European Commission FP7
ICT-2011.1.4 Trustworthy ICT
Project #318772
2012 – 2015

Contract-Based Verification of MILS-AADL Models

Stefano Tonetta
FBK-irst
tonettas@fbk.eu

D-MILS Project

- Research based on the MILS approach
  - Component-based approach for the construction, assurance, and certification of critical systems
  - Two-phase design process
    1. Architecture-based design of the information flow policy
    2. Implementation based on a platform composed of MILS foundational components
- D-MILS focused on:
  - Extending the technology to distributed systems
  - Providing an end-to-end support to
    - Design and verification
    - Deployment
    - Assurance case

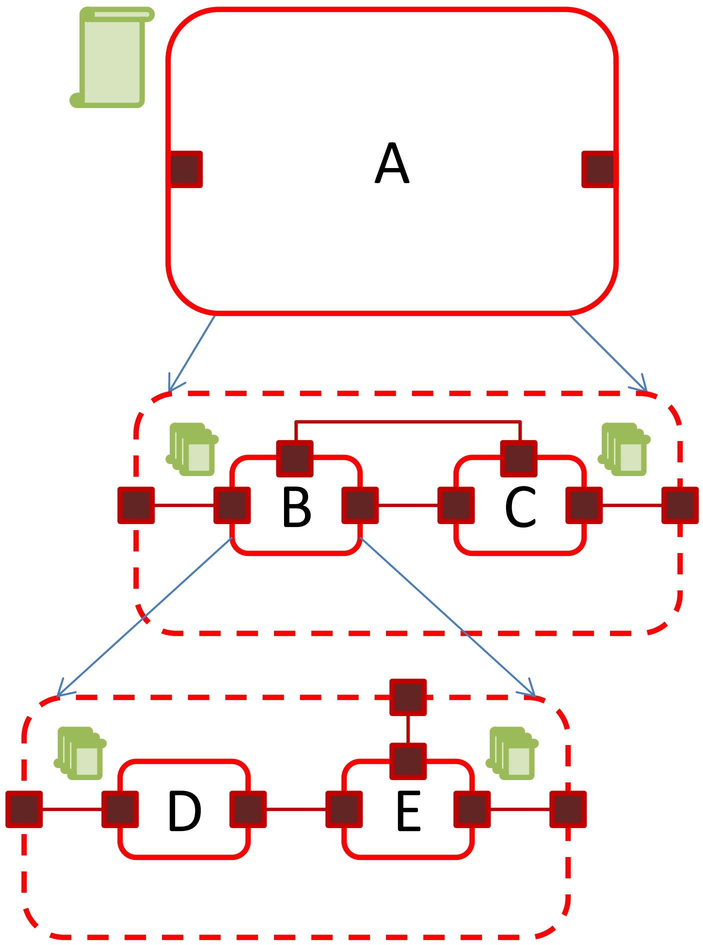
- FP7 project
- Nov. 2012-Oct. 2015
- Partners (underlined ones are present today):
  - The Open Group (UK) Lead
  - Fondazione Bruno Kessler (IT)
  - fortiss (DE)
  - Frequentis (AT)
  - LynuxWorks (FR)
  - RWTH Aachen University (DE)
  - TTTech (AT)
  - Université Joseph Fourier (FR)
  - University of York (UK)

