Model-based Safety and Security Analysis in High Consequence System Development

John Colley
Formal Verification Conference
June 2016
“Humans are Slamming into Driverless Cars and Exposing a Key Flaw”

Bloomberg, Dec 2015
Introduction

• High consequence systems must be *safe* and *secure*

• but they still need to get the job done
  – *Fail-safe* is not always a viable option

• We are responsible for delivering software/digital hardware components. How do we assess their contribution to *system* safety and security?
“Emergent behavior is that which cannot be predicted through analysis at any level simpler than that of the system as a whole. ... ”

(Dyson, George, Darwin Among the Machines, Addison-Wesley, 1997)
“the engineering-driven actions necessary to develop more defensible and survivable systems”

“Security, like safety and other system quality properties, is an emergent property of a system.”
Trustworthiness

“Trustworthiness requirements can include, for example, attributes of safety, security, reliability, dependability, performance, resilience, and survivability under a wide range of potential adversity in the form of disruptions, hazards, and threats.”

“Effective measures of trustworthiness are meaningful only to the extent that the requirements are sufficiently complete and well-defined, and can be accurately assessed.”
Where do we start?
The Development and Certification Process

- Development and Design Guidance
  ARP-4754A, 2010

- Guidelines and methods for
  Safety Assessment
  ARP-4761, 1996

  ➤ Software Considerations
    DO-178C, 2011

  ➤ Design Guidance
    Electronic Hardware
    DO-254, 2000
DO-178B

• Software aspects of airborne systems and equipment
• Introduced in 1992
• Requirements-based Testing with Structural Coverage
  – Full, bi-directional Traceability from Requirements to Implementation
  – Modified Condition/Decision Coverage (MC/DC) sign-off for Level A software
DO-178C

• Finalised in December 2011
• Updates the successful 178-B standard
  – DO-331 Model-based Development and Verification Supplement
  – DO-333 Formal Methods Supplement
  – DO-332 Object-Oriented Technology and Related Techniques Supplement
  – DO-330 Software Tool Qualification Considerations
  – Modified Condition/Decision Coverage (MC/DC) definition clarification
DO-331
Model-based Development and Verification Supplement

• Formal Modelling Notation
  – Textual *or*
  – Graphical
    – *Formal Semantics*

• Supports a model-based methodology
  – Refinement of High-Level Requirements
  – Model-based Testing
  – Co-simulation
  – Code Generation

• Methodology already used successfully in Avionics
  – *SCADE*
The outputs of a Formal Verification tool may be used to

- Replace or
- Augment

Testing

Necessary to convince the Certification Authority of the validity of the Formal Verification

- If not, must show full MC/DC coverage through testing
DO-178C Methodology for Design Assurance of Airborne Software

System Life Cycle Processes
- Requirements Safety Assessment
- Hazard Assessment
- Approval Activities
- Verification Activities
- Integration

Software Life Cycle Processes
- Planning Process
- Development Processes
  - Requirements Process
  - Design Process
  - Coding Process
  - Integration Process
- Verification Process
- Configuration Management Process
- Quality Assurance Process
- Certification Liaison Process

Hardware Life Cycle Processes
- System Safety Assessment Process
- Derived High-Level Requirements
- Derived Low-Level Requirements
- Problem/Change Documentation
The Development and Certification Process

Development and Design Guidance
ARP-4754A, 2010

Guidelines and methods for Safety Assessment
ARP-4761, 1996

Software Considerations
DO-178C, 2011

Design Guidance
Electronic Hardware
DO-254, 2000
ARP-4761 Guidelines and Methods for Safety Assessment

• Strengths
  – Practical
  – Includes a detailed worked example
    • Aircraft Wheel Brake System

• Weaknesses
  – Out-of-date (1996)
  – Out-of-step with other relevant standards
    • ARP-4754A (2010)
    • DO-178C (2011)
V Process for Traditional Safety Assessment

