EICOSE
European Institute for Complex Safety Critical Systems Engeneering

EICOSE

Transportation Roadmap 2010

Presentation for the ARTEMIS Summer Camp, Rome, 2010

About EICOSE

EICOSE
European Institute for Complex Safety Critical Systems Engeneering

- EICOSE – European Institute for Complex Safety Critical Systems Engineering
- Members:
  - Aerospace Valley (Pôle de Compétivité, France)
  - System@tic Paris-Region (Pôle de Compétivité, France)
  - SafeTRANS (Competence Cluster, Germany)

  } Funding members

  - Tecnalia (Competence Cluster, Spain)
  - AVL LIST (Company, Austria)
  - Strategic partnership to coordinate national and European R&D strategies
  - Awarded the ARTEMIS title: Center of Innovation Excellence (CoIE)
  - Responsibility: help to shape parts of the ARTEMIS SRA concerning processes and methods for complex safety critical systems in the transportation domain (Automotive, Aeronautics, Railways)

AVL tecnalia Corporación Tecnológica aerospace vallée valley SafeTRANS SAFETY IN TRANSPORTATION SYSTEMS SYSTEM@TIC PARIS-REGION

EICOSE – Way of working

EICOSE
European Institute for Complex Safety Critical Systems Engeneering

- Three theme-oriented Working Groups (WG)
  - WG 1: Methods and Processes for safety relevant embedded systems
  - WG 2: Computing environments for embedded systems
  - WG 3: Human-centred design of embedded systems

  - Results from WG are harmonised within E²GEST
    (EICOSE Expert Group on Embedded Systems for Transportation)
    → experts of EICOSE members and other members of ARTEMIS-IA

AVL tecnalia Corporación Tecnológica aerospace vallée valley SafeTRANS SAFETY IN TRANSPORTATION SYSTEMS SYSTEM@TIC PARIS-REGION

EICOSE Transportation Roadmap 2010 – Market Figures, Automotive

- European global share in the automotive market: 30%
- European turnover: 780 bn. €
- European employment:
  - Direct jobs: 2,3 mio.
  - Indirect jobs: 12 mio. (equivalent to 5,5% of European employment)
- Global vehicle park will grow about more than four times till 2035
- R&D investment in vehicle industry: about 24 bn. € (= 30% of European industrial R&D)
- Costs associated with embedded SW engineering in the automotive / transportation domain represents 51%
- SW R&D investment: Increase from 17 bn. € in 2002 till 45 bn. € in 2015 (= 35% of all R&D costs)
- Cost of electrics and electronics ~15 to ~30% of production cost, growing*

*Jean Botti, EADS: „ Automotive and Aerospace Electronics Similarities, differences, potential for synergies “. Keynote at ERTS² 2010, Toulouse, 19/05/2010

EICOSE Transportation Roadmap 2010
Market Figures, Aerospace

- European turnover: 94,5 bn. €
- Global market volume: 284 bn. €
- Europe is 2nd in market share worldwide:
  - 1. US: 51%
  - 2. Europe: 36%
  - 3. Canada: 6%
- European employment: 442,100 people
- R&D investment: 12% of turnover
- Forecast: till 2015, SW R&D will be doubled and account for at least 45% of all R&D investments
- Cost of electrics and electronics : ~20 (civilian) to ~50% of production cost, stable*

*Jean Botti, EADS: „ Automotive and Aerospace Electronics Similarities, differences, potential for synergies “. Keynote at ERTS² 2010, Toulouse, 19/05/2010

EICOSE Transportation Roadmap 2010 Market Figures, Rail

- European turnover: 122 bn. € out of which 85 bn.€ are accessible *
- European rail supply industry market share
  - in Europe: 80%
  - worldwide: 50%

- Expected annual growth rate: about 2.5%
- Rail Control systems represent 11% (approx. 9.6 bn.€) of overall rail market
  - Rail control systems include Train Control Systems, Computer based Interlocking, Traffic Control, communication
  - Rail control systems: 35% originates from Western Europe
  - This volume doesn't include systems for security, passenger information systems, ticketing
- Expected annual growth in rail control market: about 3.5% till 2016
- In 2015, the part of software R&D in railway sector is expected to represent 35% of the total R&D expenses.

