Safety first?

Security is just as important

By Markus Jastroch, Sysgo

In many applications in the railways, aircraft or automotive industry the interaction between safety and security is of particular importance, since there are many dependencies between them and they can therefore no longer be considered separately.

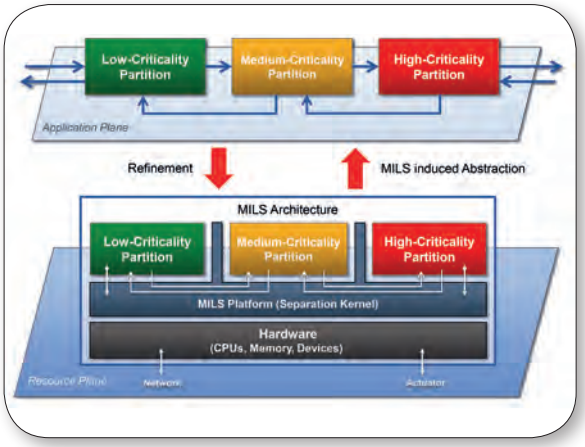

Figure 1. The MILS concept enables trusted and untrusted components to co-exist on a single platform.

Whether in railways, aircraft or the automotive industry, electronic control systems and their developers face complex challenges today. On the one hand, due to increasing networking, problems of functional safety and IT security are emerging. On the other hand, standard products are increasingly being used and individual control elements have to perform multiple tasks in order to save weight, costs and energy. Especially in such environments, the interaction between safety and security is of particular importance, since there are many dependencies between them and they can therefore no longer be considered separately.

Functional safety is about the unintentional failure of components or code, while (IT) security is about protection against intentional and mostly malicious attacks. In short, safety protects the environment from the system, while in security it is the other way round - it protects the system from the environment. Functional safety has long been one of the most important aspects of transport technology, and a large number of standards have been established to which technical systems must be certified, as follows.

IEC 61508 is an industry-independent basic standard for the functional safety of electrical, electronic and programmable systems with a safety reference. It distinguishes between four criticality levels, SIL-4 to SIL-1 (Safety Integrity Level).

DO-178B is the definitive standard for software development in aerospace. The standard knows five criticality levels DAL A to E (A=catastrophic to E=no effect).

EN 50128 is a European standard for software development in connection with railway applications with five criticality levels (SIL-4 to SIL-0). EN 50129 for signaling technology in rail traffic is related to this standard.

ISO 26262 defines the functional safety requirements for vehicles on the road. Based on the safety integrity levels of EN 61508, it defines four ASIL levels D-A, where D stands for the most critical systems.

Security deals with the prevention of errors that can lead to unauthorized access to or manipulation of data or systems. The main aim here is to avoid weak points by means of IT security measures or to make their exploitation by attacks impossible. There are also international security standards for security-critical systems, only a few of which are industry-specific.

ISO 15408, better known as CC or Common Criteria (for information technology security evaluation), is the most important standard for testing and evaluating the security properties of IT products worldwide. It introduces seven Evaluation Assurance Levels (EAL 1-7) for trustworthiness.

EUROCAE ED 202 provides developers and certification bodies with guidance for aeronautical systems that are influenced by human interaction and can affect the safety characteristics of an aircraft.

The SAE (formerly Society of Automotive Engineers) is working on a series of standards on various aspects of IT systems in automobiles and is introducing the term ACsIL (Automotive Cybersecurity Integrity Level) based on the Safety Integrity Levels in Draft J3061 published in 2016.

ISO is currently working on ISO 21434 (Road Vehicles - Cybersecurity Engineering).

Safety errors are typically random errors that are regarded as "friendly" errors in a safe environment. Added to this are random and systematic errors such as electromagnetic radiation, hardware errors, specification and design errors or software errors. All safety-relevant functions (e.g. real-time behavior) must be taken into account here. The exposure time, i.e. the period during which the system is exposed to the fault, may or may not

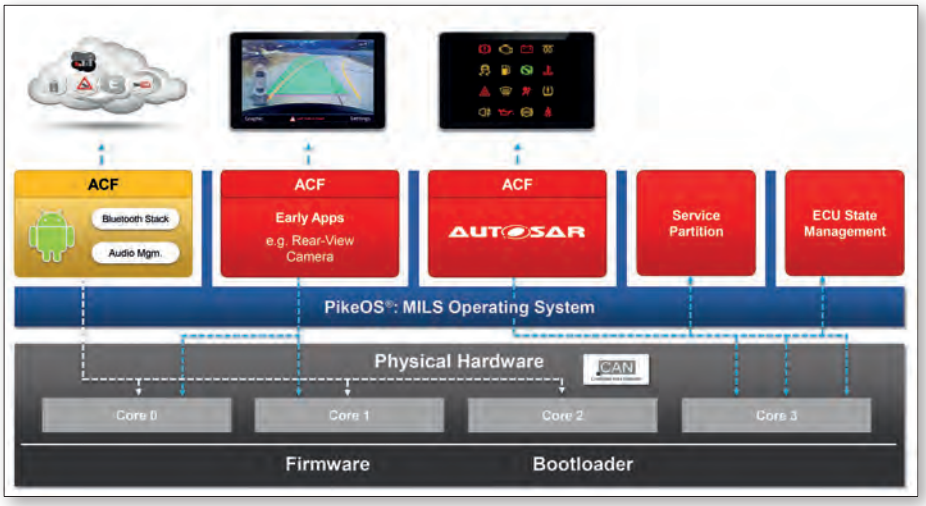

Figure 2. PikeOS can be used for implementations of the MILS concept - in this case in the automotive industry.