System Requirements and Objectives

Aircraft FHA

System FHAs

System FTAs

Derived Safety Requirements

Design

PSSAs

System FTAs

System FMEAs

SSAs

Certification

Aircraft FTA

Derived Safety Requirements

SSA: System Safety Assessment
PSSA: Preliminary System Safety Assessment

FHA: Functional Hazard Analysis
FTA: Fault Tree Analysis
FMEA: Failure Modes and Effects Analysis
ARP-4761A

• Updating the ARP-4761 standard
  – Currently in Progress

• Two major threads of the re-standardisation effort

  1. Model-based Safety Analysis

  2. System Theoretic Safety Analysis
     • A Comparison of STPA and the ARP 4761 Safety Assessment Process, Leveson et al, MIT, 2014
Model-based Safety Analysis

• System safety analysis techniques are well established, but
  – Highly subjective
  – Manual
  – Based on an informal System Model

• The Model-based Approach
  – System and Safety Engineers share a common system model
  – Model-based Development and Verification is already supported for DO-178C (DO-331 supplement)
  – Extending the system model with a Fault model enables automation of the safety analysis process
  – Allows Formal Reasoning

*Model-Based Safety Analysis, Joshi et al, NASA Technical Report, 2006*
System-Theoretic Accident Model and Processes (STAMP)

• Systems Theory Foundation
• New *Causality Model* (c. 2010)
• Change in emphasis in system safety from
  – Preventing failures to
  – Enforcing Behavioural Safety Constraints
• Component Failure still Considered
• Safety is reformulated as a *control* problem rather than a *reliability* problem
• Three main concepts
  – Safety constraints
  – Hierarchical Control Structures
  – Process Models

Engineering a Safer World, Leveson MIT 2011
Safety Requirements

“Any controller – human or automated – needs a model of the process being controlled to control it effectively”

“Accidents can occur when the controller’s process model does not match the state of the system being controlled and the controller issues unsafe commands.”

Engineering a Safer World, Leveson, 2012
System Theoretic Process Analysis (STPA)

• New Hazard Analysis Technique
  – Identify potential causes of accidents, ie *scenarios* that can lead to losses
  – **Eliminate** or **Control** hazards in design or operations before damage occurs

• Augments existing methods (FTA, FMEA)

• Includes new causal factors identified in STAMP
  – Design errors including software flaws
  – Component interaction accidents
  – Human decision-making errors
  – Social, organisational and management factors contributing to accidents

Engineering a Safer World, Leveson MIT 2011
The Two Phases of STPA

1. Identify Potentially Hazardous Control Actions and derive the Safety Constraints
2. Determine how Unsafe Control Actions could occur

Engineering a Safer World, Leveson, 2012
Controlled Phenomena

For example, Landing Gear Doors

1. The Controller will *open* the Doors when the Pilot moves the Lever to Extend or Retract the Landing Gear
2. The Controller will then *close* the Doors when the Landing Gear is fully Extended or Retracted
3. The Doors will remain *open* while the Landing Gear is Extending or Retracting
The Door Sub-system Process Models

**Controller**
- **Process Model**
  - **Door Position**
    - Locked Open
    - Locked Closed
    - Opening
    - Closing
    - Unknown

**Human Operator**
- **Process Model**
  - **Landing Gear**
    - Extended/ing
    - Retracted/ing
    - Unknown

**Actuator**
- **OpenDoor**
- **CloseDoor**

**Sensor**
- **Door is Locked Open**
- **Door is Locked Closed**

**Controlled Process**
- **Extend**
- **Retract**
Step I: Identify Potentially Hazardous Control Actions and Derive Safety Constraints

<table>
<thead>
<tr>
<th>Controller Action</th>
<th>Not Providing Causes Hazard</th>
<th>Providing Causes Hazard</th>
<th>Wrong Timing or Order Causes Hazard</th>
<th>Stopped too soon/Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Door</td>
<td>Cannot extend Landing Gear for landing</td>
<td>Not Hazardous</td>
<td>Not Hazardous</td>
<td>Damage to Landing Gear/Not Hazardous</td>
</tr>
<tr>
<td>Close Door</td>
<td>Not Hazardous</td>
<td>Damage to Landing Gear</td>
<td>Damage to Landing Gear</td>
<td>Not Hazardous/Not Hazardous</td>
</tr>
</tbody>
</table>

