Safety Element Out-of-Context (SEooC) Solution

INTRODUCTION

This white paper examines the standards and guidelines for avionics and automotive safety-critical software and hardware to show how cost savings in commercial solutions can be achieved. We begin with a description of how software and hardware requirements are traditionally developed, followed by an examination of how guidelines for commercial solutions are developed 'out-of-context' of a typical safety application. Next, this paper will describe the process of selecting a solution and putting the solution into the safety application context. Finally, it details how safety certification is supported and describes examples of commercial solutions available and in use today.

TRADITIONAL SAFETY-CRITICAL DEVELOPMENT

The basis for avionics and automotive industry guidelines and standards is a documented "V" software and hardware development process: demonstrate what you are going to do, accomplish it, and prove that you achieved what you stated you would. Beyond this basis, there is additional rigor applied to certain activities. This rigor and some activities are modulated by the Design Assurance Level (DAL) in avionics, while only the rigor is modulated by the Automotive Safety Integrity Level (ASIL) for automotive.

Both avionics and automotive industries typically employ a similar V-model development flow in which new software and hardware are developed to meet requirements passed down from the system level.

In avionics, as described in ARP 4754A and ARP 4761, there is a Functional Hazard Analysis (FHA) conducted at the aircraft function level to assist in determining the system architectural requirements along with failure effects and probability budgets for the system. At the system level, this data along with a Preliminary System Safety Assessment (PSSA) is used to help define safety requirements for the software and hardware modules (in addition to the functional requirements).

The approach is similar for automotive, as described in ISO 26262. There is a Hazard Analysis and Risk Assessment (HARA) at the concept level to develop the functional safety concept for the system. This along with system development results in technical safety requirements (requirements for safety and function) for software and hardware level development.

The degree of process modulation in addition to safety requirements differs greatly from typical Commercial Off The Shelf (COTS) products; however, do these differences exclude the possible use of commercial solutions?

CAN COMMERCIAL SOLUTIONS BE USED?

A safety-critical-ready commercial solution, developed to recognized processes with appropriate audits and inspections and no restriction on functionality, could significantly reduce overall cost and schedule for safety-critical application development. This can range from a Non-Developmental Item (NDI), to the configuration of an NDI, to customization development. That is, it takes advantage of previously developed elements as opposed to ground-up custom development.

Let's look at the provisions for a safety-critical-ready commercial solution in both avionics and automotive guidance and standards.

In the avionics industry, previously developed software and hardware are described in DO-178C and DO-254 and encompass COTS products as well as elements developed to previous or current guidance. Similarly, in the automotive industry, ISO 26262 has provisions that apply to used commercially available elements:

- The proven argument to make use of components that have been used in systems that pre-date ISO 26262.
- The qualification stage for software, where the objective is to provide evidence of suitability for reuse in items being developed in compliance with ISO 26262.
- The SEooC, in which software or hardware are not developed based on the specific requirements of an application (context) but on assumptions, and developed per ISO 26262 (safety).

A key difference between qualification and SEooC is that an SEooC development process is similar to the functional safety lifecycle; it is developed per ISO 26262 rather than another industry specification, which makes an SEooC approach less risky.

While avionics uses Previously Developed Software (PDS) and Previously Developed Hardware (PDH), which have a broad definition, automotive uses SEooC, which is more specific. It is developed to safety standards and guidelines (safety element) without consideration of the specific application or system requirements (out-of-context). SEooC is an ideal way of capturing what an application developer would look for regardless of industry. From this point forward SEooC will be used to refer to safety-critical ready commercial software and hardware elements.

For safety-critical development, SEooC promises a significant reduction in certification cost through modularization and reuse of element certification evidence. This will be addressed later in this paper.

Now that we have established that safety-critical-ready commercial solutions can be used, we can return to requirements that, for an SEooC, are assumed requirements (i.e. bottom-up defined) and examine their intersection with flow-down requirements from the system level (i.e. top-down defined).

SELECTING A SOLUTION

The decision to use an SEooC includes both system requirements and business (cost and schedule) considerations. The business considerations will depend on the extent to which the SEooC (assumed requirements) meets the system technical and safety requirements (flow-down requirements). Let's look at the flow for evaluating technical considerations.

The following is a process overview for selecting an SEooC solution in the context of an application.

