Software Safety and Security Best Practices
A Case Study From Aerospace
Agenda

• Introduction
• Why Aviation?
• ARINC 653 Real-time Linux on Xen (ARLX)
• Safety Artifacts for ARLX
• Security Artifacts for ARLX
• Conclusion
Key Features driving increased awareness of safety and security

  - Chevy Volt – 10 million lines of code
  - Boeing 787 – 8 millions line of code
  - F-35 JSF – 6 millions lines of code

- Increased complexity
  - Federated to Integrated

- Increased criticality
Why Aviation?

- Formal certification for safety since 1982
- Designated Engineering Representatives (DER)
ARLX - ARINC 653 Real-time Linux on Xen

- Funded with IR&D, SBIR awards
  - US Navy
  - DARPA
- Partitioned operating environment provides safety and security via isolation of software applications
• DO-178C processes
• Formal Methods analysis
V-model for System Development

DO178

Software Planning Process

High Level Requirements Definition

Low Level Requirements Breakout

Architecture

Detailed Design Implementation

Safety Goals and Requirements Definition

Unit Architectural Design

Unit Detailed Design and Analysis

ISO26262 Design Flow

Unit Testing And Verification

Higher Level Integration Testing

Verification of Safety Goals and Requirements

Final Integration and Verification

Design Verification

Unit Design Integration
<table>
<thead>
<tr>
<th>DO-178 Level</th>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Catastrophic</td>
<td>Prevents continued safe flight or landing, many fatal injuries</td>
</tr>
<tr>
<td>B</td>
<td>Hazardous/Severe</td>
<td>Potential fatal injuries to a small number of occupants</td>
</tr>
<tr>
<td>C</td>
<td>Major</td>
<td>Impairs crew efficiency, discomfort, or possible injuries to occupants</td>
</tr>
<tr>
<td>D</td>
<td>Minor</td>
<td>Reduced aircraft safety margins, but well within crew capability</td>
</tr>
<tr>
<td>E</td>
<td>No Effect</td>
<td>Does not affect the safety of the aircraft at all</td>
</tr>
</tbody>
</table>
DO-178 requires five plans and three development standards.

• Plans
  – Plan for Software Aspects of Certification (PSAC)
  – Software Development Plan (SDP)
  – Software Verification Plan (SVP)
  – Software Configuration Management Plan (SCMP)
  – Software Quality Assurance Plan (SQAP)

• Development Standards
  – Software Requirements Standards (SRS)
  – Software Design Standards (SDS)
  – Software Coding Standards (SCS)
SOI Audit: Inspection Packet

• Requirements:
  – System: 27
  – HLR: 222
  – LLR: 156

• Tests:
  – Low Level Tests: 2
  – High Level Tests
    • 1 Procedure
    • 7 Test Cases

Cert Documents:
• PSAC: 119 pages
• SDP: 79 pages
• SCMP: 42 pages
• SQAP: 26 page
• SVP: 86 pages
• SRS: 11 pages
• SDS: 14 pages
• SCS: 25 pages
A653 Extensions:
• IPC: 6256 SLOC
• Scheduler: 331 SLOC

A653 Drivers
• CAN: 761 SLOC
• Serial: 674 SLOC
• Common: 395 SLOC
Plan Architecture

SDP  SVP  SCMP  SQAP

PSAC
Plan for Software Aspects of Certification

- Contract with the certification authority
- Always submitted to the certification authority
- Describes the overall project and how DO-178 objectives will be satisfied
- Provides a summary of the other four plans
1. Section 1.1 mentions AC 20-115C. At this point, the AC doesn’t exist. Perhaps there should be a note stating this. Or, maybe “per AC 20-115C” could be “per the expected AC 20-115C” or “per the forthcoming AC 20-115C”. Another option is to not mention AC 20-115C.

By the time we actually use these documents for certification purposes we expect that the AC will exist. We could log a PR to ensure we check our documents against the AC, once it is finalized.

16Apr13 (LKR): I think a PR would be fine. Then if for some reason AC 20-115C isn’t out there, you can explain it in the S&S. The FAA has a draft now, so you should be okay.

1.3 states that part it is included in SCI but doesn’t give any information about the part number format. Normally, the PSAC at least gives the part number format (e.g., the first several digits) and explains that the specific dash number will be identified in the SCI. This probably isn’t a big deal but I just wanted to point out the typical.

Will have the PSAC reference the SCMP for the part number format.

16Apr13 (LKR): Response is acceptable.

