Generating Safety Verification Conditions Through Fault Tree Analysis and Rigorous Reasoning

Jeff Joyce, Raytheon Systems Canada Ltd.

Ken Wong, University of British Columbia

Overview

- Hazard Refinement
  - Generating conditions for safety verification
- Analysis of complex temporal relationships
  - Conventional techniques inadequate
- Safety Verification Condition Generation
  - “proof by contradiction” style reasoning
  - semi-formal notation
- Chemical factory example

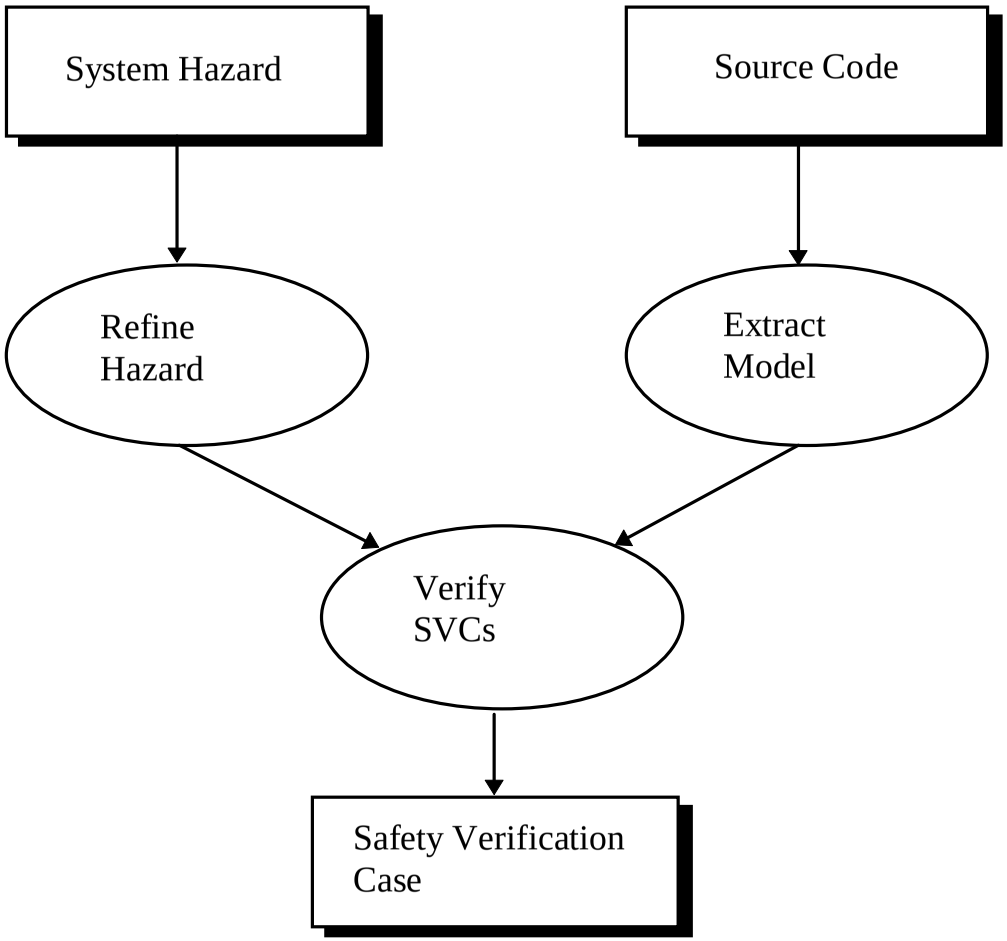
Safety Verification

System Hazard

Source Code

?

