ELISA
Enabling Linux in Safety Applications

WORKSHOP

ELISA Workshop
Munich, Germany

November 18-20, 2025
Co-hosted with Red Hat

Industry Safety Level(s) vs. Aerospace Use Cases

ELISA
Enabling Linux in Safety Applications

Matthew Weber

Associate Technical Fellow @ The Boeing Company

ELISA Enabling Linux in Safety Applications

WORKSHOP

Aerospace Working Group

Charter:

"… shall develop use cases to inform and influence Linux architecture and related tools, work to derive technical requirements for avionics operating systems, and seek to enhance and expand avionics software lifecycle processes, practices, and tools to enable use of Linux in avionics systems that are certified to high design assurance levels."

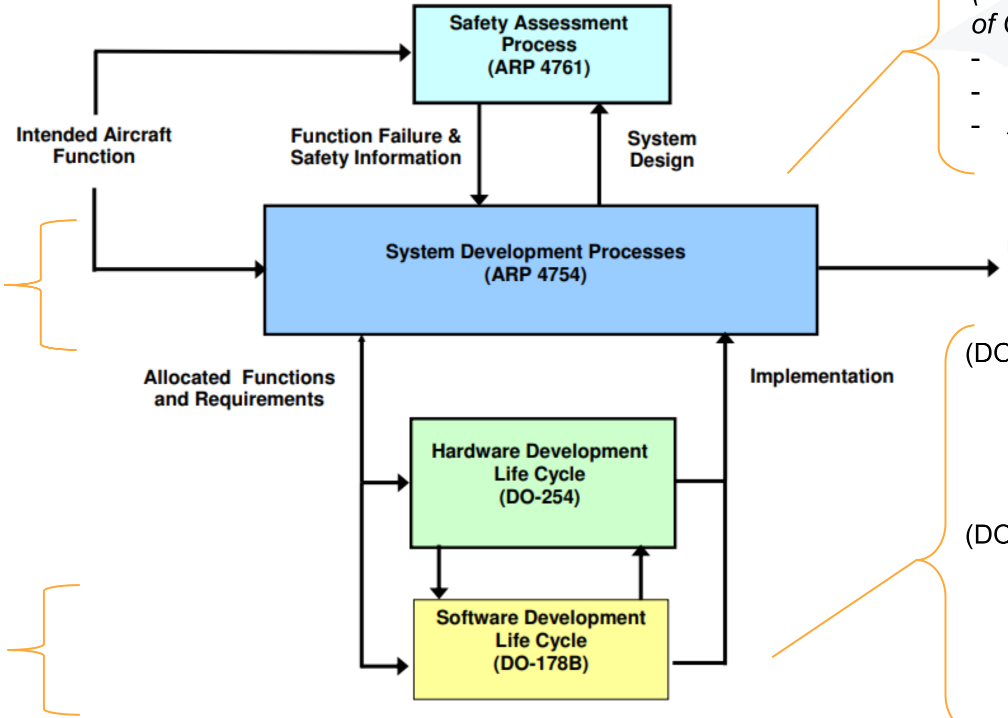
Agenda

- Aircraft Development Cycle
- DO-178C Safety Levels
- Safety Levels vs. Certification Artifacts
- A Comparison with Other Hazard Level Standards
- Use cases
- Demo

Aircraft Development Cycle

Design Assurance Level (DAL)

Software Level (SWL)



By: Alessandro Nicoli de Mattos
Standards relationship diagram and list of documents by other authors
Rev A - Jul/2012

Aerospace Recommended Practice (ARP) - Guidelines for Development of Civil Aircraft and Systems

- *Functional Safety*
- *Design assurance processes*
- *Assigns DAL to mitigate failure conditions and hazard severity*

(DO-178C Sec. 2.3) “only partitioned (time&space) software components can be assigned individual SWL by the system safety assessment process.“

(DO-178C Sec. 2.4) “if partitioning and independence between software components cannot be demonstrated, all components are assigned the SWL associated with the **most severe failure condition** to which the software can contribute”.

ELISA Enabling Linux in Safety Applications

WORKSHOP

DO-178C Safety Levels

“Software Considerations in Airborne Systems and Equipment Certification.” is published by RTCA (Radio Technical Commission for Aeronautics) - DO-178C provides guidance for ensuring the safety, reliability, and airworthiness of software used in commercial and military aircraft.