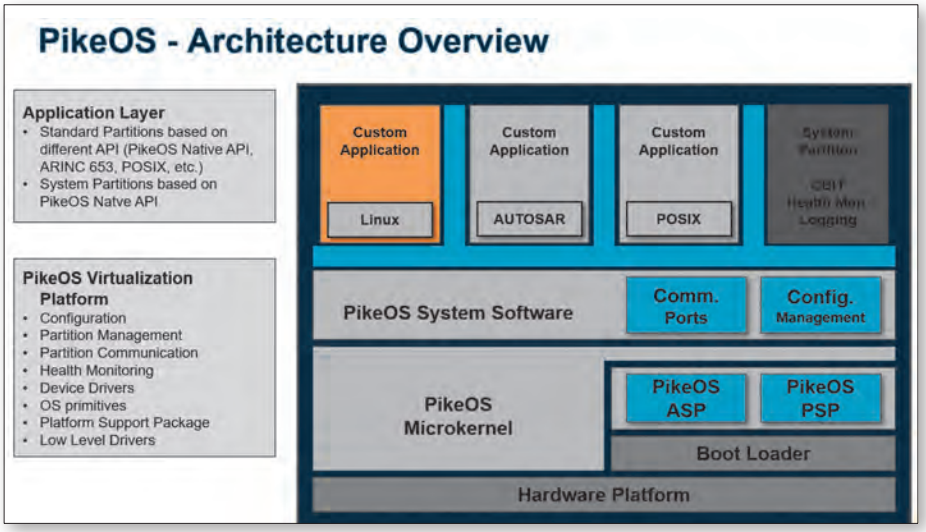

Figure 3. PikeOS is a virtualization platform based on a separation kernel.

affect the occurrence of a failure. Security, on the other hand, is typically about intentional errors caused by internal or external attacks. In addition to such attacks, however, systematic errors such as design errors, software errors, weak passwords or cryptographic keys as well as unexpected hidden channels must also be taken into account. The exposure time typically influences the success and consequences of an attack.

Although or precisely because the Common Criteria Standards are completely technology and industry agnostic, they provide a good basis for the development of critical embedded systems in conjunction with mostly industry-specific safety standards. In particular, it is possible to assign individual systems an EAL level (Evaluation Assurance Level) between 1 and 7 (from the least demanding to the most demanding in terms of design, testing and verification). However, one should be aware that CC-certified products do not guarantee the absence of vulnerabilities, but only that the test and verification objectives have been achieved and a state-of-the-art vulnerability analysis has been carried out.

While the application of good software practices, mainly with regard to verification and validation, has long been established for safety-relevant topics due to strict certification requirements, there is often still some catching up to do with security. In return, the security industry reacts very quickly to changes. Techniques must also be developed in the area of functional safety in order to shorten the time for changes to certified systems.

Today's modular systems offer improved connectivity, resource sharing between applications of different levels of criticality on the same computer, and promote the use of standard or COTS (Commercial Off-the-Shelf) products in security-related systems. These developments bring benefits such as reduced development and maintenance costs or savings in weight and energy consumption, but from the security point of view they also mean an increase in the attack surface for malicious programs. In addition, the use of COTS hardware and software gives potential malicious attackers more information about possible vulnerabilities, some of which is publicly accessible. This affects both communication between spatially separated applications and communication between applications in different partitions on the same ECU.

The main problem when using COTS and consolidating different applications on one hardware is the strict separation of the individual applications from each other, so that problems with one application cannot affect others. This requires strict partitioning of the available resources so that the applications can actually run completely independently of each other. Partitioning and separation are also the cornerstones of the Multiple Independent Layers of Security (MILS) concept, which describes a multi-layered security architecture for the coexistence of trusted and untrusted components based on verifiable separation mechanisms and controlled information flows (figure 1)

The MILS approach requires a (real-time) operating system that is able to strictly separate applications or processes and their resources - both spatially and temporally. Such a system is also called a separation kernel - an example of this is PikeOS from the German manufacturer Sysgo (figure 2). A separation kernel architecture makes it easier for the system integrator to create a clearly structured design in which safety applications coexist with less safe applications in the same system without making compromises between safety and security. For example, Linux guests which are responsible for external communication via complex network services can cooperate with applications at a higher security level. These applications with a higher level of security and the associated devices remain strictly separated from the outside world by partitioning. Since PikeOS supports not only spatial but also time partitioning, it also enables the implementation of complex time-controlled applications.

A robust partitioning approach is advantageous for both security and safety applications and is more or less explicitly required in virtually all of the above standards. Robust time partitioning also enables real-time and non-real-time applications to coexist on a single hardware, for example. In addition, this separation creates independent security domains for applications of different criticality and thus also facilitates certification considerably, since applications in different security domains can be certified independently of each other. ■