Safety Verification Case



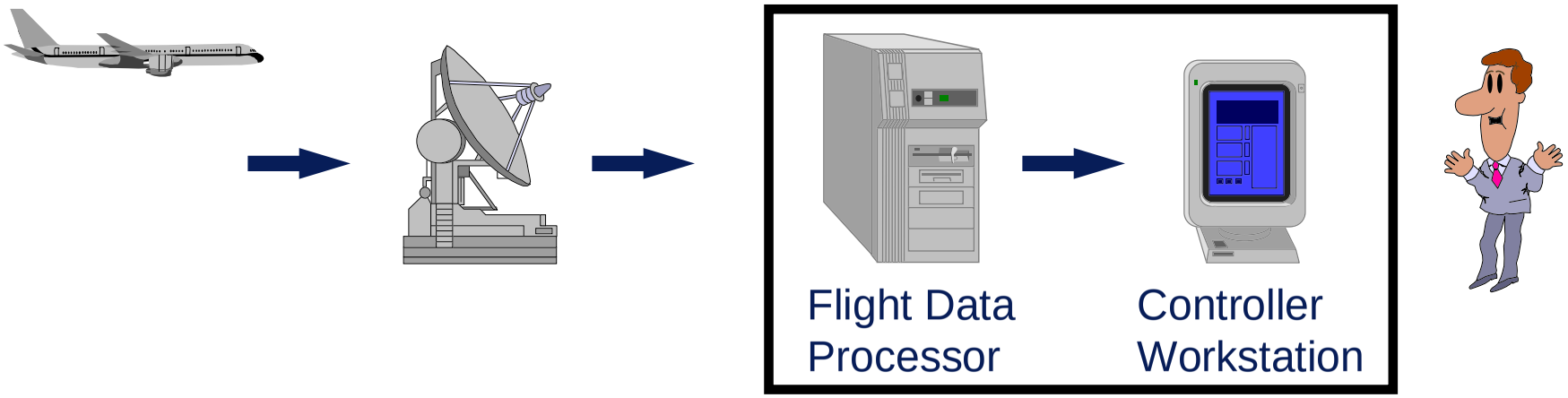
Safety Verification Conditions

- Refinement of hazard definition into SVCs
  - Used in system safety verification
- Different levels of SVC
  - System, design and code level
- Complex temporal relationships
  - e.g., Timing constraints for real-time systems

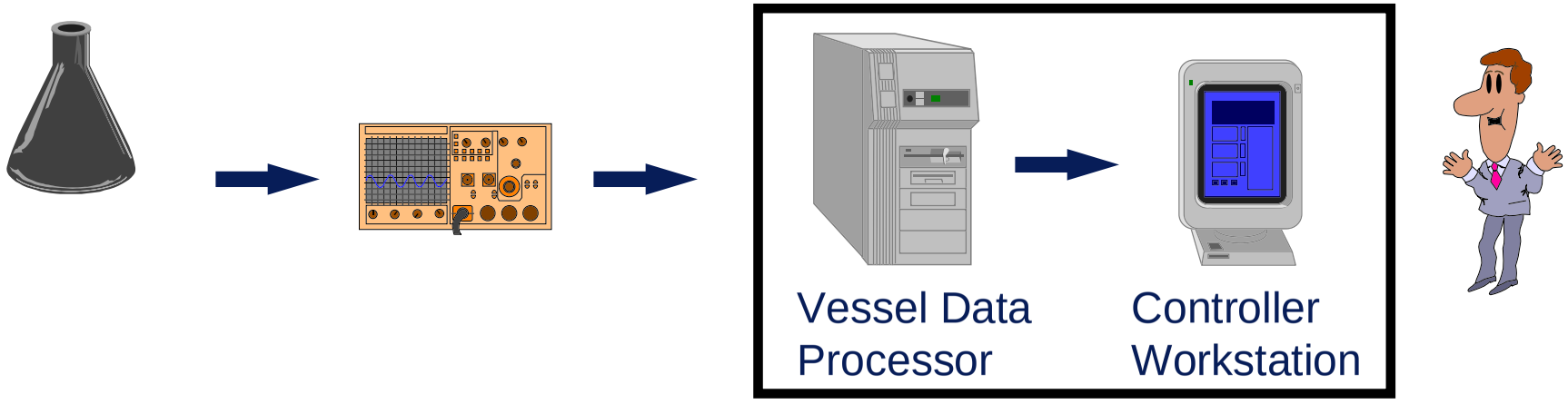
Generating SVCs

- SVCs generated in an *ad hoc* fashion
- Introduced to mitigate hazard causes
  - e.g., Fault Tree Analysis (FTA)
- Analysis of temporal relationships
  - conventional techniques inadequate

