WP6: System Qualification and Certification
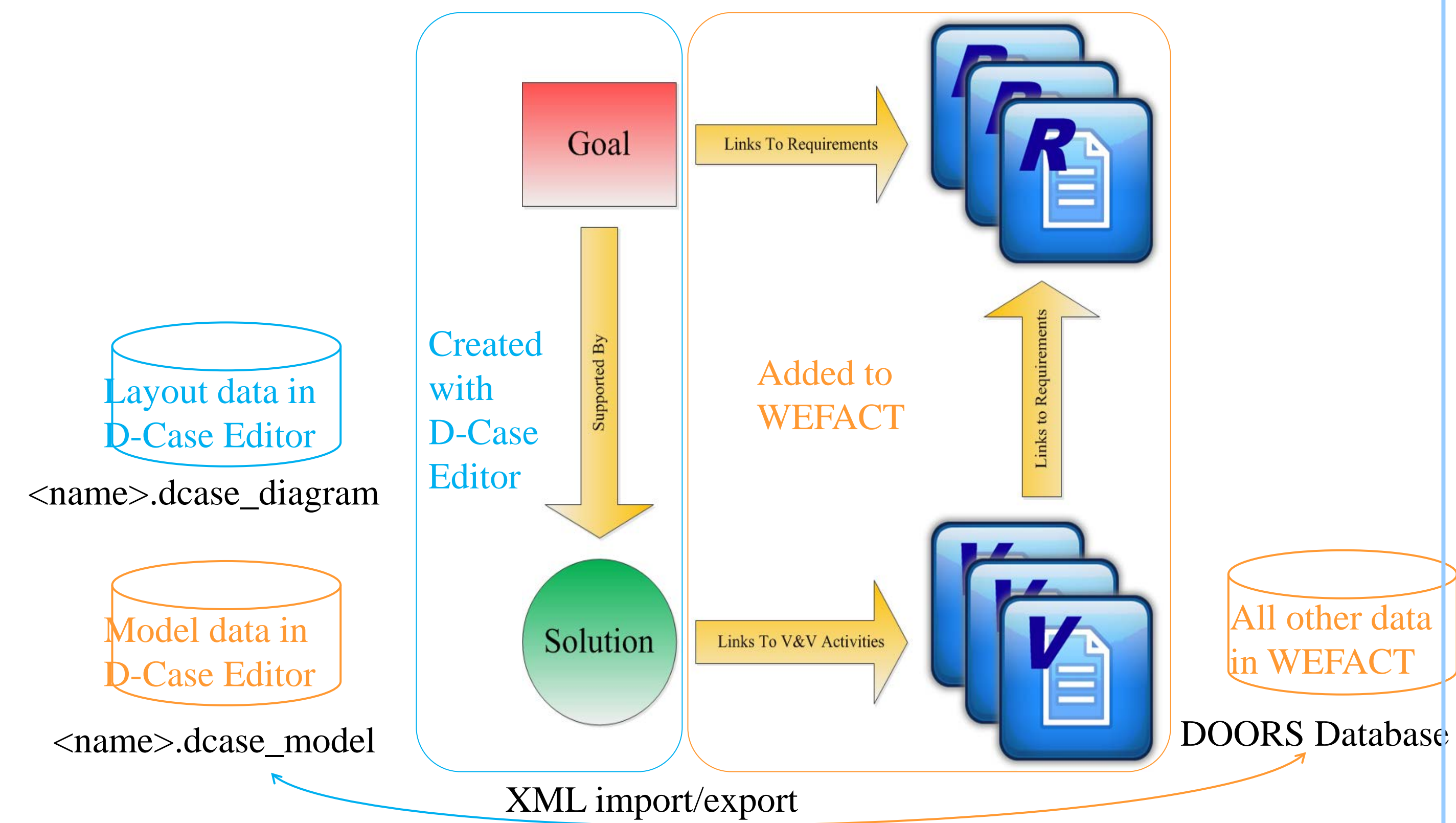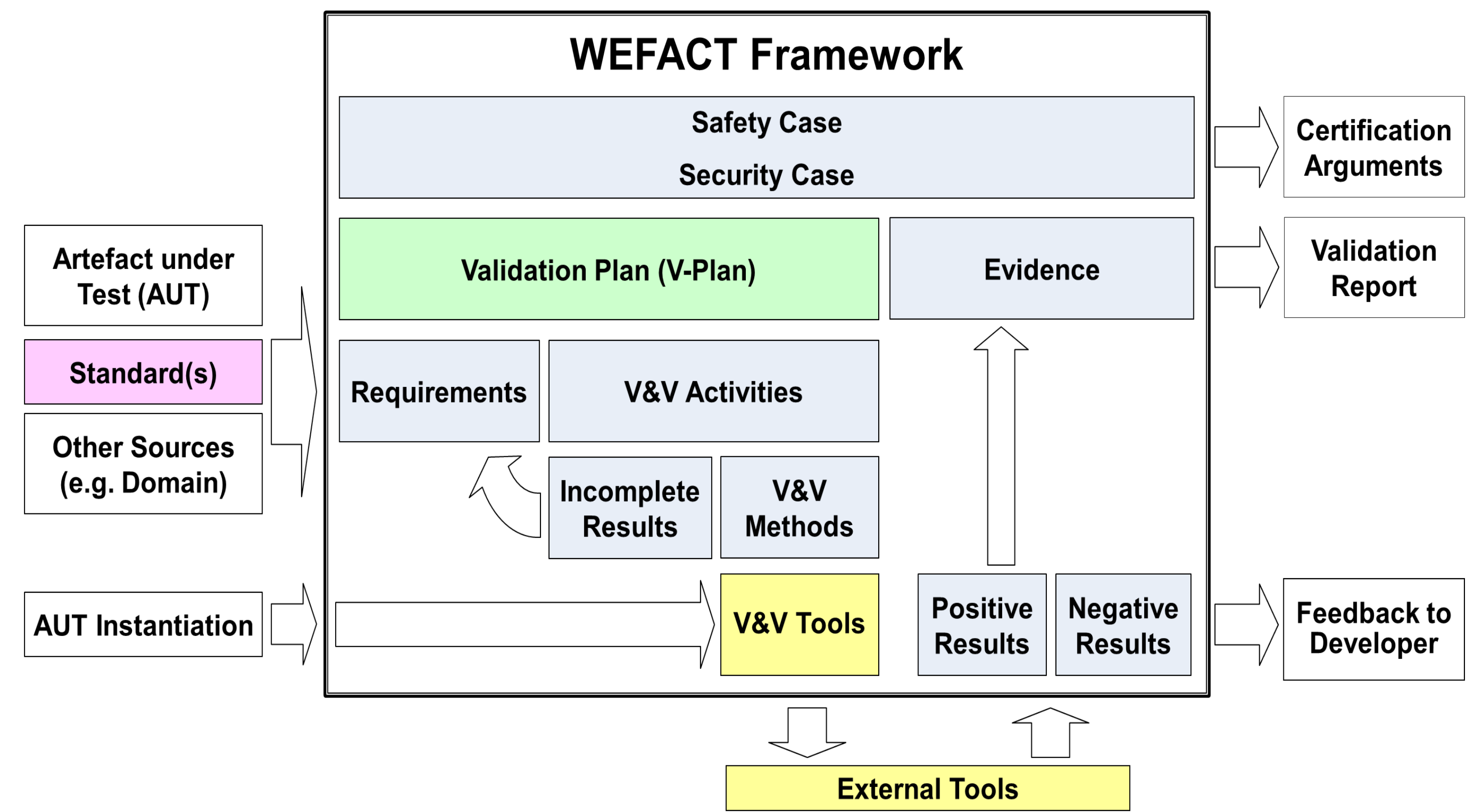