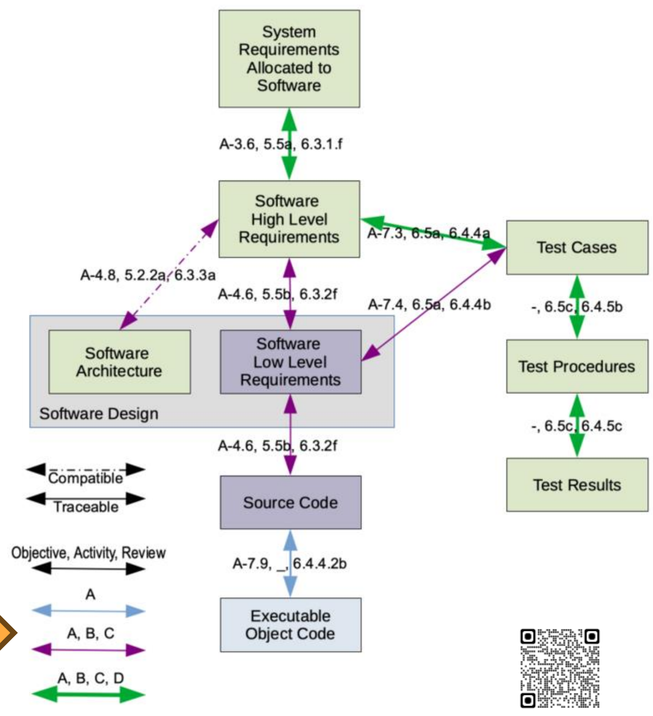
Level	Severity	Example Impact	Example system
A	Catastrophic Failure	Multiple fatalities, loss of aircraft, irrecoverable	Flight control system, Terrain Awareness Warning System (TAWS)
B	Hazardous/Severe Failure	Large impact, severe injuries, a fatality	Legacy Flight Management System(FMS), Engine-Indicating and Crew-Alerting System
C	Major Failure	Discomfort, minor injuries, increased crew workload	Datalinks, Fuel monitoring
D	Minor Failure	Inconvenience	Maintenance, Cabin Lighting, WiFI
E	No Safety Effect	No impact to airplane operation or comfort	Cargo, Entertainment

https://real-time-consulting.com/wp-content/uploads/2025/03/Understanding-DO178C.pdf
https://thecloudstrap.com/design-assurance-level-dal-in-do-178c/

ELISA Seminar talk
with more detail

Safety Levels vs. Certification Artifact

Example:
Artifact
Trace



By Steven H. VanderLeest - Own work, CC BY-SA 3.0,

Example: DO-178C Annex A

The Annex outlines process objectives, activities and outputs by software level

	Objective		Activity	Applicability by Software Level				Output		Control Category by Software Level			
	Description	Ref	Ref	A	B	C	D	Data Item	Ref	A	B	C	D
1	The activities of the software life cycle processes are defined.	4.1.a	4.2.a 4.2.c 4.2.d 4.2.e 4.2.g 4.2.i 4.2.l 4.3.c	○	○	○	○	PSAC	11.1	①	①	①	①
								SDP	11.2	①	①	②	②
								SVP	11.3	①	①	②	②
								SCM Plan	11.4	①	①	②	②
								SQA Plan	11.5	①	①	②	②
	The software life cycle(s), including the inter-relationships							PSAC					

Table example - https://www.parasoft.com/learning-center/do-178c/what-is/

A Comparison with Other Hazard Level Standards

Approximate cross-domain mapping of ASIL

Domain	Domain-Specific Safety Levels							Failure Rates [3,4]
Automotive (ISO 26262)	QM	ASIL A 1E-5			ASIL B <= 1E-6	ASIL C <= 1E-7	ASIL D <= 1E-8	- [1]
General (IEC 61508)	-	SIL-1 1E-5			SIL-2		SIL-3	SIL-4 <= 1E-9
Railway (CENELEC 50126/128/129)	-	SIL-1			SIL-2		SIL-3	SIL-4
Space (ECSS-Q-ST-80)	Category E	Category D			Category C		Category B	Category A
Aviation: airborne (ED-12/DO-178/DO-254)	DAL-E	DAL-D 1E-5			DAL-C <= 1E-5		DAL-B <= 1E-7	DAL-A <= 1E-9
Aviation: ground (ED-109/DO-278)	AL6	AL5			AL4	AL3	AL2	AL1
Medical (IEC 62304)	Class A	Class B					Class C	-
Electrical controls (IEC 60730)	Class A	Class B					Class C	-
Machinery (ISO 13849)	-	PL a	PL b	PL c	PL d	PL e	-	-
Agriculture (ISO 25119)	AgPL QM	AgPL a	AgPL b	AgPL c	AgPL d	AgPL e	-	-