Air Traffic Management (ATM) System



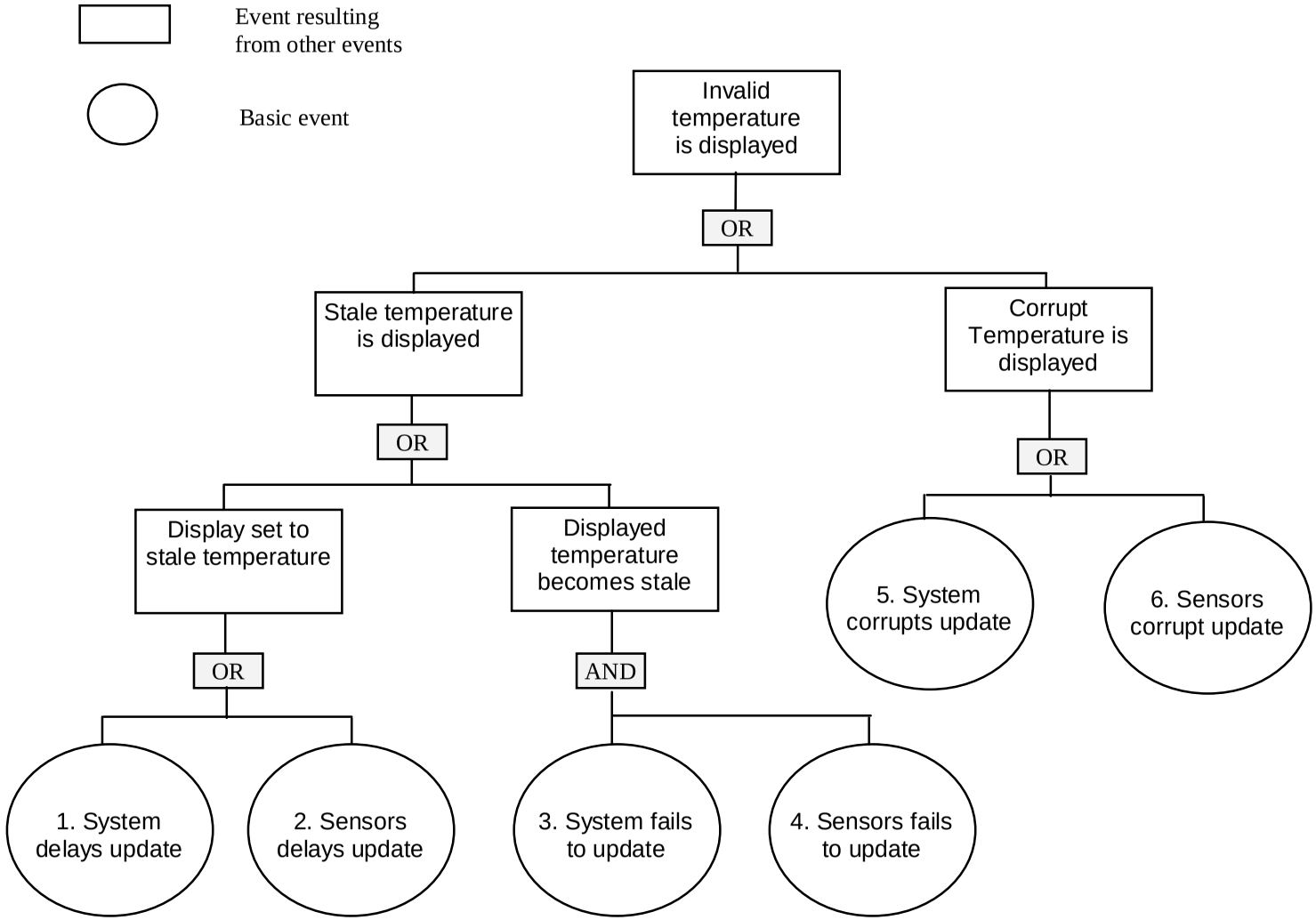
Chemical Factory Management (CFM) System



