we detect intruders?
Wanted

a “provable” robust abstraction relation between the relevant real-world artifacts and the internal digital internal world model of each system:

whenever real-world artefact \( \text{a} \) is relevant:

\[ p(a) \text{ is true in real world at time } t \]

iff

with high probability \( p_\varepsilon(a) \text{ is true in our world model at time } t \pm \Delta \)
spoiling factors

• inherent limitations of different types of sensors
  – typically compensated by sensor fusion

• inherent limitations of object identification algorithms
  – either good in recognizing a if a is in real world
  – or good in recognizing that a is not present in real world

• jitter and unreliability along the complete chain from raw sensor data to digital world model
resulting research questions

• characterize “relevant”

• precise bounds on epsilon-delta along the complete chain from raw sensor data through sensor fusion through object recognition

• work with two world models
  – safe approximation of existence
  – safe approximation of non-existence

• how can humans help to resolve uncertainty

• how can control strategies be adapted to uncertainty
Resulting Research Questions

• can we derive along each step predicates characterizing allowed environments?
• can we provide environment assumptions for allowed queries to internal digital world model?
• Can we provide probabilistic guarantees for learning algorithms in allowed real-world contexts?
• Can we extend heuristic methods such as Hazop analysis to guide search for possibly relevant real-world artifacts (see code of practice from Prevent Project!)
Coping with changing environments II

• The model explicates for each actor and each service offered by the actor the assumptions on its environment under which it is offering this service
  – including degradation levels
  – including forbidden environments

• using contracts for service specification
  – service-level is guaranteed
  – under assumptions on its own health state
  – under assumptions on its environment
Coping with changing actors

- Dynamically changing health state
  - characterized by formal specification of current set of capabilities (maneuvering, transporting, controlling environment parameters, ...)

- Dynamically changing relations
  - who can talk to whom
  - who has authority over whom (to change roles, add/delete rights, change capabilities, ...)
  - who has to coordinate his actions with whom
  - what level of observation of what other actors (only interface, grey box view, white box view)
Challenges

• providing sufficiently precise characterizations of current health state

• assuring sufficient degrees of consistency of beliefs between actors
  – what communication and coordination structures, what levels of visibility, in which roles
  – define for each of this “sufficient”
  – assure sufficient degree of consistency
  – ensure that HMI design transports relevant parts of beliefs (consistency of belief between human and technical system)
Coping with hierarchical decentralized control in dynamically changing setting

SoS objectives vs actors objectives:

• determining required level of authority enforcing availability of sufficient joint capabilities

• determining required degrees of observation of health state and environment

• determining required degree of coordination
THE BLUEPRINT
The Blueprint

• An SoS $S = S(R, G, E, CS, B, C, R)$ is characterized by:

• *Roles*, $R$, a set of finite roles the system can assume, and a finite nondeterministic automata $A(R)$ describing the possible role transitions and conditions under which these may occur,

• *Goals*, $G$, representing for each role *what the system should do* when in a given role:
Goals

- A set of objectives given explicitly in terms of interface variables of the constituent systems and parameters and/or implicitly in terms of inequalities and/or logic formulae. They are ranked according to priorities.

- Goals can be represented by a number of mathematical formalisms such as a prioritized list of LTL formula, equalities and inequalities. They include assumptions, are typically timed and are often probabilistic.
The Blueprint II

- *Environment Model, E*, representing the assumptions on the external environment of the system *S* under which the system was designed to achieve its goals in a given role.

- A set, possibly empty, of *constituent systems*, *CS*.

- *Capabilities, C*, representing what the system can do in a given role.

- *Behavior, B*, the relationship binding the variables (inputs, outputs, states) describing how a system operates.
The Blueprint III

• A *Strategy* is the decision of a constituent system about its behavior chosen according to its environment model.

• *Relations, H*, defined on the constituent systems and roles of the System of Systems S.
  – Each relation can be represented as a directed graph. We propose the following set of relations in our conceptual model:
    • *COMMUNICATION, AUTHORITY, USE, OWNERSHIP, COORDINATION, OBSERVATION*
Relations

- **COMMUNICATION**: a communicates to c, i.e., a can send messages to c,
- **AUTHORITY**: a has authority over c, i.e., a can modify c, for example, by changing its role; typically an SoS exerts some kind of authority on its constituent systems by thus modifying their goals and capabilities, and thus dictating partially or fully their behaviors;
Relations (cont.)

• **USE**: \( a \) uses \( c \), i.e., \( a \) can use \( c \) by utilizing \( c \)'s current capabilities to satisfy its goals;

• **OWNERSHIP**: \( a \) owns \( c \), \( a \) can modify \( c \) and can grant **use** to a third party \( b \) over \( c \);

• **COORDINATION**: \( a \) coordinates with \( c \), i.e., \( a \) informs \( c \) of its (entire or partial) role, capabilities, and goals;
Relations (cont.)

• **OBSERVATION**: *a observes c*, i.e., *a* has access to (can measure) the external and/or to the internal variables describing the roles, goals, behaviors and capabilities of *c*;

• **KNOWLEDGE**: *a knows c*, i.e., *a* observes all variables of *c* and its constituent systems.
The Blueprint IV

- *Classes* of constituent systems are parameterized sets of constituent systems that share the same structure in terms of roles, environment models, goals, behaviors, capabilities, strategies, and relations. An *instance* of a class is a constituent system that differs from other systems in the class only in its parameter values.
The Blueprint V

• An element of the set CS may join or leave the set at any time;
• An element joining CS may differ from the present elements in behavior, goal, and capabilities. It can be a member of a new class or a new instance of an existing class.
• An element joins CS establishing relations with its peers. The relations can be already defined in the System of Systems and in that case, new connections may appear or disappear in the directed graph representing the relations, or be new, in that case new links in the graph are added with a different color.
The Blueprint VI

An SoS configuration is determined by

• knowledge of all existing classes of constituent systems
• knowledge of all existing instances of all existing classes of constituent systems
• current relation colored graph between all existing instances of all existing classes of constituent systems
• all the variables of constituent systems that can be observed by the SoS.
Towards Formalization

- semantics of agents can be described by probabilistic hybrid automata (PHA)
- environmental models can be described as dynamic parallel composition of PHA
- SoS can be described as dynamic parallel composition of particular PHA (including variables to model its beliefs) and dynamically changing graph structures with agents as nodes
- SoS objectives can be expressed in first-order probabilistic timed LTL
Conclusion

• The blueprint covers major risks observed in existing SoS
• The blueprint can be used as a reference in engineering SoS
• A complete formalization of the blueprint can be used as a basis for formal characterization of the emergent behavior and serve as “plant model” in designing hierarchical distributed control
• The blueprint itself must be a living document
BACKGROUND MATERIAL
Relevant Roadmaps Germany/EU

• National Roadmap on Embedded Systems
• Agenda CPS, acatec
• Drafts MASRIA Joint Undertaking ECSEL
• SRA ETP Artemis
• Automotive Roadmap Embedded Systems 2030
• Round Table Autonomous Driving
• Industrie 4.0