



ELISA

Enabling **Linux** in
Safety Applications

ELISA Workshop London, UK

June 9-11, 2026

Co-hosted with Canonical

Eclipse S-CORE and AoUs to the Operating System

Philipp Ahmann, ETAS GmbH

ELISA Workshop: London, UK

June 9-11, 2026

Co-hosted with Canonical



Eclipse S-CORE status



What it is? (And what is it not...)

- **Safety-critical automotive grade middleware stack on top of POSIX OS**
- The Eclipse *Safe Open Vehicle Core* project aims to develop an open-source core stack for Software Defined Vehicles (SDVs), specifically targeting embedded high-performance Electronic Control Units (ECUs).
- S-CORE is not a ready-to-integrate series product. It is a generic foundation for commercial distributions. Responsibility for ASPICE, ISO 21434 (cybersecurity), and ISO 26262 (functional safety) compliance of the final system always remains with the series project.

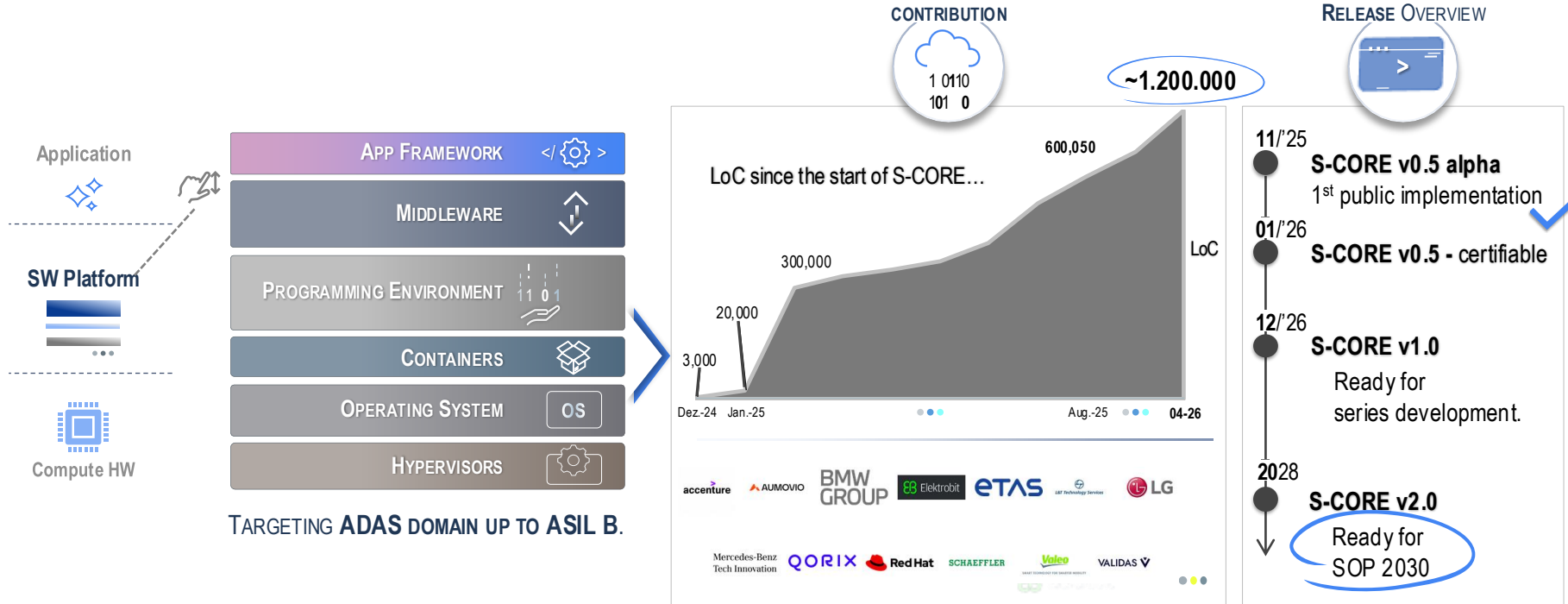
<https://projects.eclipse.org/projects/automotive.score>

Eclipse S-CORE in a nutshell

The Project is up and running, and on track according to our release plan.