CFM Hazard

- Hazard
  - An “invalid” temperature is displayed
- Hazard causes
  - corrupt or stale temperature value
- Failure to display temperature value
  - Not hazardous if displayed as “unavailable”

Fault Tree Analysis



SVCs from FTA

- SVCs
  - **Updates**: System does not delay update
  - **No updates**: System updates as “unavailable”
- Undetermined temporal relationships
  - **Time parameters**: how quickly?
  - **Relationships**: propagation vs staleness times
  - **Hazard scenario**: final update displayed after display updated as “unavailable”

SVC Generation (SVCG)

- Input from hazard analysis
- System-level SVCs
  - "black box" view of the system
- Semi-formal notation
  - representation of durations and instants of time
- Informal, rigorous mathematical reasoning
  - "proof by contradiction" style reasoning

Semi-Formal Notation: Hazard

- An invalid temperature is displayed:
  - "The temperature, D, displayed for vessel V at time T has not been within **MAX_DISP_TEMP_DIFF** degrees of the actual temperature of the vessel at any time within **MAX_DISP_TEMP_STALE** milliseconds before time T"
- **MAX_DISP_TEMP_STALE**: staleness parameter

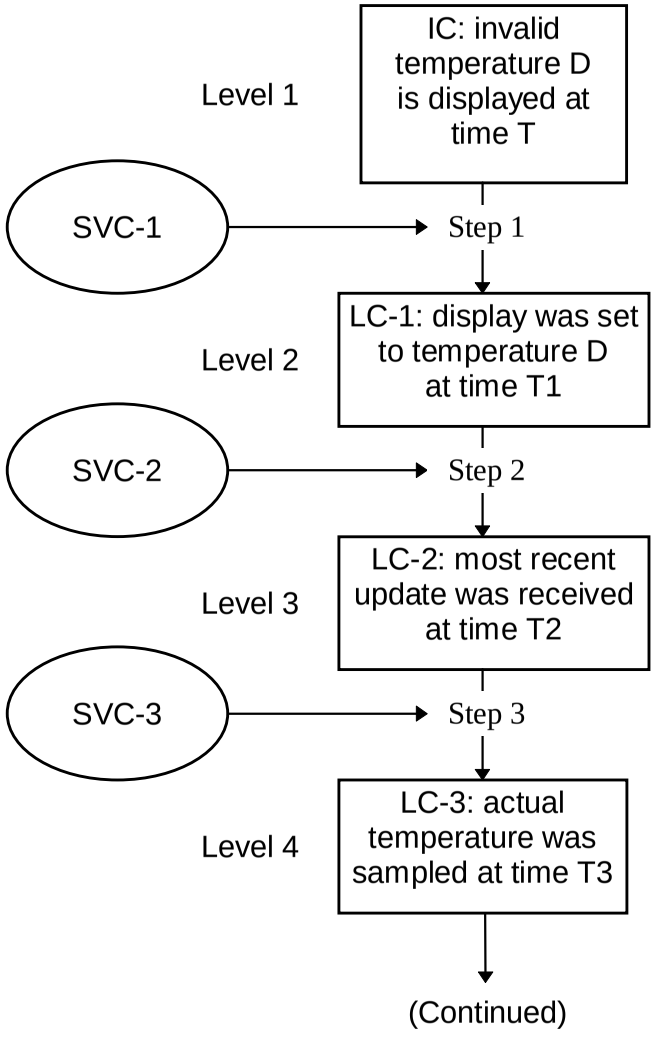
Semi-formal notation: SVC

- **FTA**
  - System does not delay update
- **SVC-2**
  - “For all vessels, v, displayed temperatures, d, and times, t, if the displayed temperature of vessel v is set to d at time t then at some time no earlier than **S1** milliseconds before t the system received a report from the external sensor monitoring system that the temperature of vessel v is d.”

