IVHM Integrity Assurance
Verification and Validation

Technical POC

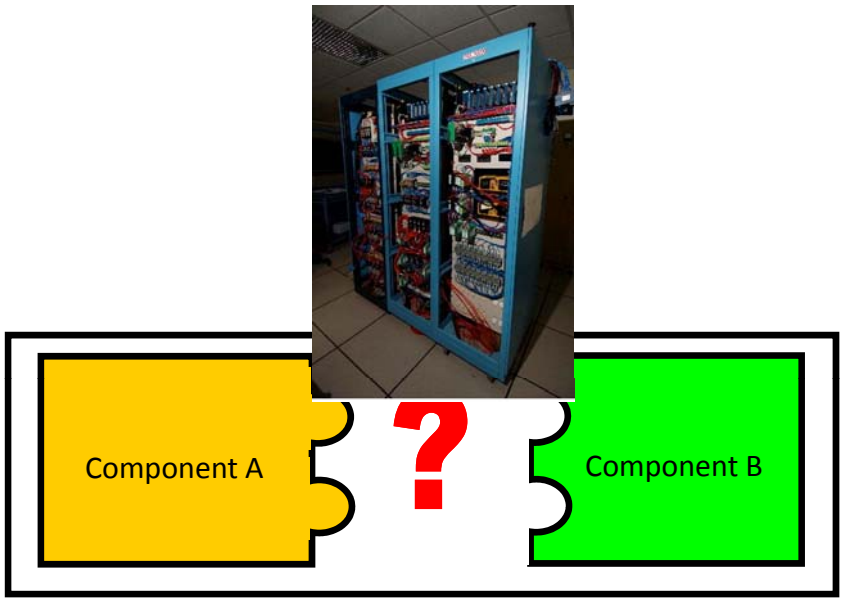
Dr. Guillaume Brat

CMU

Overview

- We will develop processes, underlying methods and tools to provide a comprehensive approach to verification and validation (V&V) that will ensure safe and reliable application of IVHM technologies to civil aviation.
- We will use modularity to decompose complex problems in smaller and manageable problems and then merge these solutions to enable greater integrity and scalable verification and validation.

IVHM Integrity Assurance



Objectives

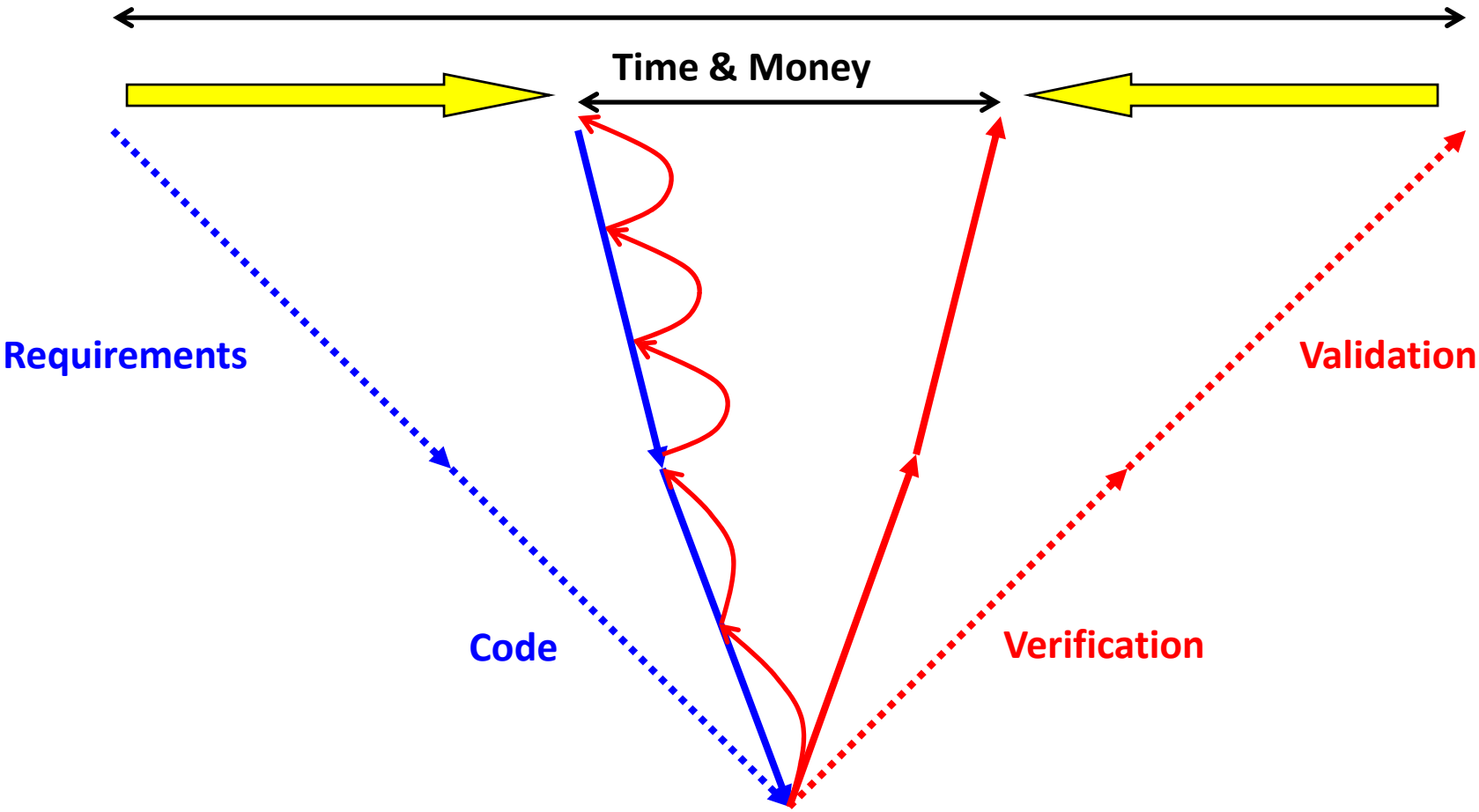
- Show that compositional verification methods are needed to verify complex, IVHM systems
- Justify the approach by comparing to traditional, non-scalable, monolithic approaches to V&V.