*Figures from UNIFE Worldwide Rail Market study 2008

EICOSE Transportation Roadmap 2010 – General Objectives

- Societal Objectives:
  - Towards zero accidents
  - Towards zero emission / zero noise
  - Towards zero congestion
  - Sustainability
- Enabling Objectives
  - Always secure
  - Always on / always connected
  - Global awareness for quicker and safer and cleaner transport
  - From interaction to cooperation
  - Affordability

EICOSE Transportation Roadmap 2010 – Key Trends – Automotive

- E-Mobility
- AUTOSAR
- Required innovations:
  - production-ready development of innovative vehicle concepts based on embedded systems are required. These systems have to integrate sustainable concepts, like:
  - Energy recovery systems including electric energy storage like hybrid vehicles
  - Advanced propulsion systems with dedicated zero emission driving ability like electric and fuel-cell vehicle
  - Advanced driver assistant systems (e.g. adaptive cruise control and lane keeping) and safety systems (e.g. pre-crash, collision avoidance systems)
  - Vehicle-To-Vehicle and Vehicle-To-Infrastructure Communications Systems, enabling wireless broadcasting of traffic and other safety-relevant information

EICOSE Transportation Roadmap 2010 – Key Trends – Aerospace

- **New technologies and development acquisition**:
  - New networks
  - New processors (multi-core, systems on chips)
  - New architectures
- **New methods for development of systems and avionic products :**
  - Model Based Engineering
  - Distributed simulation in extended enterprise
  - Interfaces definition and management
  - Virtualization of platforms
- **Required innovations:**
  - Security: integration between Open World systems and safety critical systems preventing malevolent intrusions
  - Environmental impacts: Balance between energy consumption and production / control of operational behaviour of the vehicles and through noise active control systems
  - Cost of possession:
    - minimized by the use of integrated health monitoring systems and advanced air / ground communication allowing anticipation of corrective maintenance operations.
    - Improvement of reliability of systems by decrease the maintenance costs as well as improving the operational reliability
  - Comfort and operability of Aircrafts will be improved through suitable man machine interfaces.

EICOSE Transportation Roadmap 2010 – Key Trends – Rail

- European Railway Traffic Management System (ERTMS)
- Harmonisation and Cost Efficiency

- Required innovations:
  - Satisfy more physical (reduce volume...) and logical (applications) integration
  - Provide information in a context of intelligent mobility in ubiquitous environment
  - Process / Method / Tools allowing better re-use and reduction of certification cost (modular safety case for example)
  - Reduce effort on Interoperability from definition phase to testing phase
  - Better abstraction from implementation on communication and data distribution systems
  - Security

EICOSE Transportation Roadmap 2010 – Key Trends – Cross domain fertilistaion

- **Process and tools: Methods for developing systems have to support the different drivers:**
  - Techniques like viewpoints based methods are a trends already in place in the defence domain for example (DODAF)
  - Tight coupling between the different specialities (from system to chip)
  - Integration of formal and non formal techniques
  - Common meta models; models or patterns from system to certification
- **Technology has to:**
  - Support high level integrations
  - Offer scalable processing capabilities (scalable in term of processing power but also in term of type of type of processing: general processing, signal processing, i/o processing)
  - Provide safety related mechanisms
  - Support communication and information management systems
- **Mecatronic is a relevant field for synergies between domains**

AVL tecnalia Corporación Tecnológica aerospace vallée valley SafeTRANS SAFETY IN TRANSPORTATION SYSTEMS SYSTEM@TIC PARIS-REGION