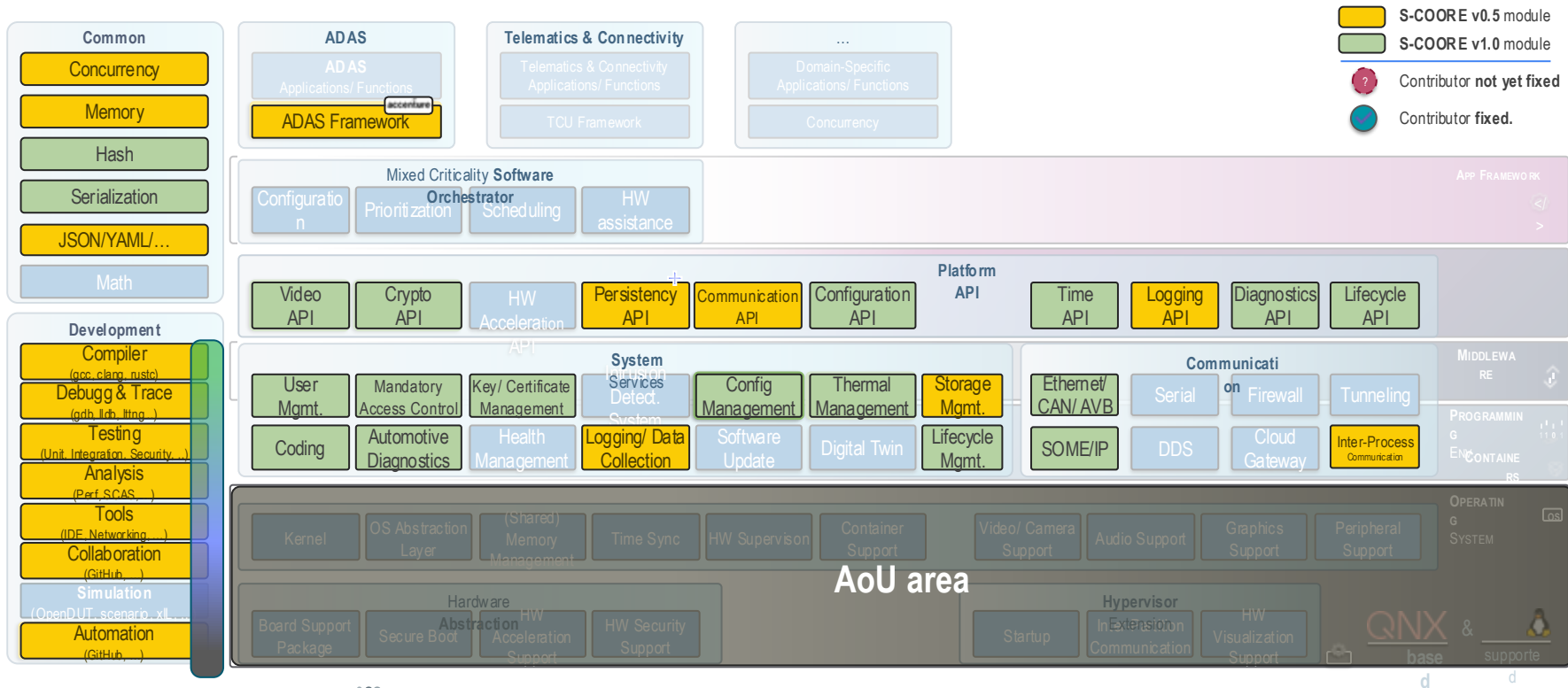
Eclipse S-CORE, **first open-source standard** to be deployed in **safety-critical automotive series projects**.

After **~1,5 years**, the project is up and running, ... and on-track to **provide a complete solution by 2028**.