When the verification lead and engineer are identified, it might be good to scope this role a bit. Does verification include reviews and test, or is it focused on testing? 1.4.1 clarifies a little but it might be good to mention it in 1.4.

Will clarify that this includes test, analysis, and review.

16Apr13 (LKR): Response is acceptable.

Should DO-330 be mentioned since tool qualification guidance is in that document? DO-178C references DO-330 for tool qualification guidance.

Will add a reference to this document.

16Apr13 (LKR): Response is acceptable.

Should the systems requirements document be listed since it drives the SW requirements? I know it isn’t a DO-178C artifact but it is input to the DO-178C process.

Will add a reference to this document.

16Apr13 (LKR): Response is acceptable.

This section states that the ARLX OS “is compliant with ARINC 653P1, P2 and P3”. However, the system requirements all seem to point to ARINC 653 Part 4. In general, the relationship between ARINC 653 Parts 1-4 are not clear.

The PSAC should only reference P4 at this point. Will update the PSAC accordingly.

16Apr13 (LKR): Response is acceptable.

Should this section mention that the OS is being developed for anticipated system and that once the specific system details are identified, a formal safety assessment will be performed and any adjustments made, etc.?

Will add description of how this information will be updated once a real system exists.

16Apr13 (LKR): Response is acceptable.
Software Development Plan

• Written for the developers
• It should guide the developers to successful implementation
• Describes
  – Standards used for development
  – Software Lifecycle
  – Development environment
<table>
<thead>
<tr>
<th>#</th>
<th>Accepted by:</th>
<th>Section</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SQAP</td>
<td>4.5</td>
<td>Quarterly involvement doesn’t seem adequate during the heavy times of a project. It’s more typical to provide goal for percentage of involvement rather than involvement per year. Instead we will have SQA perform audits when each lifecycle phase reaches 25, 50, 75, and 100% complete. 16Apr13 (LKR): Response is acceptable.</td>
</tr>
<tr>
<td>2</td>
<td>SQAP</td>
<td>4.7</td>
<td>It would probably be good to also include SQA witnessing or auditing of the test set-up here. Also, SQA involvement in test witnessing should probably be explained. Will add this information to this section. 16Apr13 (LKR): Response is acceptable.</td>
</tr>
<tr>
<td>3</td>
<td>SQAP</td>
<td>4.11</td>
<td>Why is a separate deviation process needed from the PR process? Care should be taken. Cert authorities may see this as a “hidden PR process.” If use a separate process, it should be treated like the PR process, including inclusion in the SAS. In general, I’ve found it is typically better just to include such deviations in the PRs and avoid the scrutiny. Possible exception may be if you expect a lot of deviations. Will clarify that all deviations are PRs and that the deviation process is what is followed to defer PRs. 16Apr13 (LKR): Response is acceptable.</td>
</tr>
<tr>
<td>4</td>
<td>General</td>
<td>NA</td>
<td>Many of the comments from the PSAC are also applicable to the SDP. In particular, Section 3 of the SDP, where the text is redundant. Such comments are not repeated in this report but should be considered when addressing the SOI 1 comments. These sections of the SDP will be updated by copying and pasting these sections from the PSAC. Need to make sure that these sections match in the PSAC, SDP, and SVP. 16Apr13 (LKR): Response is acceptable.</td>
</tr>
<tr>
<td>5</td>
<td>SDP</td>
<td>2.1, 2.2, and 2.3</td>
<td>It seems that the specific standards document # should be referenced in these sections (or, perhaps a reference to section 1.4.2) to ensure that the developers know the appropriate standards to use. Will reference the standard document number. 16Apr13 (LKR): Response is acceptable.</td>
</tr>
<tr>
<td>6</td>
<td>SDP</td>
<td>2.1.1</td>
<td>Where is the “DO-178C-specific requirements review checklist” located? This might be helpful for developers to know up front, so they can consider the questions during their development effort. Examples of these checklists are contained in the SVP. This issue will be addressed based on replies to other issues. 16Apr13 (LKR): Response is acceptable.</td>
</tr>
</tbody>
</table>
Software Verification Plan

- Written for the personnel who will perform verification activities
- Varies depending on the DO-178 software levels
- Explains how reviews, analysis, and tests will be performed
### SVP Finding Example