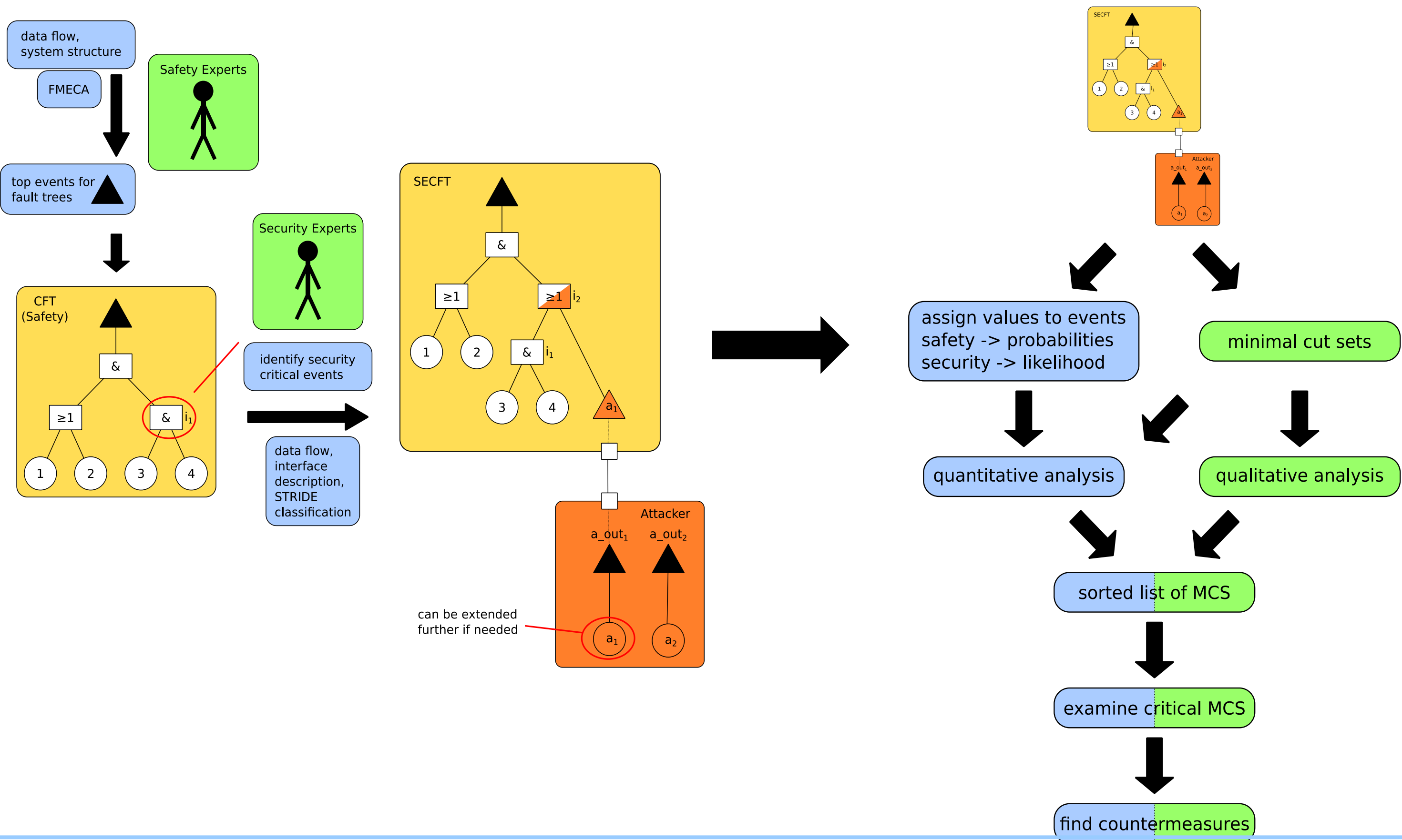
EMC²