FIRST USAGE OF COMPASS IN A NON-ESA PROJECT

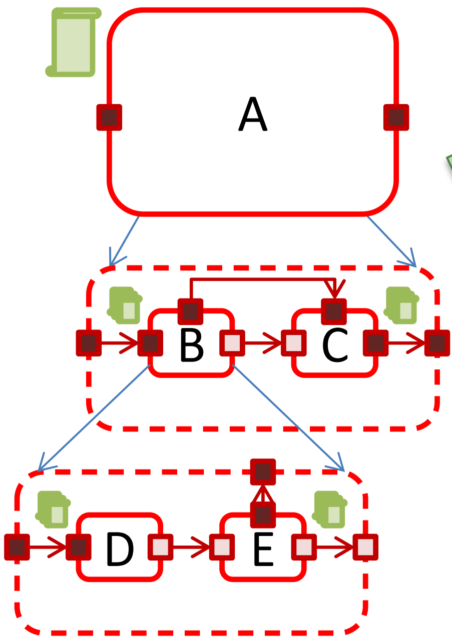
Verification goals

- Compositional verification
  - Prove that global properties are correctly refined by local properties
  - Efficient reasoning
  - Delegate proof of application components to the provider
  - Focus on the verification of the architecture
  - Formalize assumptions of system and components
- Cover different types of requirements:
  - Functional
  - Real-time
  - Safety
  - Security
- Efficient verification, effectively mixing
  - SMT-based symbolic model checking
  - Inductive reasoning
  - Automated abstraction refinement

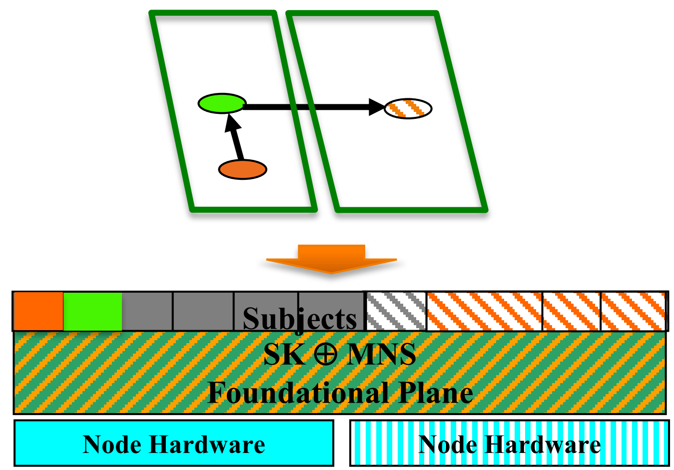
Contract-Based Design



MILS and CBD



$$\cfrac{\cfrac{\cfrac{\cfrac{\mathrm{D} \models P_{\mathrm{D}}, \mathrm{E} \models P_{\mathrm{E}}}{\gamma_B(D,E) \models \gamma_B(P_{\mathrm{D}},P_{\mathrm{E}})} \quad \gamma_B(P_{\mathrm{D}},P_{\mathrm{E}}) \models P_{\mathrm{B}}}{\mathrm{B} \models P_{\mathrm{B}}} \quad \mathrm{C} \models P_{\mathrm{C}}}{\gamma_A(B,C) \models \gamma_A(P_{\mathrm{B}},P_{\mathrm{C}})} \quad \gamma_A(P_1,P_2) \models P}{\mathrm{A} \models P}$$



AADL annotated with OCRA contracts

```
system Sys
 features
  cmd: in event data port int;
  switch_to_high: in event port;
  switch_to_low: in event port;
  return: out event data port int;
  outL: out data port int;
  { OCRA: CONTRACT secure
     assume: always (
           ({cmd} implies then ({return} releases (not ({cmd or switch_to_high or switch_to_low}))))
           and (((not {switch_to_high}) since {switch_to_low}) implies (not {is_high(last_data(cmd))}))
           and ({is_high(0)} = false) );
     guarantee: always ( ({is_high(outL)}=false));
  }
```