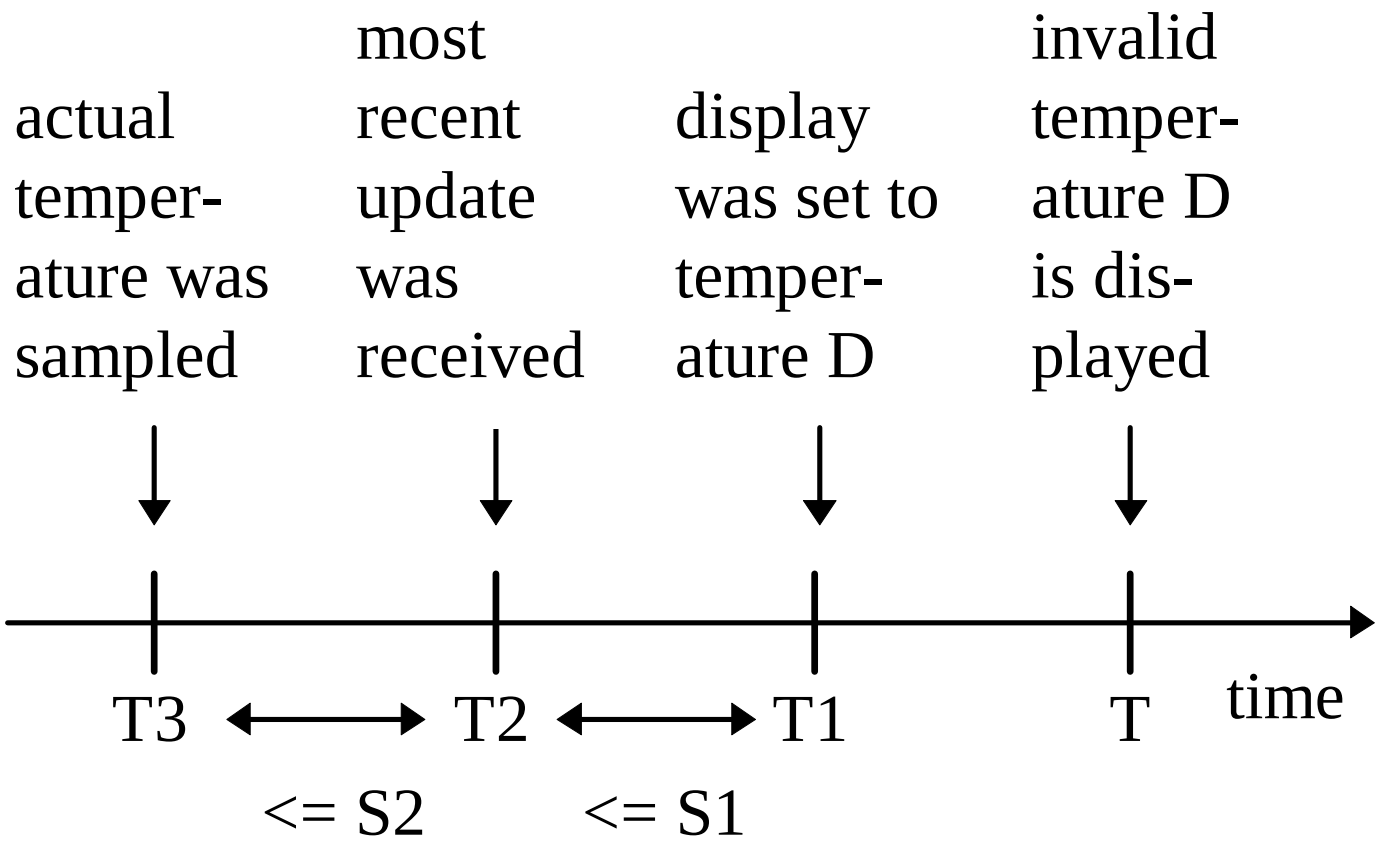
Backwards Reasoning

- **Initial Conjecture** (hazard)
  - "Invalid temperature D is displayed at time T"
- **Introduce SVC** (steer reasoning)
  - "If D is displayed at time T as the temperature of vessel V then there is some time T', T' <= T, when the temperature of V was set to D ..."
  - **Logical Consequence** (hazard cause)
  - "Display was set to temperature D at time T"