Automotive and Aerospace Electronics
Potential Areas of Cooperation, I

- **Safety critical systems: aerospace safety at automotive cost**
  - Dependable architecture
  - Design, simulation and test tools
    - Standards (Integrated Modular Architecture, Autosar …)
    - Formal proof
    - Automatic coding
    - Certifiable tools
  - Goals: automotive: become “certifiable” and introduce new functions (X by Wire, chassis control…), aerospace: reduce cost
- **Power distribution**
  - Global trend towards “more electrical systems”
    - Fuel economy & greenhouse gas reduction
    - Weight reduction
    - Maintenance reduction
  - Dependable power distribution architecture principles, power network quality rules, energy storage
  - Design, simulation & test tools, especially for harnesses and EMC
  - Common goals: save design time & costs, better efficiency
  - No real common actions as of today

*Jean Botti, EADS: „ Automotive and Aerospace Electronics Similarities, differences, potential for synergies “. Keynote at ERTS² 2010, Toulouse, 19/05/2010

Automotive and Aerospace Electronics
Potential Areas of Cooperation, II

- **Diagnostics**
  - Goal: predictive maintenance is key to reduce down time
  - Potential collaboration on
    - Diagnostics principles
    - Data handling, storage, on-line and off-line processing
    - Human Machine Interface for diagnostics
- **Modelling, simulation and testing of complex systems**
  - Goal: save development, testing & tooling costs
  - Virtual product engineering
  - Hardware in the loop
  - Methods and tools
    - Most problems are very similar
    - Common tools

*Jean Botti, EADS: „ Automotive and Aerospace Electronics Similarities, differences, potential for synergies “. Keynote at ERTS² 2010, Toulouse, 19/05/2010

Automotive and Aerospace Electronics Potential Areas of Cooperation, III

- **Driver / pilot assistance**
  - Human workload management : different workloads acceptable by automotive and aerospace, but common problems
    - Acquisition, extraction, computation, distribution, presentation of relevant data
    - HMI principles (standards ?)
    - Haptic feedbacks

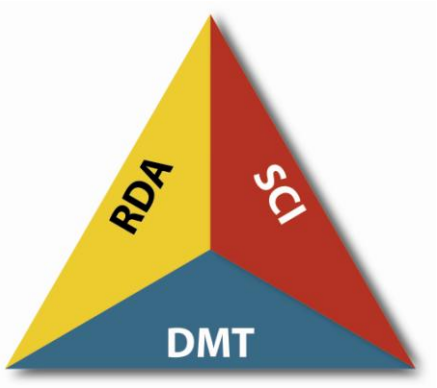
- **Data networks (field bus)**
  - Goal: standardized field bus to reduce the number of networks used to get better component prices, the numbers of tools and the investment in people training
  - Physical layers: look for a small number of common physical layers
  - Protocols: look for common protocols, especially for secure applications

- **Wireless**
  - Reducing wiring while enabling networked sensors clusters
  - In vehicle and vehicle to infrastructure communications
  - Common future standards

