Derivation of Safety Verification Conditions from Hazard Definitions

Ken Wong

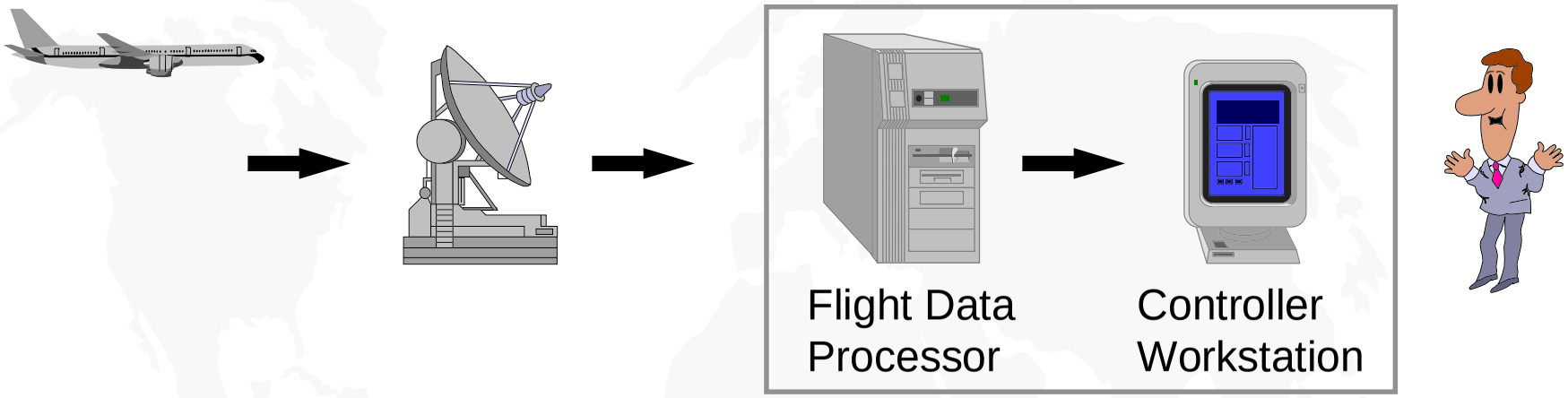
Department of Computer Science

University of British Columbia

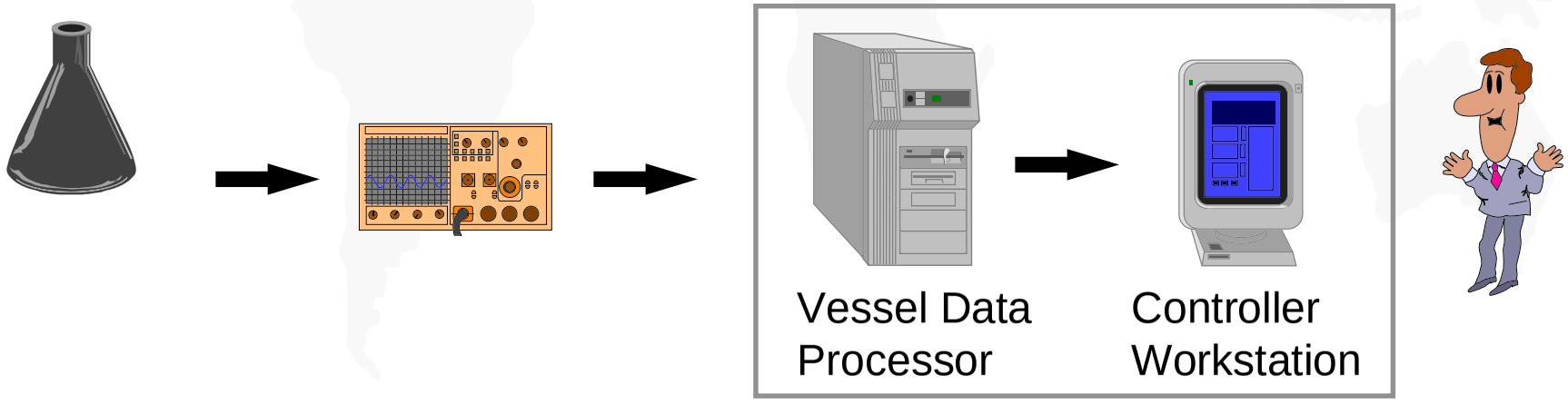
Air Traffic Management (ATM)