Cause: Corrupt Temperature



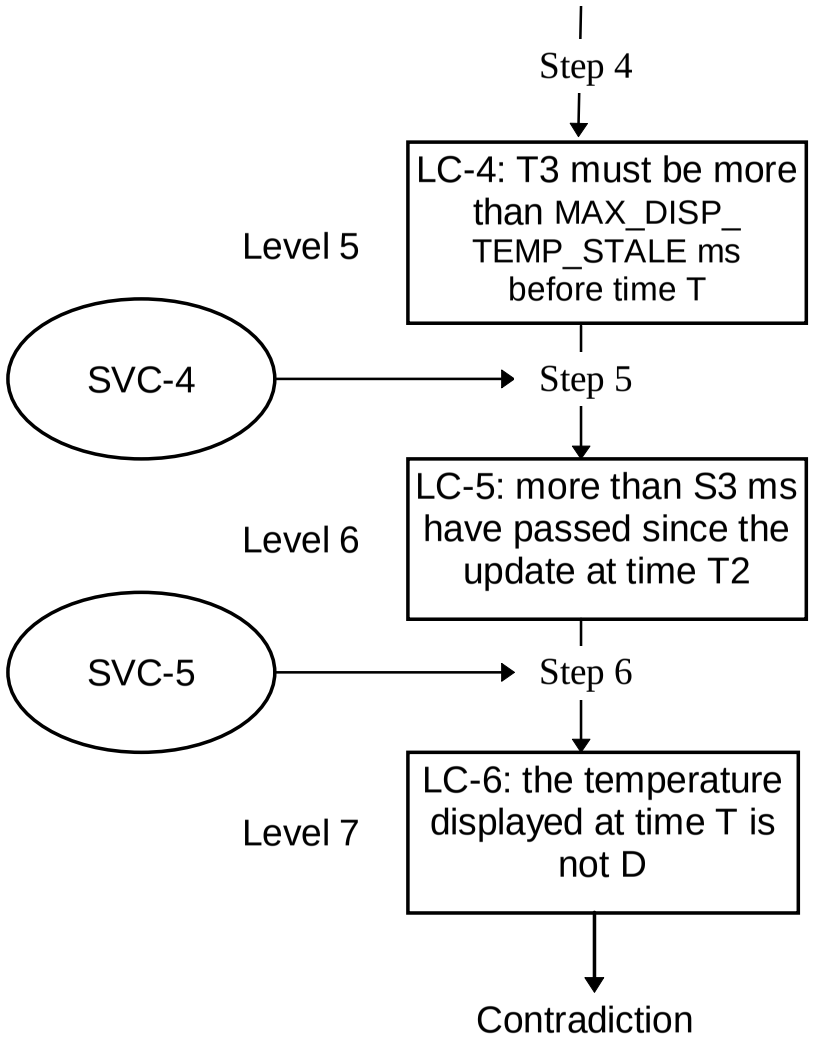
Timeline of Events



Logical Reasoning

- **System-level constants**: S1, S2 and S3
  - Relationship to MAX_DISP_TEMP_STALE?
- **Introduce SVC-4**
  - MAX_DISP_TEMP_STALE > S2 + S3
- **Derive LC-5** (use arithmetic inequalities)
  - more than S3 ms has passed since the update at time T2

Cause: Stale Temperature



SVCG Results

- Rigorous safety argument
- Generated system-level SVCs
  - Functionality constraints
  - Environmental and system assumptions
  - Key temporal relationships
- Applicable to other hazards and systems
- Derivation of design- and code-level SVCs

Conclusion

- Safety Verification Condition Generation
  - Semi-formal notation: Specifying time
  - “Proof by Contradiction”: FTA and SFTA
- “Pencil and paper” analysis
  - Reasoning about mathematical inequalities
  - Validation with formal verification technique?
- More complex than FTA
  - Simpler than formal analysis of system