**Safety Constraints**

1. If the Landing Gear is Extending, the Door must be Locked Open
2. If the Landing Gear is Retracting, the Door must be Locked Open
3. A “Close Door” command must only be issued if the Landing Gear is Locked Up or Locked Down
4. An “Open Door” command must only be issued if the Landing Gear is Locked Up or Locked Down
Step I: Identify Potentially Hazardous Control Actions and Derive Safety Constraints

<table>
<thead>
<tr>
<th>Controller Action</th>
<th>Not Providing Causes Hazard</th>
<th>Providing Causes Hazard</th>
<th>Wrong Timing or Order Causes Hazard</th>
<th>Stopped too soon/Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Door</td>
<td>Cannot extend</td>
<td>Not Hazardous</td>
<td>Not Hazardous</td>
<td>Damage to Landing Gear</td>
</tr>
<tr>
<td>Close Door</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Safety Constraints**

1. If the Landing Gear is Extending, the Door must be Locked Open.
2. If the Landing Gear is Retracting, the Door must be Locked Open.
3. A “Close Door” command must only be issued if the Landing Gear is Locked Up or Locked Down.
4. An “Open Door” command must only be issued if the Landing Gear is Locked Up or Locked Down.

```
gearstate ∈ {locked_down, locked_up} ∨ doorstate = locked_open

event Close
where
  @grd1 gearstate ∈ {locked_down, locked_up}
  @grd2 doorstate ∈ {opening, locked_open}
then
  @act1 doorstate := closing
end
```
The Model Extended FSM
System Theoretic Early Concept Analysis (STECA)

• Begins at Concept Stage
  – Requirements
    • Have multiple sources
    • Are evolving
  – No Specification

• Model-based

• Starting point is Concept of Operations (Con-Ops)
The Concept of Operations (CONOPS) is a user-oriented document that describes the characteristics for a proposed asset or system from the viewpoint of any individual or organizational entity that will use it in their daily work activities or who will operate or interact directly with it.

U.S. Coast Guard Press release, 2007
STPA-sec

1. Identifying the losses to be considered
2. Identifying system hazards or security vulnerabilities
3. Drawing the system functional control structure
4. Identifying unsafe or insecure control actions
5. Identifying intentional actions in the generation of causal scenarios
An Integrated Approach to Safety and Security* I

• Augments STPA to consider
  – External Threat
  – Inside Risks

• Added Causal Scenarios
  – Intentional Actions

• Hazards lead to safety incidents in the same way that vulnerabilities lead to security incidents

• Mission Assurance
  “the ability to complete a wide range of missions across a wide range of degradations”

Linton Wells, Former US Defense Dept Chief Information Officer, 2004-5

*Inside Risks, An Integrated Approach to Safety and Security
Based on Systems Theory, Young, Leveson, CACM Feb 2014
An Integrated Approach to Safety and Security*  

• Augments STPA to consider  
  – External Threat  
  – Inside Risks

Focus is on  
**Mission Completion**  
NOT  
Protecting the infrastructure used to complete the mission

• Mission Assurance  
  “the ability to complete a wide range of missions across a wide range of degradations”  
  Linton Wells, Former US Defense Dept Chief Information Officer, 2004-5

*Inside Risks, An Integrated Approach to Safety and Security  
Based on Systems Theory, Young, Leveson, CACM Feb 2014
An Integrated Approach to Safety and Security* II

• Top-down
  – Assuring the overall function of the enterprise

• Initial focus on controlling vulnerabilities rather than avoiding threats (strategic)
  – Likely to be far fewer vulnerabilities than threats

• Provides the context for subsequent threat analysis (tactical)
  – External and Internal
  – Know and unknown

An Integrated Approach to Safety and Security* III

“... the physical (or proximate) cause of a disruption does not really matter. What matters is the efficacy of the strategy in dealing with (controlling) the effects of that disruption on overall system function or assuring the mission.”
Model-based Trustworthiness Analysis