- Raytheon Systems Canada Ltd.
- Real-time information system
- Large scale Ada system
  - 700,000 production SLOC + COTS
- Modern architecture
  - Object-oriented, layered, distributed

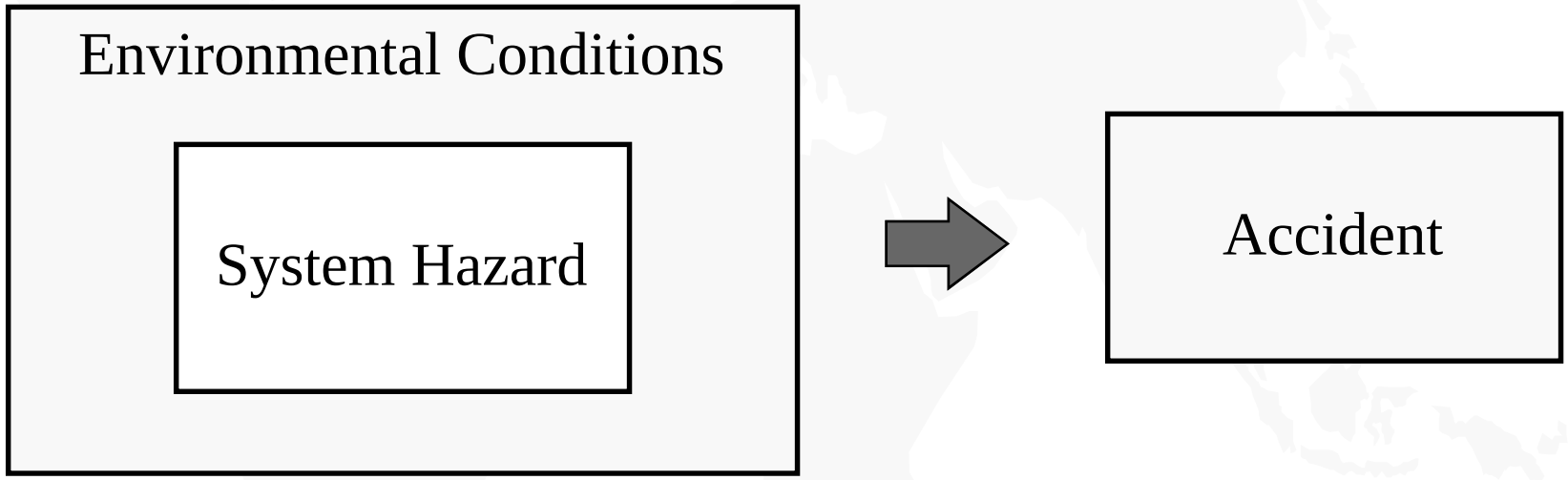
Air Traffic Management (ATM) System



Chemical Factory Management (CFM) System



System Safety Engineering



- Identification, analysis and elimination or control of system hazards

CFM Safety

- **Accidents**
  - e.g., Vessel rupture, fire or explosion
- **System Hazards**
  - e.g., An “invalid” temperature, D, is displayed for vessel V at time T
- **Hazard Analysis**
  - e.g., temperature value is stale or corrupted