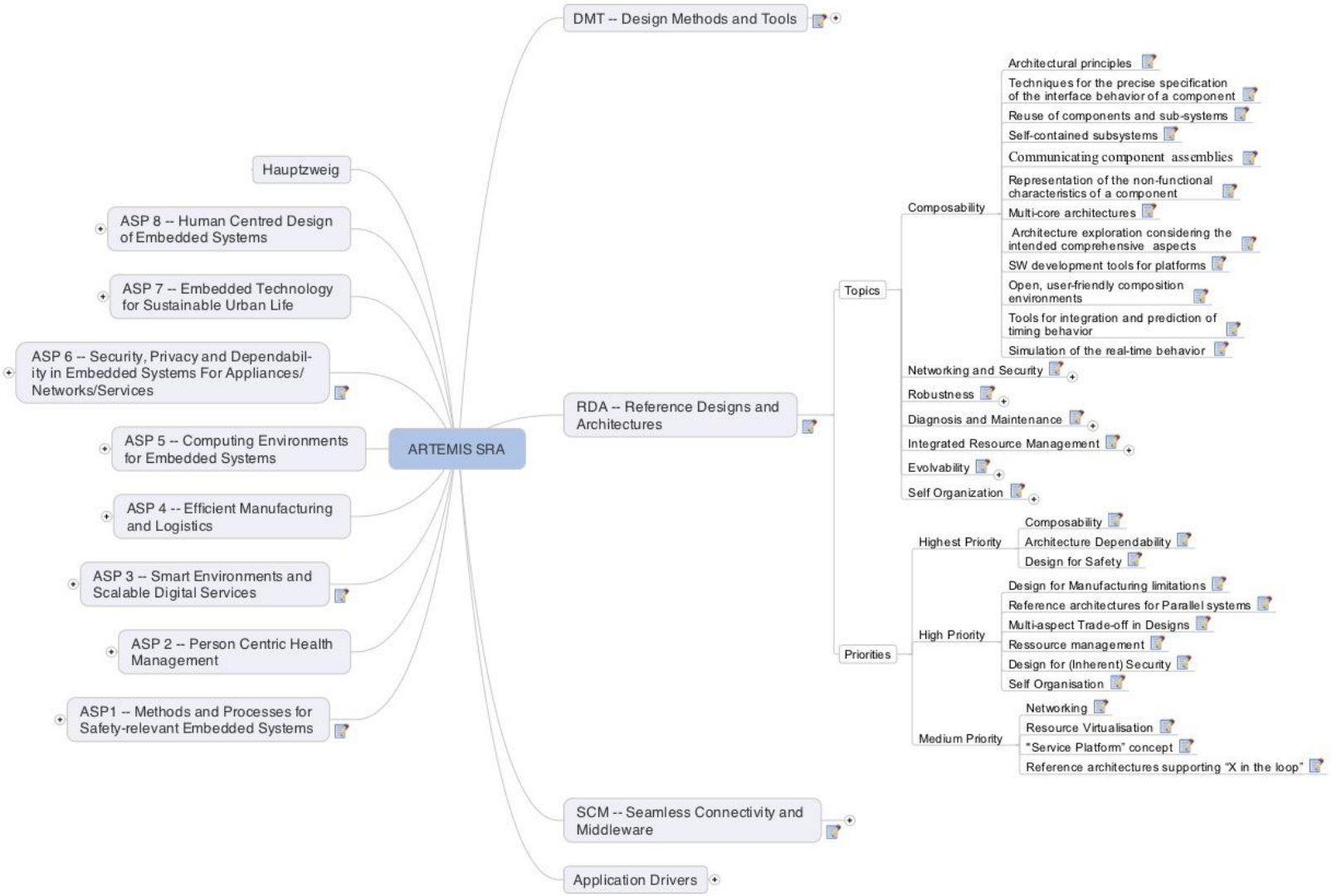
*Jean Botti, EADS: „ Automotive and Aerospace Electronics Similarities, differences, potential for synergies “. Keynote at ERTS² 2010, Toulouse, 19/05/2010

EICOSE – R&D Priorities

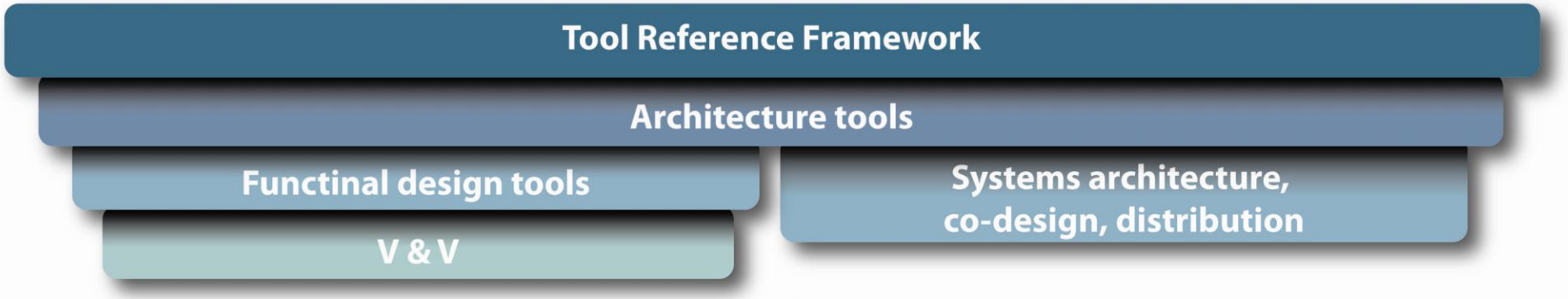
- Yearly update research topics (EICOSE Priority List)
- Defined by E²GEST
- Aligned with ARTEMIS SRA and AWP, RA
  - "horizontal components":
    - **RDA (Reference Design and Architecture)**
    - **SCI (Seamless Connectivity and Interoperability)**
    - **DMT (Design Methods and Tools)**