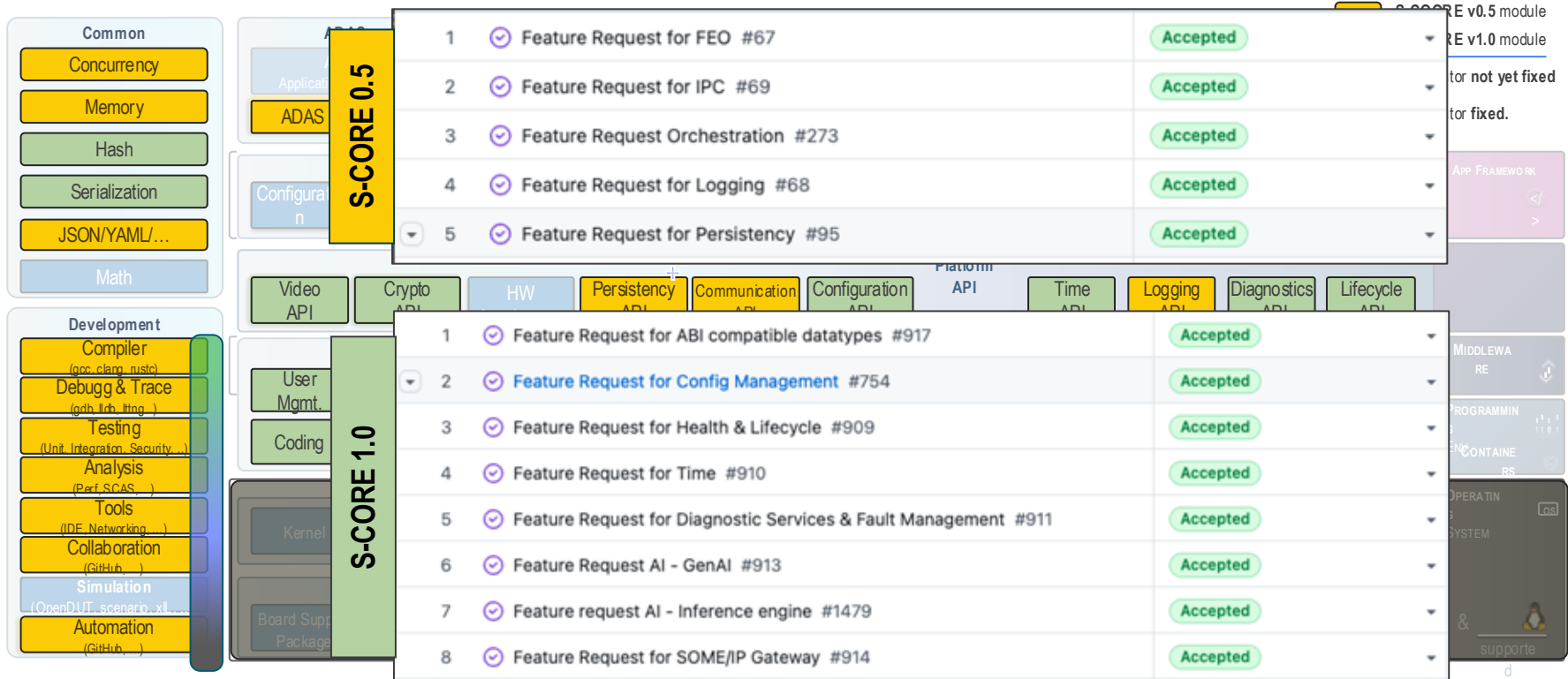


S-CORE SW-PLATFORM | THE MIDDLEWARE IS IN FOCUS OF THE RELEASE 0.5.

