Safety Critical Design Process (& ISO 26262)

Chair:
Igor Mezic, UCSB

Contributors:

Notes:
Matt Boesch, Ford

Dionisio De Niz, SEI
Phil Koopman, CMU
Levasseur Tellis, Ford, Active Safety
Prashant Ramachandra, Toyota
Gopal Raghav, LMS North America branch of Belgium MBSE Company
Lee Pike, Galois Inc.
Graham Hellestrand, EST
Prasad Sistla,Univ of Ill, Chicago
Art Carter, NHTSA
Joe D'Ambrosio, GM

Research Challenges

- Emergence: Competing (safety) goals of separately safe systems. E.g. ACC wants to speed up as the car ahead speeds up to avoid a merging vehicle, but a collision avoidance wants to slow down.

- Non-deterministic behavior - how do we learn from components and analyze/compose them?

- Requirements Analysis - In combinations of separately developed subsystems, how do we identify and handle conflicting and/or missing requirements, prior to integration level testing?

- ISO26262 is a functional safety (electrical/software) reference, but insufficient for total system safety. ISO is a quality office issue. How do we track the safety aspects beyond the scope of ISO-26262?

State of the Art …

FMEA, Concept FMEA (inductive, like a top-down FTA), Design FMEA (deductive, after a design is complete).

USTAG required ISO26262 standard to include ***functional interaction failures*** (emergent properties). This modified the original definition of safety analysis from component failure to unsafe malfunction.

VDA EGAS – German developed standard for throttle by wire, asymmetrical CPU hardware monitoring (enhanced watchdog).

Formal methods - inefficient for large scale systems

… State of the Art

Tools for system safety analysis (e.g. formal methods) are not commonly in use by all engineers.

Integrity monitoring is useful to safety

Simulink/Stateflow is platform dependent and cannot verify timing.

Learn over time & retrofit (e.g. FAA).

Recommendations for Institutions & Cross-Institutional Collaboration

1. Promising Opportunities for Research

3-5 Years

1. Theories of Monitorability is an area to develop. Safety specification of the monitor, is the system predictable, observable? What about in the presence of noise?

2. Timing needs to be part of the V & V. Realtime guarantees of deliveries of packets for sensor – extend this approach to the safety system and analysis.

Recommendations for Institutions & Cross-Institutional Collaboration…

… Promising Opportunities for Research

10 Years

1. Integration of different safety methods, tools, approaches.

2. Integration of analyses, top-down (new functions) and bottom-up (legacy components, new components)

20 Years

Emergence: Competing (safety) goals of separately safe systems. E.g. ACC wants to speed up as the car ahead speeds up to avoid a merging vehicle, but a collision avoidance wants to slow down.

…***Recommendations for Institutions & Cross-Institutional Collaboration***

2. Education Based Recommendations

CPS needs cross-disciplinary curricula inclusive of safety.

MechE's/ElecE's don't appreciate software safety sufficiently. This leads to process failures if safety is put off until the end when it is too late to make big changes.

We need to be able to find trained safety engineers. Can there be a degree program developed?