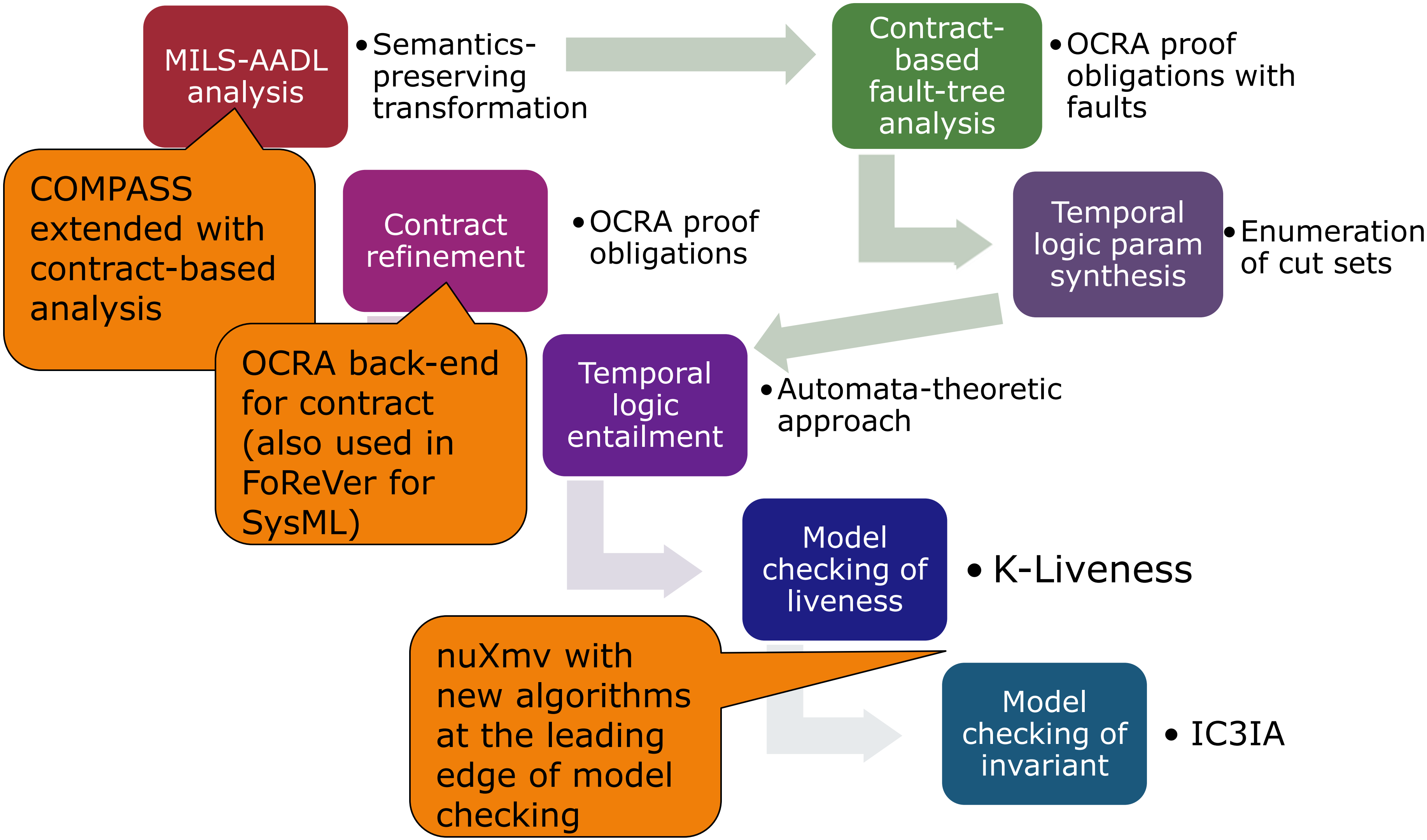
Property Specification Language

- LTL
  - always (p implies in the future q)
- First-order
  - always (high(value) iff high(cmd)) implies never (high(output))
- Real-time
  - always (corrupted(memory) implies time_until(alarm)<=time_bound)