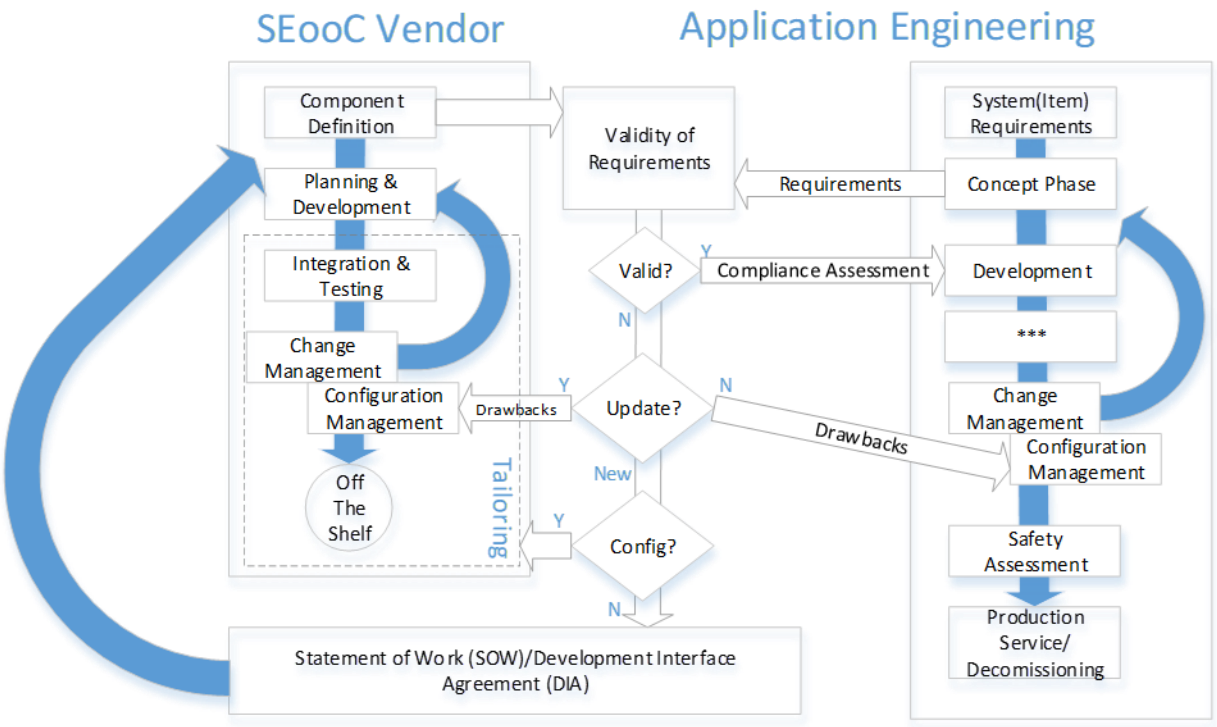

Figure 1: Process Overview for Selecting an SEooC

The requirements assessment approach is:

1. Assess the validity of the requirements by evaluating product briefs to determine if the functional, technical, and safety requirements (including DAL/ASIL level) address the application requirements within the system architecture.
2. If there is a mismatch in requirements, the following actions may be taken:
   - The SEooC vendor may issue a problem report and correct the identified drawback.
   - The system integrator may decide to address the drawback through a change in the system architecture and/or application, resulting in compliance.
   - An evaluation may be conducted to see if the product can be tailored via a different build configuration (a software example would be to target a different host processor, GPU, and/or RTOS).

- If the drawback goes beyond tailoring, a Statement of Work (SoW) or Development Interface Agreement (DIA) is required to describe the requested additional and/or changed product requirements.

ISO 26262 describes the use of the DIA for successful planning and execution of activities and work products between a customer and supplier; the DIA is a specific implementation of a Statement of Work. For products off the shelf, a DIA is not required, while for custom developments a DIA is used to define and agree to the aspects of development activities and provided work products. Please see the DIA section of relevant product briefs for more information.

PUTTING A SELECTED SOLUTION INTO CONTEXT

ISO 26262 has an additional item beyond what avionics guidelines mention, although it is similar in concept to documentation needed in the case of a Technical Standard Order Authorization (TSOA). The SEooC developer must document usage, assumptions, issues, and more, of the SEooC for customers. This documentation is normally delivered in a safety manual but may be delivered in a safety application note. While not specifically called DO-178C and DO-254, this data is equally useful to avionics application development. In avionics, a safety manual can refer to a different type of document entirely, so the title User Integration Manual (Safety Manual) is used, making it common for both avionics and automotive customers.

From a system safety perspective, assuring the safe and correct function of an element does not mean the integrated system will remain safe. This is where the User Integration Manual (Safety Manual) provides the necessary information to gain an understanding of the SEooC use in the context of safety-relevant applications. The User Integration Manual (Safety Manual) provides the following information that applies to software and hardware elements: (This list is not exhaustive; it is tailored to each product.)