RELEASE 1.0 WILL HAVE A BIGGER SCOPE & COVER MOST PARTS OF THE SW-PLATFORM



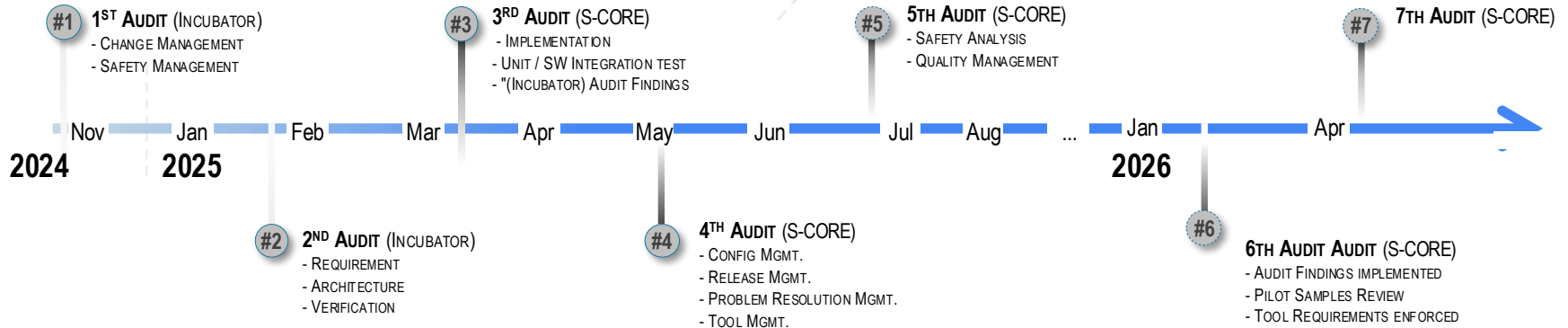
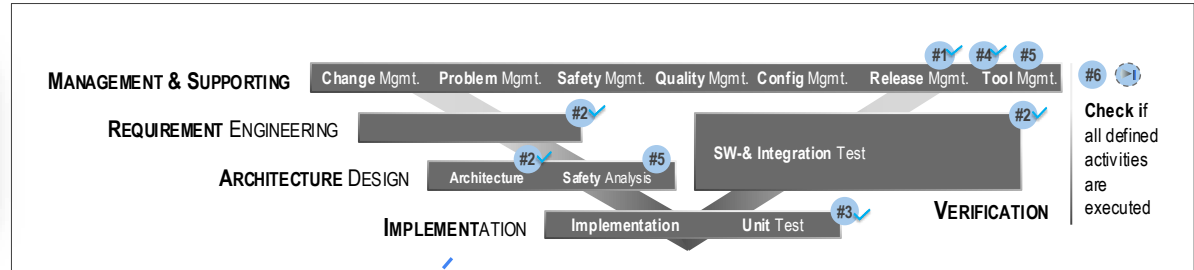
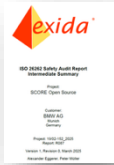
S-CORE SW-PLATFORM | THE MIDDLEWARE IS IN FOCUS OF THE RELEASE 0.5.
RELEASE 1.0 WILL HAVE A BIGGER SCOPE & COVER MOST PARTS OF THE SW-PLATFORM



Eclipse S-CORE's Process Setup

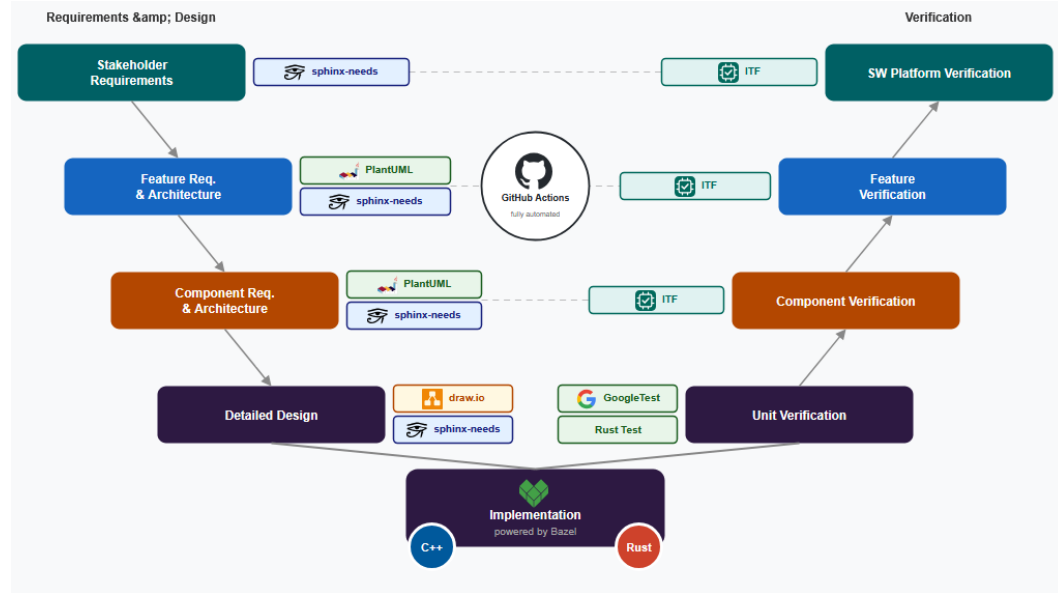
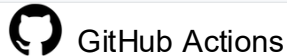
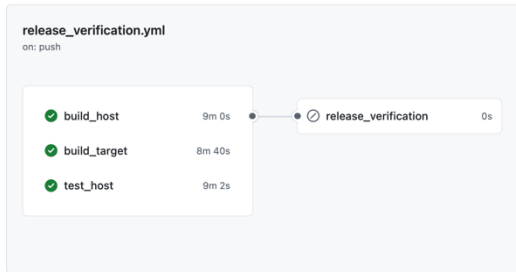
Ensure efficient development of Software as well as complimentary work products.