- POC: Guillaume Brat
- Organization:
  - RSE group at Code TI (ARC)

Milestones:

- FY'09: Identify suitable approaches, candidate problems with metrics for compositional verification performance.
- FY'10: Document a design whose verification is intractable due to an exponentially large state space using monolithic approaches.
- FY'11: Demonstrate compositional verification to ensure that individual components satisfy safety requirements, and, once assembled, satisfy global safety properties.
- FY'12: Show that these new compositional verification methods provide an equal or greater level of integrity as provided by current assurance approaches.

V&V earlier in the lifecycle



Advanced V&V techniques:
model checking, static analysis, certifiable code synthesis

Compositional verification

- Divide-and-Conquer approach to verification
- Process:
  - Divide system into sub-systems
  - Verify local properties on sub-systems using assumptions about the environment, which includes the other sub-systems
  - Lift to global properties on system without requiring flattening into a huge model

Specific IVHM Aspects

- IVHM is usually part of a complex system
  - Control system for complex problems
  - IVHM engine is added to detect and respond to faults
- IVHM mixes several programming paradigms
  - Traditional engineering languages (C, C++, Java, …)
  - Data-driven techniques
  - Model-based techniques
  - Rule-based techniques
- IVHM will require composing heterogeneous models

Work Plan

- FY09 plan is to select a compelling example and use it to quantify the scalability problems in verifying and validating complex aerospace systems
  - Explore what properties should be verified
  - Select a testbed for evaluating IVHM solutions
    - The ADAPT testbed for power system avionic applications
    - The DAME software, which is an embedded system
    - Other testbeds
  - Work on the modeling aspect to translate them to a proper "model-checking" format (e.g., UML-statechart or Java programs for Java PathFinder, Promela models for SPIN, or SMV models, and decide properties to verify

Work Plan (Cont…)

- FY09, Q3 plan is to work on characterizing the scalability problem
  - Decide Criterion for scalability
    - Number of states
    - Degree of interrelationships between models
    - Range of environment (input) variables
- FY09, Q4 will focus on the compositional aspect to put in place a compositional framework which works with selected model checkers
  - Quantify benefits in terms of state space and analysis time
  - Characterize the properties that can be addressed within the compositional framework