EICOSE basis for delta analysis



EICOSE delta analysis for ARTEMIS SRA:
DMT



- [...]
- Composable V & V technologies
- Product line verification

- [...]
- Verification of non-functional requirements
- Design to cost
- Optimisation against multiple constraints, perform trade-off analysis for multiple viewpoints
- Progress from engineering judgment architecture solution to guided architecture solution
- Technologies for maintaining trade-off justification and enabling long term evolution of systems architecture
- Formalized and systematic architecture exploration with respect to variability management and product lines

EICOSE delta analysis for ARTEMIS SRA: DMT

Tool Reference Framework

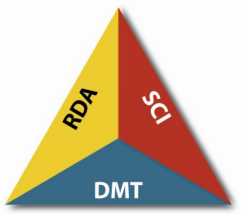
Transversal tools

Certification, safety planning

- [...]
- Design for Dependability
- Proof of Segregation between critical and non-critical functions
- Similarity Analysis

Requirements and Traceability Management & Configuration Management, Methodology & Life Cycle Management

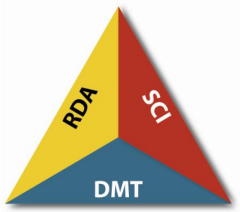
- [...]
- Elicitation of requirements
- Methods and tools for supporting domain analysis and product variability definition
- Requirements formalisation
- Requirements allocation, trade-offs - Allocation of product requirements to functions
- Methods for enhancing soundness and completeness of requirement sets
- Method and Tools for assessing dependability requirements
- Method and Tools for assessing industrial requirements (cost, etc.)
- Ensuring traceability between requirements and modeling elements
- Ensure seamless, complete and understandable requirements propagation across the supply chain



EICOSE delta analysis for ARTEMIS SRA: DMT

End-to-end process optimisation

- [...]
- Technologies for sharing potential between multiple related product lines
- Contract based engineering and reasoning
- Composition/modification operations
- Certification evidences
- Methods and tools for automatic generation of connectors
- Methods and tools for ensuring that middleware services support extra-functional requirements
- Trade-off analysis between component complexity and architecture complexity
- Technologies for improving adaptability of components to various deployment contexts



EICOSE delta analysis for ARTEMIS SRA: DMT

Tool Reference Framework

Transversal tools

- [...]
- Large scale cross domain tool interoperability

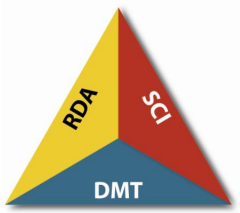
Tool integration framework

- [...]
- Legacy integration, data migration, long term data retention, reverse engineering

Integration tools

Systems integration and testing

- [...]
- Systems interfaces management
- Interface checking
- Signal data bases
- Data models
- Collaborative processes
- Ontologies
- Interoperability standards
- Standard formats for exchange for signals (physical level)
- Testability technologies breakthrough



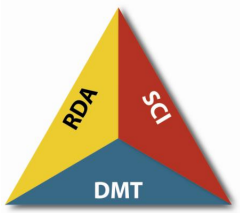
EICOSE delta analysis for ARTEMIS SRA: SCI