- Document assumptions
  - Possible use scenarios (not limited to those listed)
  - Design constraints
    - Timing
    - Memory usage
    - Resource items and usage
    - Requirement on the run-time environment
  - External interfaces
  - DAL/ASIL classification
- Description of potential safety requirements fulfilled by the element
- Description of how the element must be configured and integrated
- Any post-integration module testing that must be performed
  - Example: verification procedures, especially for verification activities that the integrator or vendor must repeat for the integrated software.

- Description of known safety impacting issues:
  - Vulnerabilities
  - Partitioning requirements
  - Hardware failure effects
  - Data latency
  - Deactivated code
  - Unused hardware functions
  - Behavior in an overload situation (robustness)

SAFETY CERTIFICATION SUPPORT

System assurance is based on component assurance data and integration assurance data. The SEooC vendor must provide a certification data package (safety case) for each element. The certification data package provides the deliverable lifecycle data items to demonstrate compliance against the objectives in DO 178C, DO-254, and ISO 26262 as needed by certification authorities and third party certification. Additional lifecycle data can be viewed at the SEooC vendor's premises. A list of lifecycle data and all other deliverables is included in applicable product briefs.

SEooC vendors typically involve Federal Aviation Administration (FAA) Designated Engineering Representatives (DERs) and ISO 26262 auditors to provide oversight during development and to provide compliance letters demonstrating that, in their opinion, the product is suitable for obtaining system-level certification.

For non-DIA driven ISO 26262 SEooC solutions, or as included in a DIA, an accredited safety assessment certificate is available.

For hardware products, an FAA TSO-C153A IMA hardware authorization may be available.

SEooC SOLUTIONS FOR AVIONICS AND AUTOMOTIVE

Wouldn't it be cost and schedule efficient to find software and hardware SEooC solutions for both avionics and automotive safety-critical applications and be able to source these platform solutions from one supplier? While there is a growing number of solution providers in the automotive space, there is one that provides safety-critical software and hardware for both automotive and avionics market spaces - Core Avionics & Industrial Inc. (CoreAVI).

CoreAVI develops driver and library software, most to industry API standards, and Single Board Computer (SBC) and graphics hardware modules following industry standards. Using industry standards such as those provided by the Khronos® Group, VITA, SOSA™, and FACE™ for safety-critical rugged compute and graphics capabilities, CoreAVI can define the functional requirements and interfaces for use in most rugged embedded safety-critical applications independent of the application context.

CoreAVI's software and hardware elements are developed following DO-178C/DO-254/ISO 26262 processes to produce the lifecycle data required to allow each element to be used in a safety-relevant application.

Development occurs without the knowledge of the system-level design or requirements. CoreAVI product management defines the functional and interface requirements for the element to address an industry need and interoperate with other CoreAVI products to further enable platform solutions. To ensure products can be used across a wide range of applications, there is a requirement for the most stringent DAL/ASIL applicable.

Beyond technical functional requirements and development process, there are additional considerations when developing safety-critical products. While hazard and safety assessments are performed at the platform and system levels to define the safety requirements that flow down, these are not requirements that can be easily assumed when developing an SEooC. CoreAVI has gained extensive experience from working with many safety-critical systems and application developers; experience that is incorporated into design standards to ensure products not only meet technical feature requirements but safety requirements as well. For hardware developments, Failure Modes and Effects Analysis (FMEA) is also performed and used to determine additional safety requirements for the product.

CoreAVI works with FAA DERs and TUV ISO 26262 auditors for oversight of the SEooC developments. Resulting safety-critical process evidence is documented in the CertCore178C, CertCore254, and CertCore26262 product briefs.

CoreAVI reduces the cost of critical embedded systems by mutualizing the developments for various safety standard domains to provide components that can be reused across industries. CoreAVI also provides licensing for lower DAL/ASIL usage. This ensures any cost advantage expectation of top-down development for a lower DAL/ASIL level can be met.

CONCLUSION

This white paper has examined the current standard and guidelines for avionics and automotive safety-critical software and hardware development and has demonstrated how using commercial solutions is possible. This paper has described a process for selecting a commercial solution and putting it into a safety application context. It has introduced how some available commercial solutions are developed to be safety ready and are in use in safety-critical applications around the world.

DEFINITIONS

- **Component**: A non-system level element that is logically and technically separable and comprises more than one hardware part or one or more software units.
- **Element**: A system or part of a system including components, hardware, software, hardware parts, and software units.
- **Hardware part**: Hardware that cannot be subdivided
- **Item**: A system or array of systems to implement a function at the vehicle level to which ISO 26262 is applied.
- **Software component**: One or more software units.
- **Software unit**: An atomic-level software component of the software architecture that can be subjected to stand-alone testing.
- **TSO Authorization**: Legal recognition by the certification authority that a system, equipment or part satisfied the TSO requirements and minimum specification applicable for that equipment (MOPS).