Exida is continuously conducting Safety Audits of S-CORE, in order to ensure standard compliance.



Eclipse S-CORE's Toolchain Setup

A fully open-source toolchain is established



Linux in S-CORE



ELISA Member Linux provider (or engagement)



Assumptions of use on...

- Environment
- The external SW element integration
- Application
- Safety System

https://eclipse-score.github.io/score/main/requirements/platform_assumptions/index.html

OS Safety functions

If the system using the SW-platform has safety goals, the used OS module shall offer the following safety related functions:

- configuration of HW safety mechanisms as in [Safe HW platform \(aou_req_platform_hardware_safety\)](#)
- startup of OS
- loading and starting of processes
- management and restriction of process privileges
- process execution (including starting and stopping threads/processes according to priorities, management of interrupts and exceptions)
- volatile memory management (including static, dynamic memory allocation and access)
- filesystem access (data integrity of read-only-memory)
- DMA
- IPC communication primitives (shared memory and message passing)
- C++ standard library (according to ISO 14882)
- C library
- math library
- high precision time source (HW synchronized)

Taken from here: [aou_req_platform_os_safety_functions](#)

Process isolation

- If the system using the SW-platform has safety goals, the used operating system shall offer POSIX processes isolation.
 - This shall cover memory isolation.
 - Timing isolation may be covered.

Safe HW platform

- [HW Self-Test \(stkh req dependability safety features 3\)](#)
- [Safe Startup and Reset \(stkh req dependability safety features 4\)](#)
- [DMA Protection \(stkh req dependability safety features 5\)](#)
- [Memory Protection \(stkh req dependability safety features 6\)](#)
- [Cache Protection \(stkh req dependability safety features 7\)](#)
- [Memory Error Correction \(stkh req dependability safety features 8\)](#)
- [External Supervision \(stkh req dependability safety features 10\)](#)

Note: These safety mechanisms are mostly OS/Hypervisor/HW specific, ...

Examples:

- The SW-platform shall support IO MMU protecting DMA accesses
- The SW-platform shall support Memory Management Unit
- The SW-platform shall support Power management integrated circuit (PMIC), external watchdog and voltage monitoring

Note: Support means here that a functionality offered by external SW (e.g. an OS) or HW may need to be configured and used.

DMA Protection	status: valid security: YES safety: ASIL_B	⊕
tags: safety_mechanism rationale: DMA function usually grants also QM HW direct access to memory. reqtype: Functional valid_from: v1.0.0		
The SW-platform shall support IO MMU protecting DMA accesses		
Note: Support means here that a functionality offered by external SW (e.g. an OS) or HW may need to be configured and used.		
stkh_req__dependability__safety_features_5	Stakeholder Requirement	

Memory Protection	status: valid security: YES safety: ASIL_B	⊕
tags: safety_mechanism rationale: ASIL SW components memory may be corrupted by QM SW components if those are located on the the same physical memory. reqtype: Functional valid_from: v1.0.0		
The SW-platform shall support Memory Management Unit		
Note: Support means here that a functionality offered by external SW (e.g. an OS) or HW may need to be configured and used.		
stkh_req__dependability__safety_features_6	Stakeholder Requirement	

Thank you!
Questions?



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.