Statement

ATI ACCURATE TECHNOLOGIES

International Electrotechnical Commission (IEC) 61508:

IEC 61508 creates requirements to ensure that systems are designed, implemented, operated, and maintained at the safety level required to mitigate the most dangerous risks. The international standard is used by a wide range of manufacturers, system engineers, designers, and industrial companies, and others that are audited based on compliance. The standard applies to safety-critical products including electrical, electronic, and programmable-related systems.

The ISO 26262 series of standards is the adaptation of IEC 61508 series of standards to address the sector specific needs of electrical and/or electronic (E/E) systems within road vehicles. This adaptation applies to all activities during the safety lifecycle of safety-related systems comprised of electrical, electronic and software components.

International Organization for Standards (ISO) 26262 (2018): Intent

Intended for:

This document is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles, excluding mopeds. This document does not address unique E/E systems in special vehicles such as E/E systems designed for drivers with disabilities.

Not intended for:

Systems and their components released for production, or systems and their components already under development prior to the publication date of this document, are exempted from the scope of this edition.

Not a sole standard:

Other dedicated application-specific safety standards exist and can complement the ISO 26262 series of standards or vice versa.

Integrating with prior released systems:

This document addresses alterations to existing systems and their components released for production prior to the publication of this document by tailoring the safety lifecycle depending on the alteration. This document addresses integration of existing systems not developed according to this document and systems developed according to this document by tailoring the safety lifecycle.

Provides a guide for developing a safety-related system were intended:

This document describes a framework for functional safety to assist the development of safety-related E/E systems. This framework is intended to be used to integrate functional safety activities into a company-specific development framework. Some requirements have a clear technical focus to implement functional safety into a product; others address the development process and can therefore be seen as process requirements in order to demonstrate the capability of an organization with respect to functional safety.

This document specifies the requirements for supporting processes, including the following:

- interfaces within distributed developments
- overall management of safety requirements
- configuration management
- change management
- verification
- documentation management
- confidence in the use of software tools
- qualification of software components
- evaluation of hardware elements
- proven in use argument
- interfacing an application that is out of scope of ISO 26262; and
- integration of safety-related systems not developed according to ISO 26262.

ISO 26262: Goal/explanation

Focus/goals:

Currently, with millions of lines of code per vehicle model, guidelines are needed to protect road users (drivers and pedestrians) from injuries caused by faults in vehicle electronics and software. As vehicles become more software than hardware based in production, safety between software and hardware needs to provide a level of safety based on A Safety Integrity Level (ASIL). ASIL has four levels: A, B, C, and D. ASIL A represents the lowest degree, like window controls, and ASIL D represents the highest degree, like cruise control, of an automotive hazard. ISO 26262 is recommended starting from ASIL B and obligatory for ASIL C and D. Through functional safety it aims to reduce risks to a level that society finds acceptable, preventing harm caused by malfunctioning electronics. These requirements are to assure safety throughout the lifetime of the vehicle. By providing an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases.

A safety lifecycle is defined as an engineering process that is designed to ensure that a safety system used can work continuously and effectively throughout the entirety of its lifespan.

An automotive functional safety lifecycle begins with hazard analysis and risk assessment. At this stage, the developer will analyze the faults, failures, and resulting hazardous situations that could pose harm to users of the end products. For each vehicle's state, driving situation, and environmental condition, they will evaluate hazards based on their severity, exposure, and controllability values. This helps prioritize hazards by assigning ASIL level to them based on those three values. ASIL defines the necessary actions and measures to be taken during development and after the start of production.

During this process, hardware and software components will be tested and integrated. This will be followed by the integration of these product components to form a complete system, which in turn will be integrated in the vehicle at the end of the process. The goal of this integration process is to ensure compliance with the specified safety requirements, and to verify that the overall system design covers all safety requirements.

Verification/validation process:

ISO 26262 recognizes that using widely accepted software tools simplifies or automates activities and tasks required for the development of electrical, electronic, and software elements that provide safety-related functions. Software tools referred to are for verification and validation processes. Validation differs from verification testing. Verification testing is the process of confirming that the way a product performs meets the predetermined product specifications. Validation testing is the process of assessing a new software product to ensure that its performance matches consumer needs. Product development teams might perform validation testing to learn about the integrity of the product itself, how well it will integrate with existing products, and/or its performance in different environments.

Qualification process:

Qualifying software components involves activities such as defining functional requirements, resource usage, and predicting software behavior in failure and overload situations. This process is dramatically simplified by using qualified software during development of an application. Qualified software components are generally well-established products that are re-used across projects and include libraries, operating systems, databases, and driver software. To qualify a software component, the standard requires testing under normal operating conditions along with inserting faults in the system to determine how it reacts to abnormal inputs. Software errors such as runtime and data errors are analyzed and addressed throughout the design process.

Proven in use clause:

Hardware and software components can comply with ISO 26262 requirements through the “proven in use” argument. This clause applies when a component has been used in other applications without incident. ISO 26262 also addresses older systems that have been proven in use. In many circumstances, it does not make sense to apply a standard to a system that has been previously deployed in millions of vehicles. For instance, many systems in currently manufactured cars were manufactured to a high level of safety before the publication of ISO 26262. Throughout use in the real world, these safety-critical components have shown that they can exhibit reliable behavior. Reliable systems that remain unchanged from previous vehicles are still certifiable with ISO 26262. The combination of certifiable components from similar applications and from older, widely-deployed applications greatly reduces the overall system complexity.

ISO 26262 Intended System Examples:

A window control could have ASIL A level due to its hazard severity resulting in a pinched finger; whereas a cruise control will have ASIL D level due to its potential hazard of an accident. An airbag could have ASIL D due to a malfunction causing premature deployment also resulting in an accident.

These examples are software-controlled hardware in production vehicles. The software must be able to monitor its hardware as well as control it. It must have a predetermined result for any errors detected/sensed. In these systems is where safety lifecycles are to be implemented, and its software qualifications verified/validated before product launch.

Data acquisition:

ATI software is data acquisition software. The goal of the vehicle data acquisition system is to create a publicly available data archive taken from the operation of a real car under various real conditions of the driver and the road. The data is collected from a vehicle's communication bus and from an image acquisition system. A data acquisition system is a system that includes measurement devices, sensors, a computer, and data acquisition software. A data acquisition system is used for acquiring, storing, visualizing, and processing data. This involves collecting the information required to understand electrical or physical phenomena.

In Conclusion:

Software/hardware products used in data acquisition and not used in vehicle production releases do not fall under IEC 61508 and/or ISO 26262 requirements. ATI’s software/hardware is not the intended focus for IEC 61508 and/or ISO 26262.

Note:
Information for ATI's statement is a summary extracted from both IEC 61508 and ISO 26262 (2018).