Ressource Management

- [...]
- Support for deterministic behaviour
- Energy management (including degraded mode)
- Resource management and virtualisation
- Energy harvesting in the sensor network

Robustness & support for diagnosis

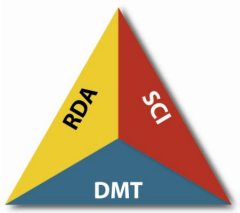
- [...]
- Fault isolation/containment
- Support for diagnosis
- Methodology for verification/qualification of complex components including COTS



EICOSE delta analysis for ARTEMIS SRA: SCI

System Organisation & deployment

- [...]
- Reconfiguration (static, dynamic, incl. multi process or multi core, redundancy management)
- New communication concepts wrt. reconfigurability, robustness, security
- Changing topology, network management, service discovery
- Collaborative algorithms
- Semantic services



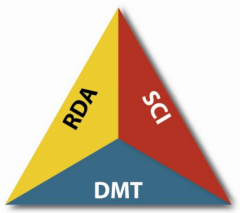
EICOSE delta analysis for ARTEMIS SRA:
SCI

Global connectivity

- [...]
- Access layers (wireless, optical, etc.)

Security

- [...]
- Security (as a safety issue)
- Dependability, security



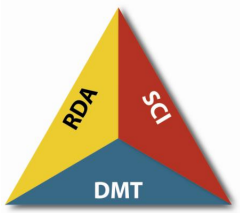
EICOSE delta analysis for ARTEMIS SRA: RDA

Architectural exploration

- [...]
- Impact on sustainability
- Impact on emergent properties of non-functional characteristics
- Methods, techniques and tools that allow for making design trade-offs between aspects of evolvability and system properties, such as cost and robustness

Multi-core

- [...]
- Extending design environments to support multi-core architectures (including compilation, Run-time infrastructure, simulation, analysis, configurability wrt number of cores, ...)
- Supporting certification / safety assessment for multi-core architectures



EICOSE delta analysis for ARTEMIS SRA: RDA

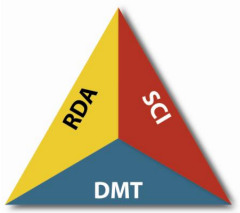
Evolvability

Supporting product line design

- [...]
- Tradeoff analysis between optimisation for product line design and optimisation of product instances
- Evolvement of product line over time

Composability

- [...]
- Co-simulation and co-analysis across multiple technical domains (electronics, mechanical, hydraulic)
- Simulation-based analysis of emergent properties of component based designs
- Analysis methods for emergent properties of component based design
- Including dynamically networked systems (each system viewed as „component“)



EICOSE delta analysis for ARTEMIS SRA: RDA

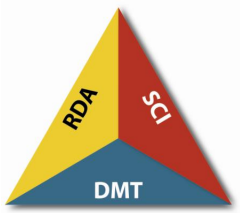
Robustness

Architectural patterns supporting robust distributed control

- [...]
- Allowing mode dependent tuning of communication characteristics such as jitter and latency
- Supporting prediction and analysis of stability and safety requirements on control loops
- Supporting diagnosis of distributed control loops

Robustness

- [...]
- Analysis method to verify the claimed assurance level of trusted embedded environments
- Increasing Robustness in degraded modes including situation where a security attack were successful



EICOSE delta analysis for ARTEMIS SRA: RDA

Networking and Security

- [...]
- Automatic security management of trusted embedded environments considering the limited resources of embedded nodes under hard real-time constraints in highly dynamic situations (new)
- Analysis methods to verify the claimed assurance level of trusted embedded environments

Diagnosis and Maintainability

- [...]
- Exploiting inverse control for improved diagnosis

Contact information

www.eicose.eu

info@eicose.eu

- Aerospace Valley: louis-claude.vrignaud@continental-corporation.com
- SafeTRANS: werner.damm@safetrans-de.org
- System@tic: jean-noel.patillon@cea.fr