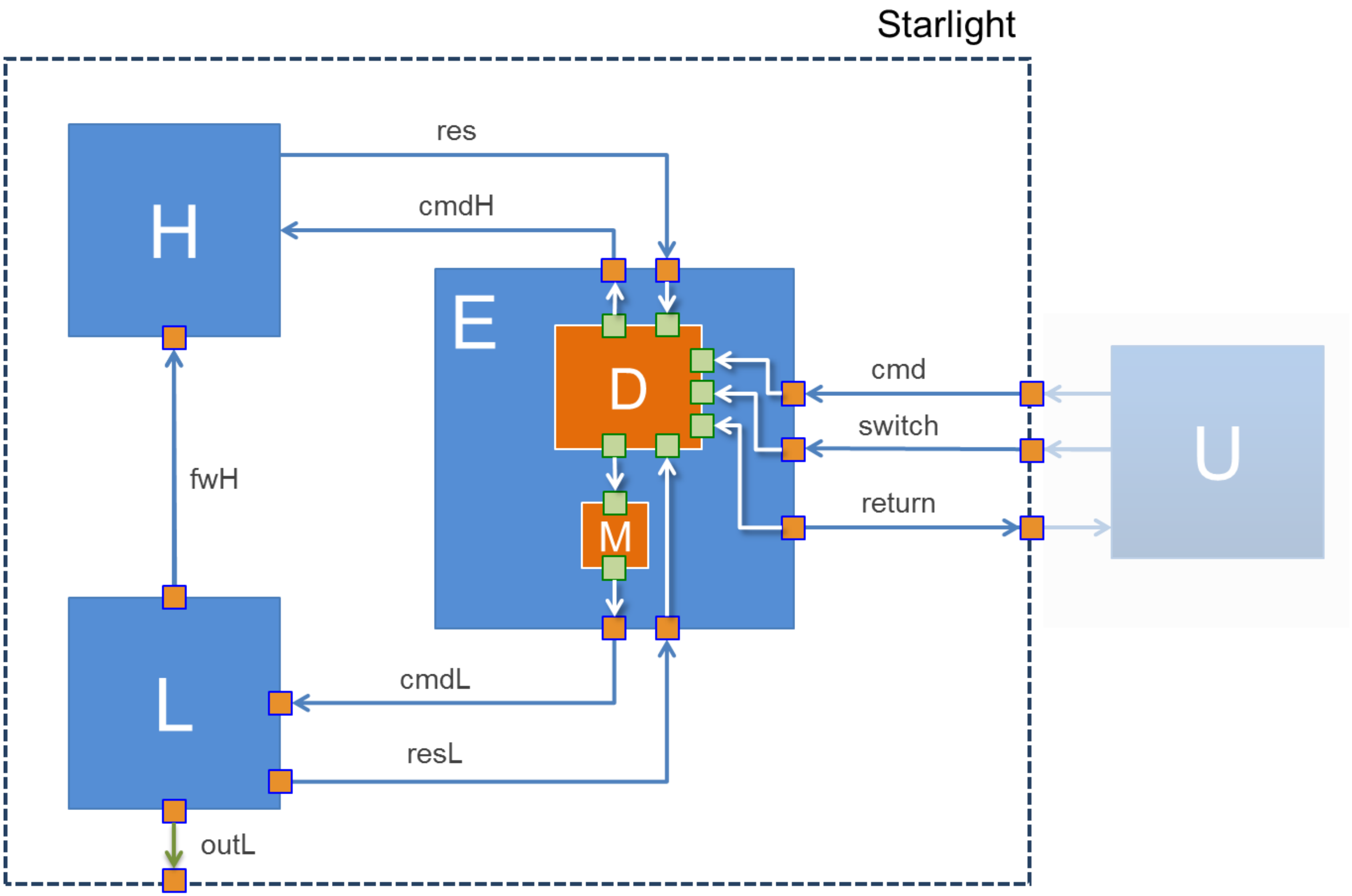
Verification Framework

- The framework consists of a collection of tools
  - COMPASS (baseline developed in ESA projects) as front-end for MILS-AADL models
  - OCRA for contract-based
  - nuXmv for model checking
  - xSAP for safey analysis (e.g. FTA)
  - secureBIP for transitive non-interference
  - RT-DFinder for invariant and deadlock checking
- Validation with
  - Simulation
  - Deadlock checking
  - Timelock checking
  - Reachability and other queries in temporal logic
- Verification of
  - Functional requirements
  - Real-time requirements
  - Security requirements
  - Safety requirements