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>SVP</th>
<th>General</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>N/A</td>
<td>SVP</td>
<td>General</td>
<td>Many of the comments from the PSAC are also applicable to the SVP. In particular, Sections 2.1 and 4 of the SVP, where the text is redundant. Such comments are not repeated in this report but should be considered when addressing the SOI 1 comments. These sections of the SVP will be updated by copying and pasting these sections from the PSAC. Need to make sure that these sections match in the PSAC, SDP, and SVP.</td>
</tr>
<tr>
<td>F</td>
<td>Added to SVP review checklist as issue 165</td>
<td>1.2</td>
<td>This section states: “This plan will be used by the certification authority to determine if the Software Life Cycle Process is commensurate with the rigor required for the level of software being developed.” The plan is actually to be used by the verification team, not the cert authority.</td>
<td>Will clarify who is the user of the plan.</td>
</tr>
<tr>
<td>O</td>
<td>N/A</td>
<td>2.0</td>
<td>The “Team” and “Outsource” columns of the table are not clear. Should explain in the paragraph before the table.</td>
<td>There is a pending review comment concerning this as well. Will make this clearer.</td>
</tr>
<tr>
<td>O</td>
<td>Added to SVP review checklist as issue 348</td>
<td>3.2</td>
<td>The section states: “The following matrix shows the DO-178C objectives that will be satisfied with independence”. Should “as a minimum” be added, since in many cases you are also satisfying other objectives with independence through the peer review process?</td>
<td>Will add “at a minimum”.</td>
</tr>
<tr>
<td>C</td>
<td>N/A</td>
<td>3</td>
<td>Good job of explaining independence.</td>
<td>Thanks.</td>
</tr>
<tr>
<td>5</td>
<td>SVP-222</td>
<td>4.1</td>
<td>The section states: “Examples of the review checklists are contained in the appendices.” Why are these only considered as examples?</td>
<td>The checklists in practice are in Excel spreadsheets. They are the same questions but in a spreadsheet format. Since they are just a different format of the checklists should we remove “Examples of” or should we just reference the Excel checklists? Updated all applicable sections of the SVP to indicate that the baselined (not example) versions of the checklists are in the appendices.</td>
</tr>
</tbody>
</table>
Software Configuration Management Plan

- How configuration items are uniquely identified
- What is used for SCM
- Many companies have a company-wide SCMP
- If suppliers are used, this document describes the supplier’s SCM process
<table>
<thead>
<tr>
<th></th>
<th>HYP-28</th>
<th>SCMP</th>
<th>3.3</th>
<th>When does official problem reporting begin? After document is baselined or after it is released?</th>
<th>After the document is baselined.</th>
<th>Will clarify this.</th>
<th>16Apr13 (LKR): Response is acceptable.</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>HYP-28</td>
<td>SCMP</td>
<td>3.3.7.2</td>
<td>DO-248C DP #9 and EASA CM-SWCEH-002 provide some suggested classification schemes for PRs. These are often included in issue paper or CRI as well.</td>
<td>Will look at this document and update classification schemes accordingly.</td>
<td>16Apr13 (LKR): Response is acceptable.</td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>HYP-38</td>
<td>SCMP</td>
<td>3.4.12 .1</td>
<td>Since many projects are not under a TSO, the TC/STC definition of major/minor should also be included: 21.93. Order 8110.49 Ch 11 also has some info. In general, major/minor classification is controversial. Not sure it needs to be included for the OS level.</td>
<td>Will look at this document and update classification schemes accordingly.</td>
<td>16Apr13 (LKR): Response is acceptable.</td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>HYP-29</td>
<td>SCMP</td>
<td>3.5.3</td>
<td>Not sure the list is consistent with DO-178C section 11.16 (for example, the load instructions seem to be missing).</td>
<td>Will add missing items j and k from DO-178C to this list.</td>
<td>16Apr13 (LKR): Response is acceptable.</td>
<td></td>
</tr>
<tr>
<td>?</td>
<td>HYP-29</td>
<td>SCMP</td>
<td>3.5.3</td>
<td>When is the SCI prepared?</td>
<td>Will add a reference to the baseline section where this is discussed.</td>
<td>16Apr13 (LKR): Response is acceptable.</td>
<td></td>
</tr>
</tbody>
</table>
Software Quality Assurance Plan

