CAN YOU AFFORD NOT TO CERTIFY YOUR CONTROL SYSTEM?

ENGINEERS FROM CC SYSTEMS INTRODUCE THE CURRENT MOST IMPORTANT SAFETY DIRECTIVES AND STANDARDS FOR INDUSTRIAL VEHICLES AND MACHINES

Industrial vehicles typically contain heavy moving parts that could cause harm to people if they do not behave as intended or if they do not offer adequate protection. At the same time, electronic control systems are responsible for more and more of the core functionality in the vehicles, such as engine control, braking and steering, and the functions performed by the vehicles, such as buckets, cranes and drills.

Legislative and standardisation authorities around the world are currently increasing the pressure on vehicle manufacturers to comply with safety standards for their electronic systems, such as the updated EU machinery directive (EU Directive 2006/42/EC), which is planned to take legal effect at the end of 2009, the safety standard for earthmoving machinery (ISO 15998) from 2008, the safety standard for the safety-related parts of machinery (ISO 13849) from 2006, the safety standard for programmable electronic control systems in machinery (IEC 62061) from 2005, the general standard for safety-related electronics (IEC 61508) from 2005, and the upcoming safety standard for on-highway vehicles (ISO 26262).

The whole safety area for electronic control systems may at first seem an insurmountable number of additional requirements to comply with. Nevertheless, there is not really any other choice than to work according to these standards. Even when there are no strict legislative requirements, the market will most certainly gradually increase expectations on products to be certified according to the relevant safety standards. And there will be a competitive advantage in doing so.

What do the standards require?

In general, the approach to demonstrate adherence to safety standards of modern electronic control systems in all types of industrial vehicles consists of both quantitative and qualitative evidence. The standards mandate a lifecycle model where risk analysis is performed early in the project. The main potential hazards involving the control system are determined, as well as a target level for safety. These levels are termed the safety integrity level (SIL in ISO 15998, IEC 61508, IEC 62061, ISO 26262) or the performance level (PL in ISO 13849). All later activities in the lifecycle are heavily influenced by the SIL or PL.

The quantitative part of the safety evidence consists of hardware reliability figures, the failure rates (sometimes called λ or MTTF(d)) for devices, channels, safety functions, and related metrics such as safe failure fraction (SFF) and diagnostic coverage (DC). The overall design must be analysed and the resulting probability of failure must meet a certain level, depending on the SIL or PL stipulated by the standard. This can be a fairly time-consuming but straightforward process consisting of calculating the reliability figures of the design components, and choosing suitable circuits for which such (high MTBF) figures are available or can be calculated. As higher protection levels imply lower failure rates, usually redundant circuitry is used to build parallel channels that tolerate single faults within the system. Several safety standards even constrain the architecture to be used as a relation between the three parameters – safety level, SFF/DC, and hardware fault tolerance (Category), such as IEC 61508-2 and ISO 13849-1.

Qualitative evidence is also needed as part of the total evidence handed to certifying authorities. The safety standards cover many practices in the system's entire lifecycle that must be appropriately addressed, such as how requirements are handled and traced development process, how the system is designed and programmed, how the potential safety hazards are analysed and handled, what compilers and development tools are used, which test strategies to use, and how the system is planned to be maintained, including managerial issues, such as using staff with appropriate skills.

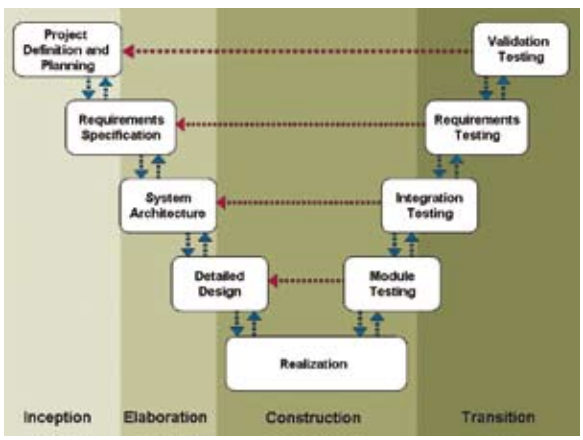

FIGURE 1: **A hybrid process model based on an iterative RUP-based process and the V-model mandated by safety standards**

To be presented as evidence, all this has to be documented. The strategy is to document every piece of evidence so that it can contribute to the final safety case (or safety file), to prove that the planned safety integrity level is actually reached by the means and measures applied during product realisation.

Safety cannot be assessed later on the basis of the developed product, particularly not the software in the system which has to be treated mainly qualitatively. Software behaviour is discrete, and a seemingly small difference in input may cause it to behave quite differently. Reliability and predictability, and therefore safety, can never be shown statistically for software. Software testing can only reveal errors; it cannot prove their absence.

Conclusions

This introduction to the current most central directives and standards in the area of safety for industrial vehicles and machines will hopefully be useful for those new to the area of safety, and also have a calming effect regarding the work that has to be done.

Ultimately, safety is about building better and more reliable systems. If you think safety is too expensive for your organisation, try having an accident! **iVT**

ON THE WEB

Click here / read the full version online at: **www.iVTinternational.com**