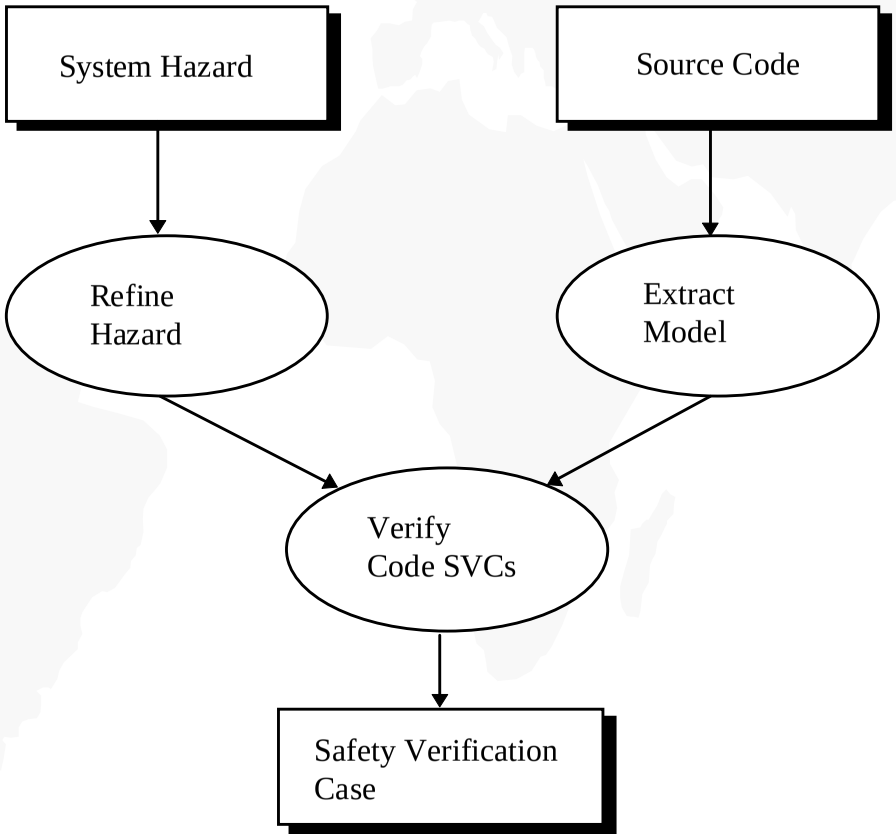
Safety Verification

System Hazard

Source Code

?

Safety Verification Case



Semantic Gap

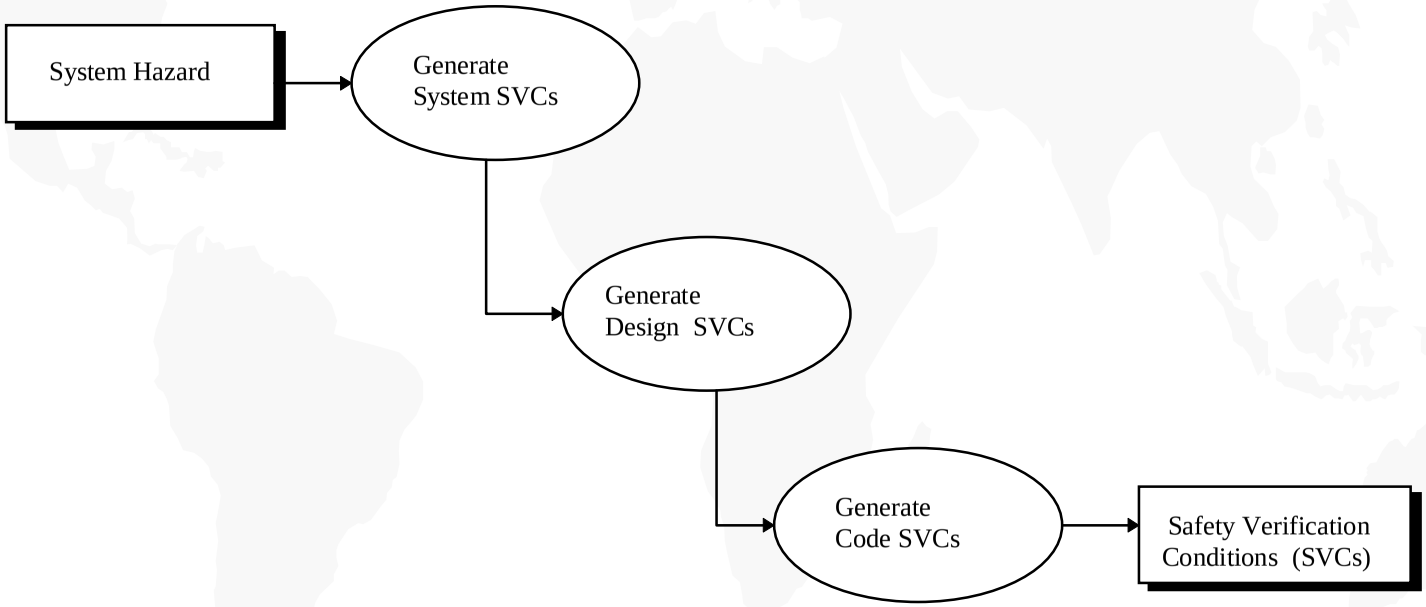
System Hazard

- end-user terminology
  - temperature, vessel
- abstract relationships
  - invalid temperature
- temporal relationships
  - “at some time T ...”