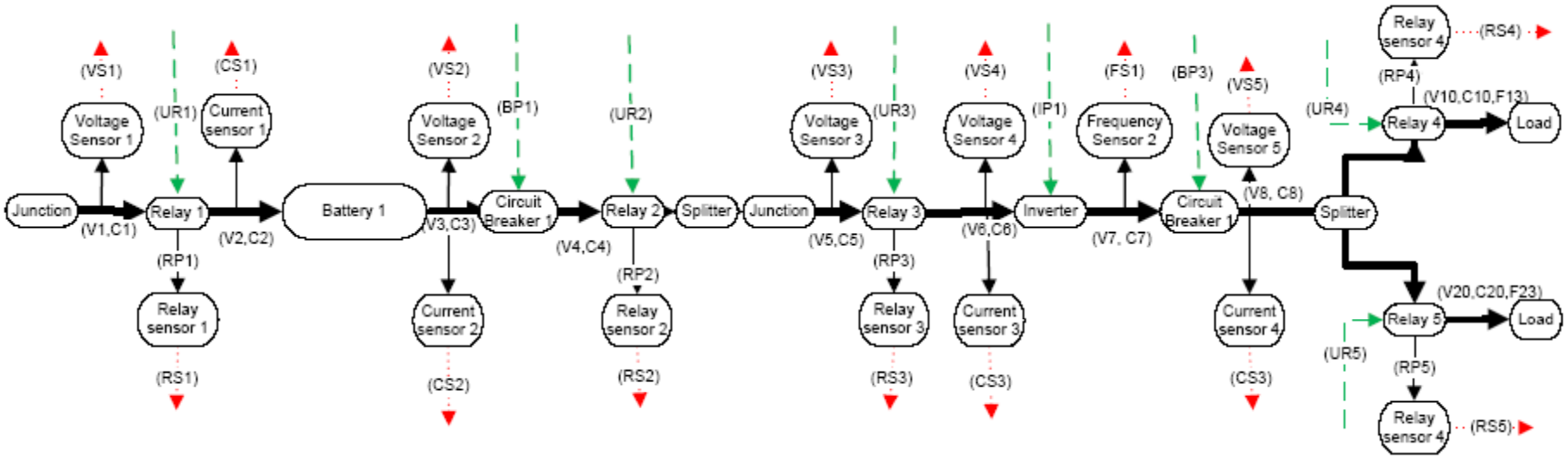
Case Studies

- Current potential case studies:
  - The ADAPT testbed, which is a testbed for evaluating IVHM solutions for a Power System for avionic applications; it includes several diagnosis modules.
  - The DAME software, which is a controller for a drill similar to the ones which will be used on Mars; it is not a proper avionic system, but it is an embedded system and it includes several diagnosis modules.
- We are planning to investigate the availability of other systems (which might be more relevant to the civilian aircrafts) and select one as our case study by the end of the first quarter of FY'09. Possible candidates will be evaluated according to the following criteria:
  - relevance to the Aero program,
  - IVHM features (diagnosis, prognosis, s/w health management, …), and,
  - difficulty in obtaining/building models for the system.

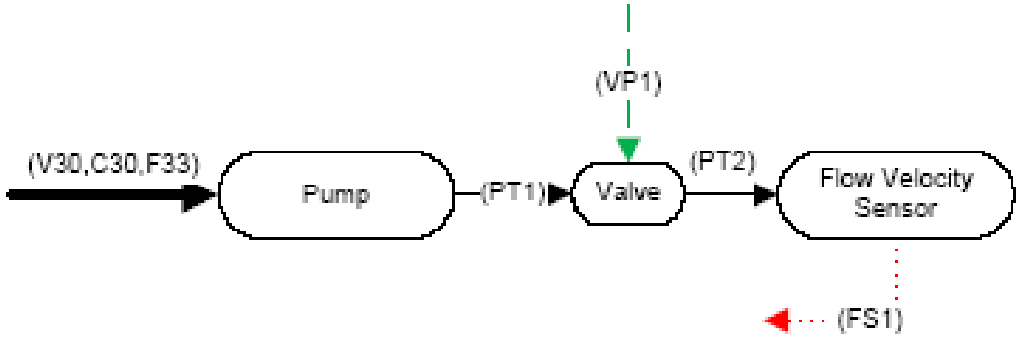
Diversity of models

- Structural (or architectural) models
  - describe the physical layout of a system
  - In hardware, it basically describes the physical components and their connections.
  - In software, it describes the different software modules and the way they interact with each other.
- Functional models
  - Functional models indicate the functions of different elements and their relationships.
  - When it comes to V&V, function is what we need to validate and verify.
  - It indicates what an element is meant to perform as a function and how it relates to other elements.
- Mathematical models
  - precise mathematical descriptions of a function performed by some sub-system.
  - E.g., mathematical equations describing the physics behavior of the system.
- Behavioral models
  - Describe the behavior of the systems
  - Often expressed as finite-state machines