• Describes the plan for assuring that the software complies with the approved plans and standards, as well as the DO-178C objectives
• Describes the software QA engineer’s role
• Who is on the QA team
<table>
<thead>
<tr>
<th></th>
<th></th>
<th>SQAP</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>N/A</td>
<td>SQAP</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Document has been reviewed but not updated. Need to look at the differences. Please provide redlines.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Will provide once the review has been closed out.</td>
</tr>
<tr>
<td>O</td>
<td>N/A</td>
<td>SQAP</td>
<td>1.4.2</td>
<td>Some of the internal documents do not have document #s (e.g., standards, change impact analysis process, deviation process)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Will give the standards a number. This was resolved as part of the SQAP review.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The Change Impact Analysis Process is documented in the SCMP and the Deviation Process is documented in the SQAP. Do they need to be separated out into individual documents?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16Apr13 (LKR): No, they do not need to be separated as long as it is clear where they are. It also should be clear what the scope of the CIA process is. Does it cover during development, after formal test, and/or after certification? Oftentimes, there are slight differences in the process depending on the phase of the project.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Response about standards #s is acceptable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16Apr13 (LKR): No, they do not need to be separated as long as it is clear where they are. It also should be clear what the scope of the CIA process is. Does it cover during development, after formal test, and/or after certification? Oftentimes, there are slight differences in the process depending on the phase of the project.</td>
</tr>
<tr>
<td>5</td>
<td>N/A</td>
<td>SQAP</td>
<td>1.4.2</td>
<td>Are the change impact analysis process and deviation process separate documents? If so, they should be included in the SOI 1 data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The Change Impact Analysis Process is documented in the SCMP and the Deviation Process is documented in the SQAP. Do they need to be separated out into individual documents?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HYP-209 created to address this issue.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16Apr13 (LKR): No, they do not need to be separated as long as it is clear where they are. It also should be clear what the scope of the CIA process is. Does it cover during development, after formal test, and/or after certification? Oftentimes, there are slight differences in the process depending on the phase of the project.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Response about standards #s is acceptable.</td>
</tr>
<tr>
<td></td>
<td>Added to SQAP review checklist as item 301</td>
<td>SQAP</td>
<td>4.1.1</td>
<td>Will SQA ensure that the environment complies with SECI? This is typical – especially prior to formal testing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Will add this information to this section.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16Apr13 (LKR): Response is acceptable.</td>
</tr>
</tbody>
</table>
• Galois tasked with performing initial Formal Methods analysis during Phase I.
  • Formal model of three scheduler subroutines
  • Created formal specifications of the subroutines’ functional correctness and properties
• Worked with Rockwell Collins to create initial target of evaluation (TOE).
  • Initial analysis
    • 551 functions
    • 76 files
    • 26K SLOC
• Accuvant- white hat hacking ARLX/Xen
  • Accuvant will deliver a final report – any identified vulnerabilities will be addressed in the developed validation guard
• We realize that safety and security artifacts are expensive, so we set out to work with Rockwell Collins to establish a method of proving security that fits our business model of giving away the software for free.
• SKPP is being deprecated
  • Moving towards a certification system similar to that of DO-178, meaning that the system is the focus of security as opposed to specific pieces.
• NIAP has concerns with the SKPP related to lifecycle costs and meaningful assurance. Therefore judiciously scalable analysis methods will be employed to:
  • Minimized lifecycle costs
  • Focus the efforts on high-value security concerns (i.e. areas where proper data flow is critical)
• RC conducted formal analysis process suitable for high assurance environments with multiple levels of security
What we did

- Rockwell Collins analysis guided by Separation Kernels in Environments Requiring High Robustness (SKPP)
  - Conformance with SKPP requires a minimum Evaluation Assurance Level of 6.
- Formal models and report of analysis were developed and delivered as a security document
- Investigated the ARLX ARINC 653 scheduling subsystem
  - Identified the target of evaluation (TOE)
  - Identified the security boundaries – any component that is accessible from outside of the TOE (interface to the system)
  - Structural analysis of the TOE – to ID the scope of the effort
- Functional security requirements are created for the TOE
ARLX Security Policy
Formal Methods Results

• One failure
  – only one procedure, ioapic_guest_write(), which, it turns out, is not in the schedule TOE

• 3672 exceptions
  – Over half of these exceptions are due to assembly language

• Still a relatively manual process to evaluate the exceptions
  – Do they violate the security policy or are they outside of the security policy
  – Do they contain assembly language (goal is to add assembly language analysis)
What we learned

• A study comparing the certification requirements of DO-178 Level A and Common Criteria [1]
  – Concluded that a product that is used in a DO-178 certified system could achieve up to Common Criteria EAL 7 by completing a few missing requirements
  – Most significant missing requirements are those that pertain to formal analysis.

• Safety and security are closely related

• Adhering to a certified safety process, lends itself to a more secured system and makes the security certification process less time consuming