[2]

Military (MIL-STD-882E), "Level of Rigor"
NASA (NPR 7150.2), "Class"

[1] https://www.rapitasystems.com/blog/whats-difference-between-sil-and-dal-how-does-it-affect-my-code-coverage
[2] https://en.wikipedia.org/wiki/Automotive_Safety_Integrity_Level#Comparison_with_Other_Hazard_Level_Standards
[3] https://www.rapitasystems.com/do178c-testing (DO-178C Failure Rate)
[4] https://en.wikipedia.org/wiki/IEC_61508#Probabilistic_analysis (SIL Failure Rate)

ELISA Enabling Linux in Safety Applications

WORKSHOP

Use Cases

Our Process:

1) Propose, 2) Capture, 3) Establish concept, 4) Demo in environment, and 5) Publish results

Level	Severity	Case	Goals
A/B/C	Catastrophic Failure	Fault Tolerant (1) High Integrity Compute (1) Cabin Lights (1)	- Mixed criticality architecture w/ partitioning - Minimal Codebase / configuration defined - Fault tree / recovery / injection - Voting schemes - IO and protocol approach appropriate for level
D	Minor Failure	Cabin Lights (5) Cabin Lights w/ cFS (2)	- First use case - Established outline to capture use cases - Runtime Verification w/ Copilot - Basic build/emulation/test workflow (patches welcome!) - Environment/Tool container
E	No Safety Effect	Attested Boot (1)	- Boot chain integrity/authenticity

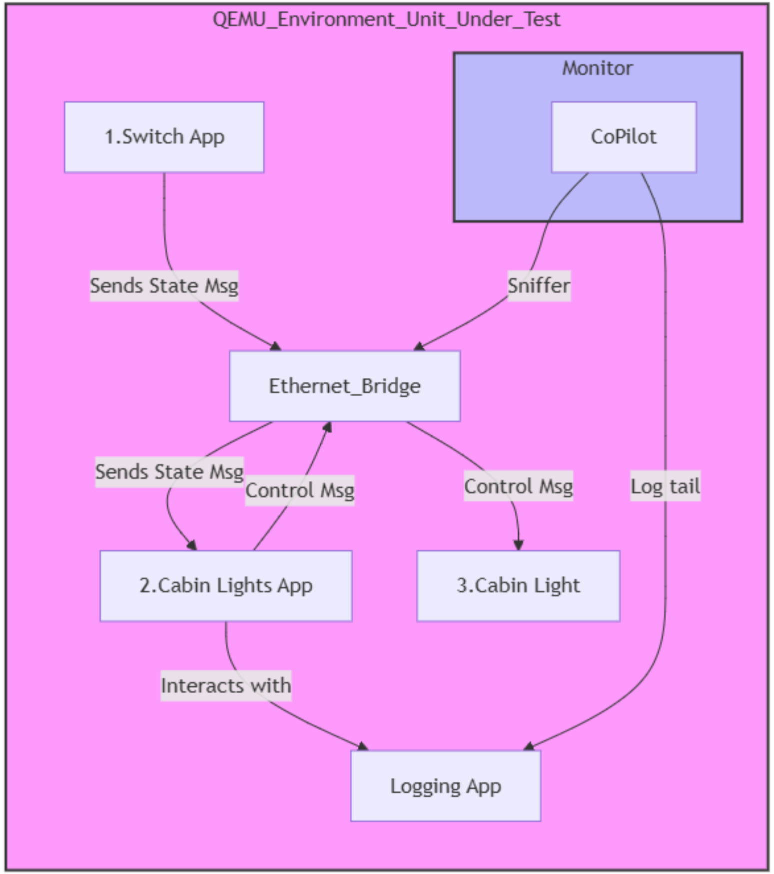
ELISA Enabling Linux in Safety Applications

WORKSHOP

Please suggest new Use Cases or upvote/add notes on existing!