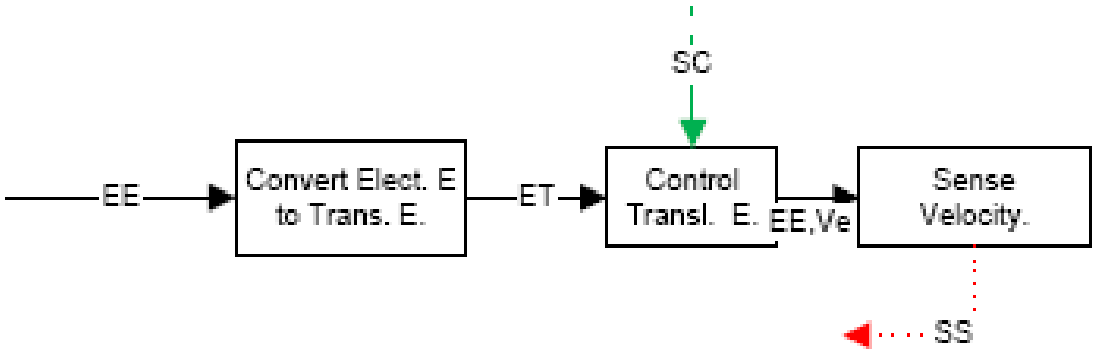
ADAPT partial structural model



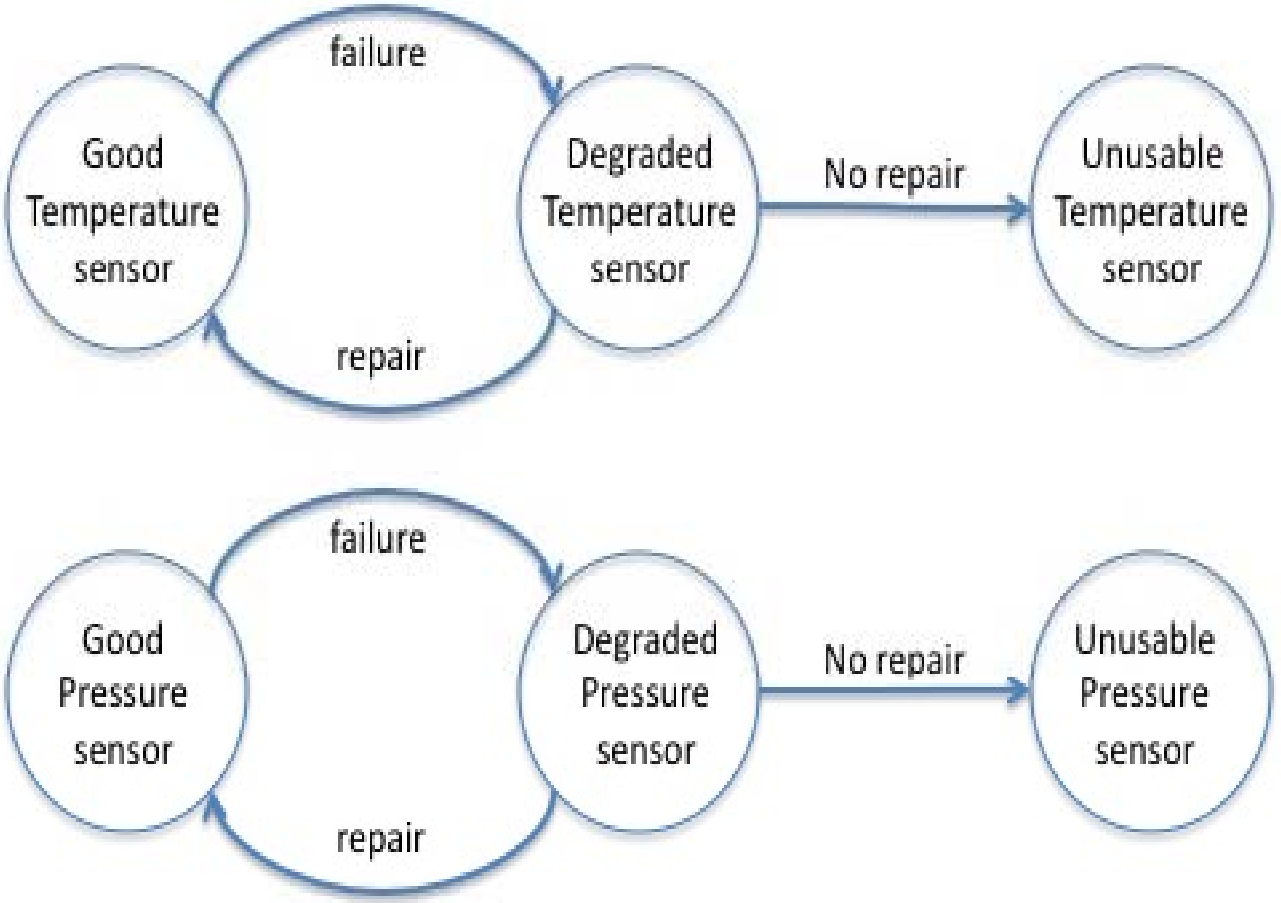
Structural model example



Functional model example



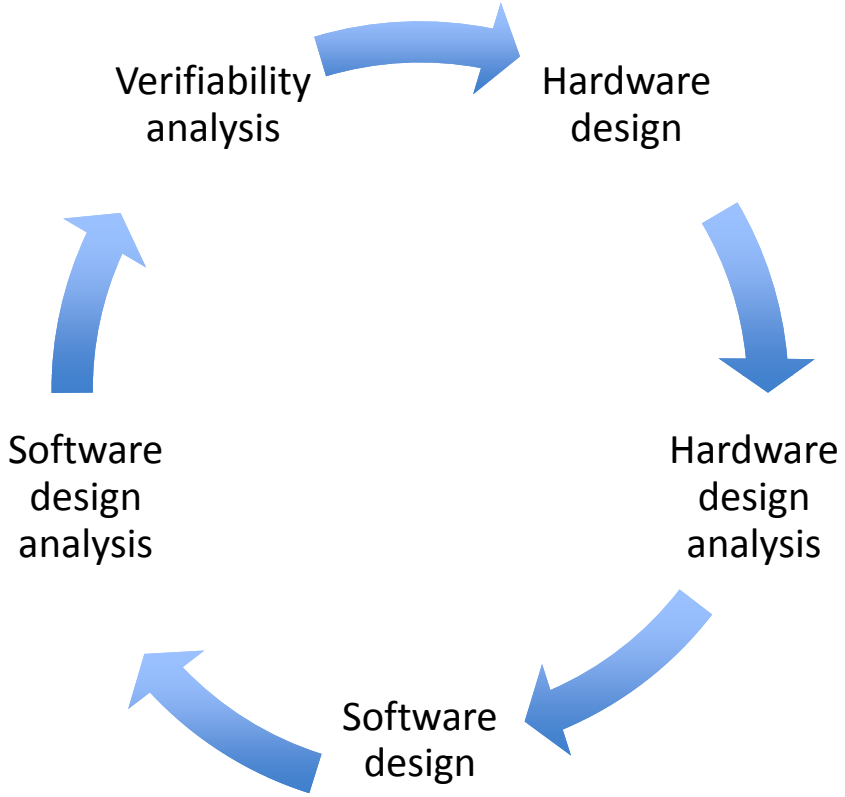
Behavioral model example



Where this should lead to?

- *Design for Verifiability:*
  - *formalize the development of robust software-hardware systems by using formal methods to analyze early design stage system models representing function, configuration, and behavior, by adding a "verifiability" dimension so that the design of software-intensive systems can be refined for increased verifiability*
- Team:
  - Irem Tumer (HW design)
  - Carol Smidts (SW design)
  - Guillaume Brat (Verifiability)

New Design Feedback Loop



- Aim for simplifying V&V for a complex system with IVHM
  - Predict V&V costs
  - Balance them against IVHM features

Plan Forward

WBS number	Task	Dates
4.5.1	Demonstration of compositional verification framework that provides assurance that key system safety properties are met.	10/1/08 – 9/30/09
4.5.1.1	Select a complex aerospace case study	10/1/08 – 12/31/08
4.5.1.2	Select model-checking tools, and, build models for all elements of the selected case study	1/1/09 – 3/31/08
4.5.1.3	Characterize scalability of traditional model-checking approach	4/1/09 – 6/30/08
4.5.1.4	Build compositional framework and characterize its gains	7/1/08 – 9/30/08