Analysis Tool Chain



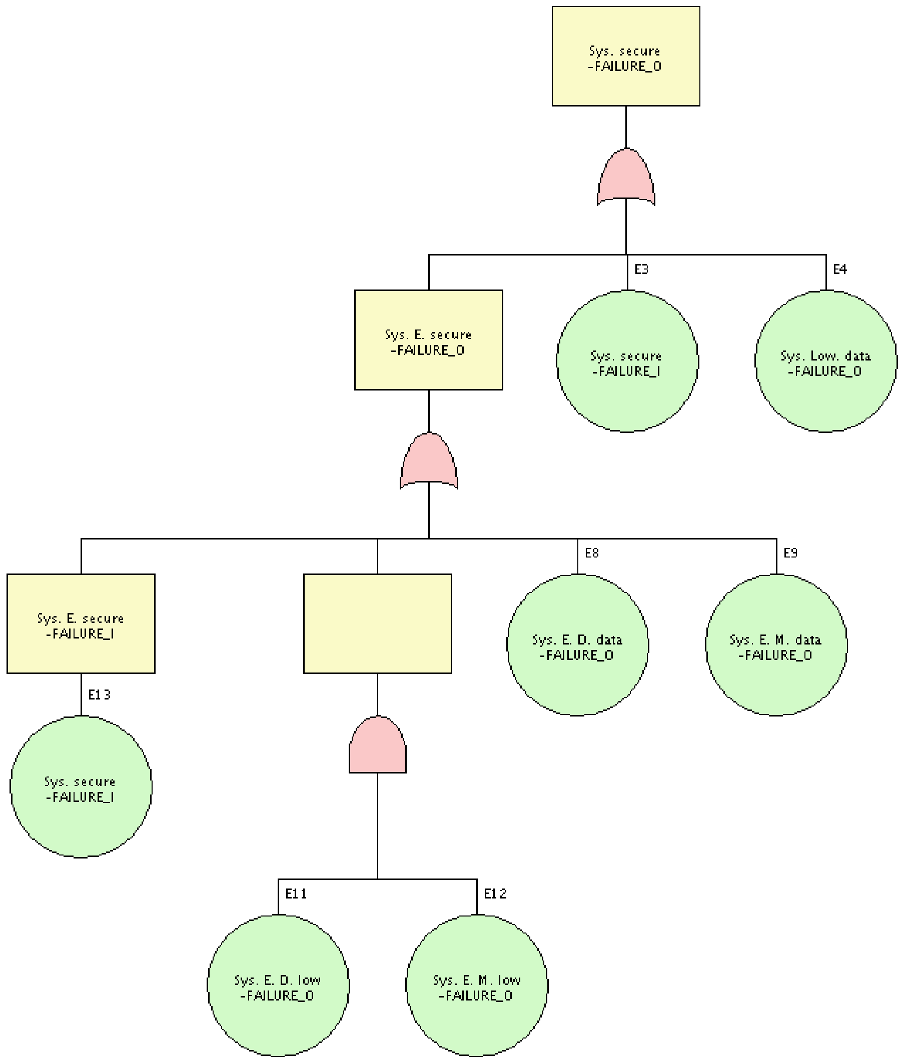
Starlight Architecture



Starlight reqs formalization

- Req-Sys-secure: No high-level data shall be sent by L to the external world.
  - Formal-Sys-secure: never is_high(last_data(outL))
- Req-User-secure: The user shall switch the dispatcher to high before entering high-level data.
  - Formal-User-secure: always ((is_high(last_data(cmd))) implies ((not switch_to_low) since switch_to_high))
- Proved system guarantess Formal-Sys-secure assuming Formal-User-secure.
- Req-Sys-safe: No single failure shall cause a loss of Req-Sys-secure.