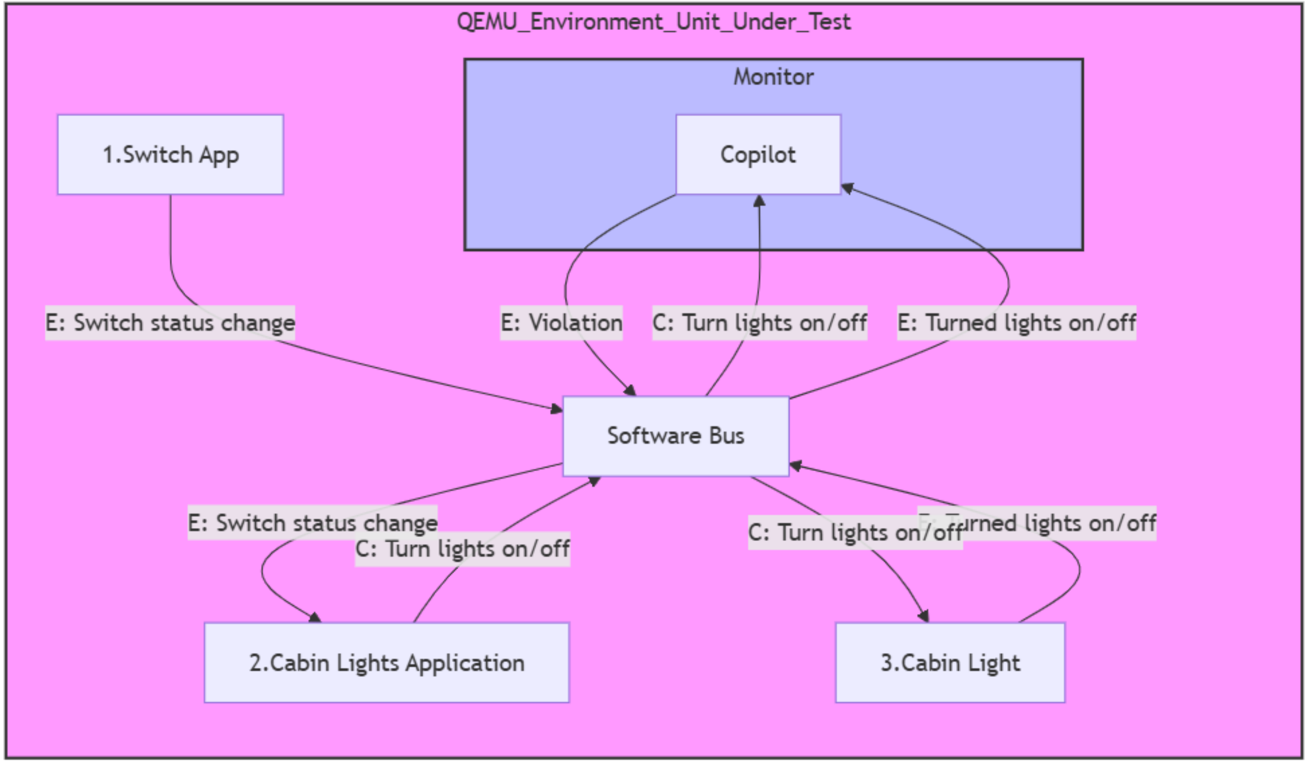
Demo: Cabin Lights

- Requirements
  - The Cabin Lights system shall turn lights on in less than 500 ms of the light switch turning on.
  - The Cabin Lights system shall turn lights off in less than 500 ms of the light switch turning off.
- Design
  - Switch, Server and Actuator(Light)
  - Ethernet and system logging are used
- Test / Demo approach
  - Applications are paired with CoPilot monitoring of logs / package



ELISA Enabling Linux in Safety Applications WORKSHOP

Demo: NASA Core Flight System (cFS)



Maturing Steps*

1) Demo cFS Sample app
2) Demo monitor event from sample app
3) Create Lights demo w/ framework**
4) Create Switch + Lights demo

* Assumes cFS running in embedded minimal Linux
** Ogma – generator of runtime monitors

ELISA Enabling Linux in Safety Applications

WORKSHOP

How to engage with us?

Join our monthly call(s)

- 2^{nd} Thursday – "General Topics"
- 3^{rd} Thursday – Space Grade Linux SIG
- 4^{th} Thursday – "Industry Papers" working session
- Weekly (Friday) – "Use Case" testing call

Mailing list / repos / resources

https://lists.elisa.tech/g/aerospace

Register here to receive a calendar invite

https://elisa.tech/community/meetings/

ELISA Enabling Linux in Safety Applications

WORKSHOP

Licensing of Workshop Results

All work created during the workshop is licensed under Creative Commons Attribution 4.0 International (CC-BY-4.0) [https://creativecommons.org/licenses/by/4.0/] by default, or under another suitable open-source license, e.g., GPL-2.0 for kernel code contributions.

You are free to:

- Share — copy and redistribute the material in any medium or format
- Adapt — remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Thank you for attending!