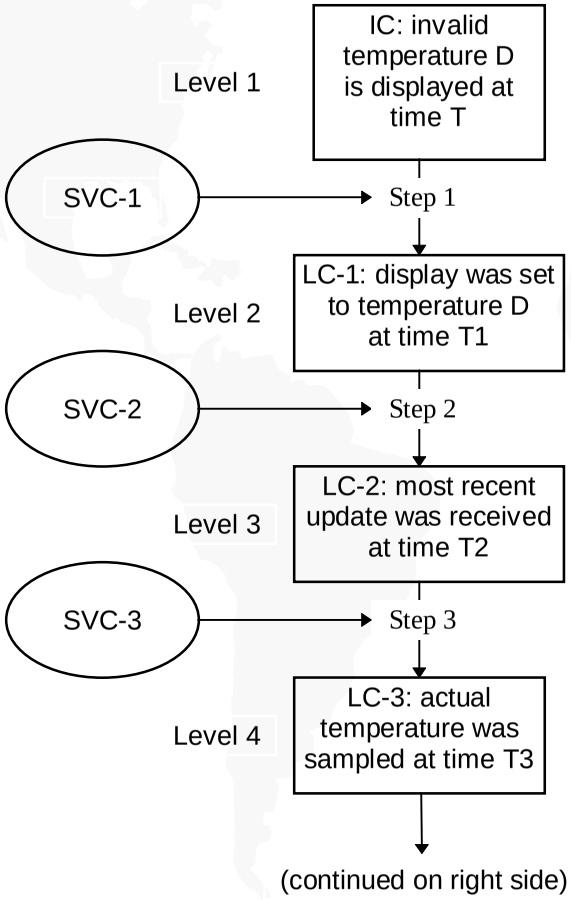
Source Code

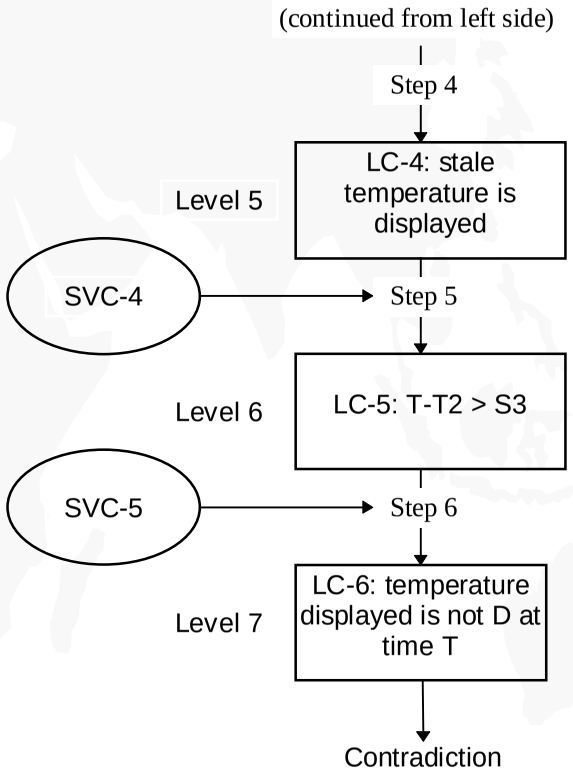
- programmer’s lexicon
  - abstract classes
- concrete relationships
  - arithmetic, logical
- causal relationships
  - program execution

Hazard Refinement



Generate System SVCs: CFM





Source Code Level SVCs

- Verifiable Code Assertions
  - Feasibility of code verification tools
  - e.g., SPARK Examiner
- Formal source code level SVCs
  - Formalizing object-oriented software
  - e.g., Typed, predicate logic

References

- http://www.cs.ubc.ca/formalWARE/safety.htm
- Generating Safety Verification Conditions By Means of Reductio Ad Absurdum, ISSC'98 (to appear)
- Refinement of Safety-Related Hazards into Verifiable Code Assertions, SAFECOMP'98 (to appear)
- Formalization of Safety Verification Conditions, 1st ROOM Workshop (to appear)
- Ensuring the Inspectability, Maintainability and Repeatability of the Safety Verification of a Critical System, UBC Technical Report 98-06
- Looking at Code With Your Safety Goggles On, Ada-Europe'98