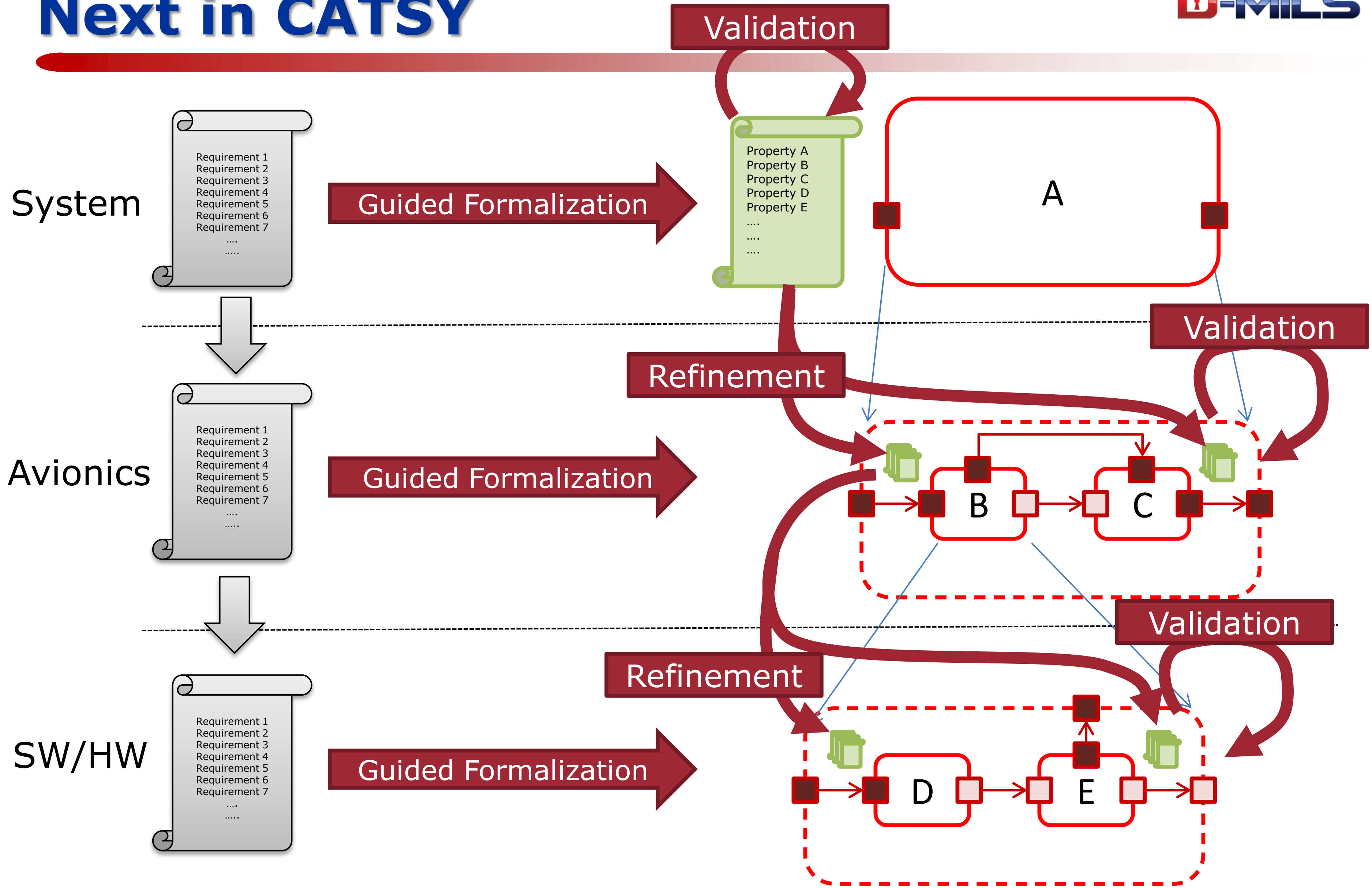
Starlight fault tree for secure req



Conclusions

- COMPASS used in a non-ESA project
- MILS-AADL (a variant of SLIM) models annotated with OCRA contracts
- Efficient analysis tool chain for scalable verification on very expressive logic
- Verification applied to both safety and security requirements.

Next in CATSY



Next in CATSY

- Guided formalization based on CSSP
  - Taxonomy of requirements and
  - Formal property patterns
  - Specific patterns for low-level properties (deadline, monitoring frequency, threshold, …)
- Validation of the formalization with
  - Queries to test the formalization
  - Traces to show possible executions
  - Explanation/debugging of the refinement
- Language tailored to property and contract specification
  - Abstract components
    - No required implementation
    - No required hw bindings
  - Mode transitions only for component configuration (behaviors only in the leaf components)
  - Simpler semantics of interaction
- Paving the way to higher TRL
  - New code repository management
  - Improve testing framework