# SRA 2016 – Strategic Research Challenges

## Design Methods, Tools, Virtual Engineering

Jürgen Niehaus, SafeTRANS

# THE CHALLENGE

# As always….

- Embedded Systems and Cyber-Physical Systems
  - are becomming more and more complex
    - New functionality
    - Networked systems
    - Higher level of automation/autonomy
  - interact with (or comprise) physical environment
    - therefore safety critical
    - therefore analysis / V&V methods and tools needed
      - Matching current (and future) ‚complexity levels' of systems
      - beeing (cost-)efficient
        - » Large part of design costs go to V&V
  - make use of new technology (needing adapted/new (design/V&V/…methods&tools)
    - Multicore
    - new sensors
    - …
- Therefore we need more/better/more cost-efficient Design Methods and Tools

These ‚old' arguments are still valid

# But with CPS, it get‘s worse…

- Networked Systems
  - Security (resp. Security impact on Safety)
  - Cooperation, Coordination
    - of systems from different manufacturers
  - Handling uncertainty
    - Wrt. trustworthyness of ‚external information‘
- Increasing Level of Automation (up to Autonomy)
  - Explosive increase in possible system behaviour
    - The amount of testing needed to be even only ‚reasonable sure‘ of system‘s correctness is prohibitive
  - Complex decision making
    - Self Learning?
      - How to analyze such systems at all?
    - Ethics?
  - Handling uncertainty
    - Oberservation of environment is often incomplete

# … and worse

- Humans are integral part of the overall system
  - Human Machine Interaction
  - Human Machine Cooperation
  - Machine Adaptation to Human needs
- Long lifetime of systems
  - Need to cope with
    - New situations
    - new cooperations partners (with new capabilities)
    - new requirements
  - which were not even envisioned during design time…
  - (Also the other way around: Need to cope with legacy systems)

# Another set of challanges: Changes in development processes

- Multi-diciplinary design teams
- Physically distributed design teams
- Organizationally distributed design teams
  - … spanning more than one company
- Changes in OEM – Supplier relationships
  - From supplier chains to supplier nets
  - OEM not necessarily the (sole) integrator any more

- Need to adapt/enrich Design Methodology and have corresponding tool support

# Yet another set of Challenges: Where worlds collide…

- Consumer Electronics and Assistance Systems
  - Part of the same system, but
    - Different lifecycles / lifetimes
    - Feature interaction? Impact on Safety (and Security)?
    - Different possibilities for Upgrades/Changes/Evolutions
      - Apps for Assistance Systems?
- Embedded Systems and Internet / Cloud
  - Reliability / Trustworthyness (of information)
  - Quality of Service (latency, accuracy,…)
  - Security (who gets in and who stays out…)

# Overarching challenge

- How can we
  - design
  - do V&V for
- these kind of ‚beasts'
- such, that requirements on
  - Safety (and Security)
  - Real-Time behaviour
  - Cost Efficiency
  - …
- are met

Same question as before, but for a (more or less) completely new type of systems.

# HIGH LEVEL RESEARCH TOPICS

# High level topics I

- Model based design, including
  - multi-domain, multi-dimensional , and multi-objective specification and modelling
    - across application domains
    - across engineering domains
    - across supply chain
  - support for heterogeneous models
  - support for re-use of models
  - models for certification
  - support for an integrated safety and security development process

- Multi-Objective Optimization
  - For heterogeneous models
  - with multiple objectives from different application and engineering domains
  - across the supply chain

# High level topics II

- V&V - Verification and validation methodology and tools
  - Including formal verification, simulation, testing,…
  - for complex, extendable, upgradable and evolvable Cyber-Physical Systems
    - including on-line validation/verification
  - supporting
    - Incremental analysis and certification
    - Integration of heterogeneous models
    - Model-/software-/Hardware/system-in-theloop simulation and testing
  - able to handle
    - new functionality
    - uncertainty stemming from incomplete environment observations ans different levels of trust placed in external information
    - The dynamic behaviour of CPS
  - to establish properties like
    - Safety
    - Security
    - Real-time behaviour and quality of service
    - …

- Monitoring and Diagnosis in the field
  - Failure detection
  - Adaptation, fail-safe degradation
  - Self-Healing
  - Life-long ‚learning‘

# High level topics III

- Human Aspects
  - Human Machine Interaction
  - Human Machine Cooperation
  - Machine Adaptation to Human needs
- Pushing Open, horizontal Standards
  - Interoperability
  - Communication, Cooperation, Coordination
  - Test- resp. V&V Szenarios
- Build Eco-System for processes, methods and tools for the cost efficient design, analysis and test of safe and secure CPS based on standards, including the whole value chain

# Closely related topic in SRA: Cyber-Physical Systems of Systems

- Key features
  - Size and distribution
  - Distributed Control and Mangement
  - (Partial) autonomy of the constituent systems
  - Continuous evolution and dynamic reconfiguration
  - Emergent Behaviours

- Research Challenges
  - Decision structures and system architectures
  - Self-organisation, structure formation, and emerging behaviour in technical systems of systems
  - Real-time monitoring, exception handling, fault detection and mitigation of faults and degradation
  - Adaptation and integration of new components
  - Humans in the loop and collaborative decision making
  - Trust in large distributed systems.

ARTEMIS
Industry Association

# Thank you for your attention