ARTEMIS

WEFACT: Safety & Security Assurance @ Design Time

- Traceability from claims to requirements to evidence
- Integration / interaction of D-Case Editor with WEFACT
- Building a Dependability Assurance Case

Safety & Security Co-Analysis with CFTs

- Enhance CFTs by adding basic events representing security concerns
- Qualitative & quantitative analyses

Certification of Safety and Security in Cyber-Physical Systems @ Run-time

- Safety critical open adaptive system cooperate to provide functionalities not achievable by a single system
- However, the overall constituents and configuration of a (super-)system cannot be assessed a-priori at development time
- Solution: shift parts of the safety certification activities into runtime, and perform automated safety checks for dynamic systems integration and adaptation
- ConSerts: modular conditional certificates that are issued at development time for each system
- Investigating support for security assurance between safety critical open systems
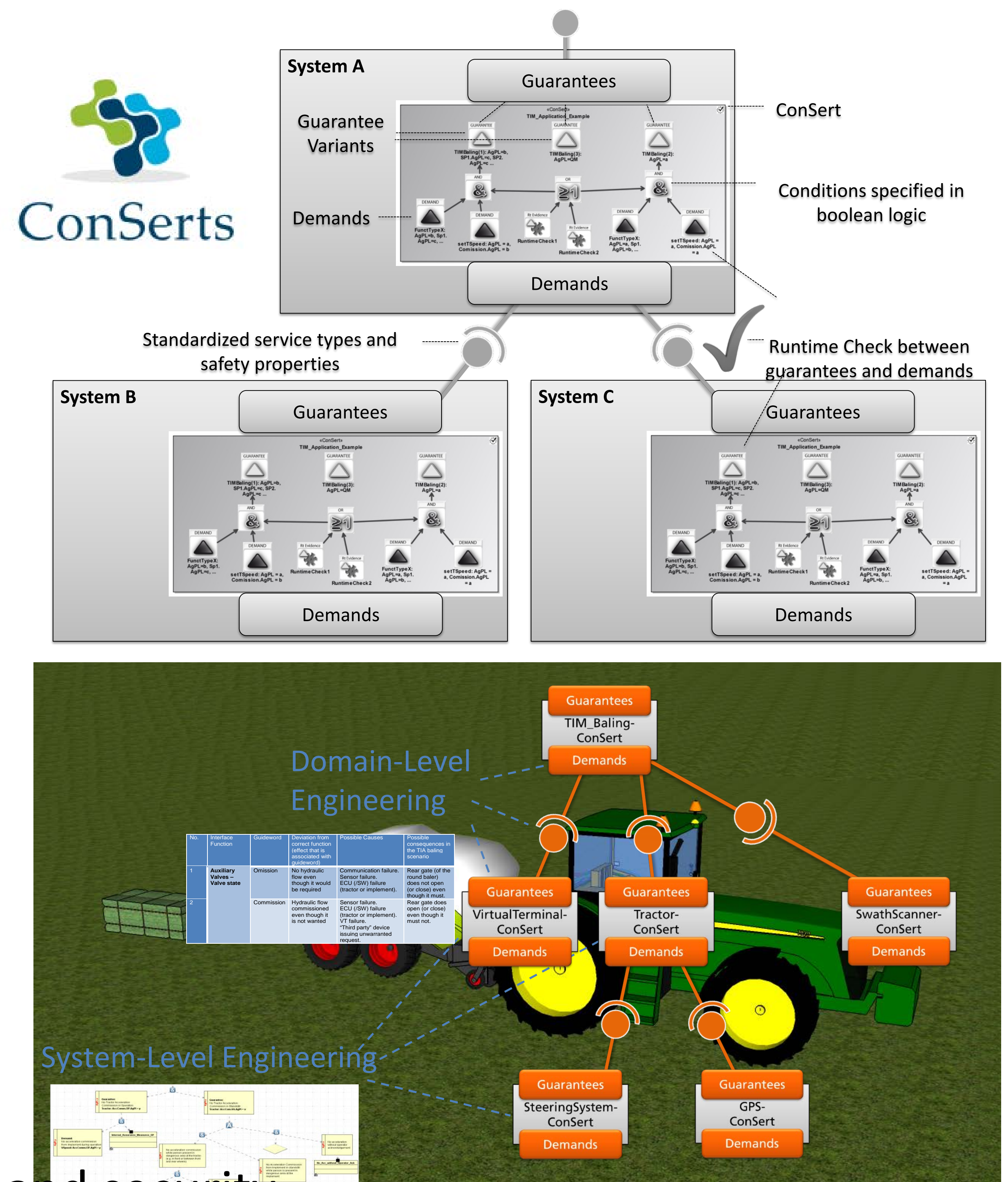
Active Contribution to Standardization: Cybersecurity & Safety Co-ordination

- IEC TC65 AHG1 – Framework toward coordinating safety and security
- IEC SC65A MT IEC 61508-3 – Preparing IEC 61508 Ed. 3.0, Task Group
- ISO TC22 SC32 WG08 – Cybersecurity & Safety Task Group