- Incorporates STPA, STECA, STPA-sec
  - Model-based
  - Early Concept
  - Architecture
- Augments the traditional Avionics Flow
  - Software/Digital Hardware Development
  - Verification/Validation and Acceptance
- Event-B, PSL, SVA Modelling and Formal Analysis
Case Study: Next Generation Transportation System (NextGen)

• Driven by the FAA
• 2012 – 2025 rollout
• NextGen Focus
  – More efficient flight paths
  – Shift in responsibility from ground-based crews to flight crews and flight-deck decision support tools
  – Shift of emphasis from clearance-based to trajectory-based operations
Independent of the aircraft, the ANSP uses ADS-B position reporting for lateral and longitudinal progress, altitude reporting for vertical, and tools that measure the time progression for the flight track. Data link provides aircraft intent information. Combined, this position and timing information is then compared to a performance requirement for the airspace and the operation. ...precision needed...will vary based on the density of traffic and the nature of the operations. [JPDO, 2011]

Four Dimensional Trajectory (4DT)

- 3 dimensional space + time
- Represents not only current state of aircraft but also intent
- Specifies the tolerances in which the aircraft must operate
  - Required Navigation Performance (RNP)
  - Required Time Performance (RTP)
- Conformance
  - Monitoring the aircraft’s performance against the agreed 4DT
CONCEPT OF OPERATIONS FOR THE NEXT GENERATION AIR TRANSPORTATION SYSTEM (NEXTGEN)
Joint Planning and Development Office June 2007
Conformance Monitoring

• Automated
• On the ground and in the air
• Generates alerts if an aircraft does not meet its agreed 4DT performance
• We consider security and reliability as well as safety
Hazard/Vulnerability Analysis

1. Aircraft violate minimum separation
2. Aircraft enters uncontrolled state
3. Aircraft performs controlled maneuver into ground
System-level Constraints

1. Aircraft must remain at least \( n \) nautical miles apart en-route

2. Aircraft position, velocity must remain within airframe manufacturer defined flight envelope

3. Aircraft must maintain positive clearance with all terrain (other than runways and taxiways)
Control Hierarchy

- Route Planning
- Piloting Function
- Aircraft
- Environment

Composed Control Function

Data Link

ANSP: Air Navigation Service Provider
CA: Controller Actions
CDTI: Cockpit Display of Traffic Information
FMS: Flight Management System

System-Theoretic Process Analysis (STPA)

1. Identify Potentially Hazardous Control Actions and derive the Safety Constraints
2. Determine how Unsafe Control Actions could occur

Engineering a Safer World, Leveson, 2012
Potential unsafe control action for trajectory generation function: Approving a 4DT that will lead to LOS or not modifying a 4DT that will overlap

Potential unsafe control action for piloting function: Aircraft is following a 4DT that will lead to LOS

ANSP: Air Navigation Service Provider
CA: Controller Actions
CDTI: Cockpit Display of Traffic Information
FMS: Flight Management System
STPA Step 2

Potential unsafe control action for trajectory

1. Error in ANSP algorithms (deliberate or otherwise)
2. 4DT is modified by Data Link (deliberate or otherwise)
3. Misleading or faulty display of 4DT to pilot (deliberate or otherwise)
4. Latency in communication (deliberate or otherwise)

ANSP: Air Navigation Service Provider
CA: Controller Actions
CDTI: Cockpit Display of Traffic Information
FMS: Flight Management System
Mitigating/controlling the Hazards/Vulnerabilities Architectural Considerations

GROUND
- Algorithm
- Add Timestamp, CRC, Encrypt

Data Link

AIRCRAFT
- Display
- Decrypt, CRC, Check Timestamp

Safety/Security/Reliability Critical Modules
The Model-based Flow

• Driven by CONOPS
• System-level Constraints derived from System-level Hazard/Vulnerability Analysis
• System Control Hierarchy is defined
• Unsafe control actions are identified
• Hazards/Vulnerabilities are eliminated/mitigated
• Formal, Model-based
• Integrated within Software/Digital Hardware Development, Verification, Validation Flow