QNX
A Subsidiary of BlackBerry

CASE STUDY

MEN and QNX Software Systems

A highly-efficient path to functional safety certification for railway transportation

Terry stares at his project proposal on the table for the fifth time that morning. The title reads: Project Proposal – Automatic Train Protection System (Certified to EN 50128 SIL 4). Although Terry has managed the development of multiple technology systems in the past, this project is different and has cost him several nights of sleep.

Customer Snapshot

Company
MEN Mikro Elektronik GmbH
www.men.de
@MEN_Germany
info@men.de

Headquarters
Nuremberg, Germany

Founded
1982

Number of Employees
Approximately 290 worldwide

About
Offers highly reliable embedded COTS boards and devices widely used in extreme environmental conditions found in industrial and safety-critical application

Certified to ISO 9001, ISO 14001 (environment), EN 9100 (aerospace) and IRIS (railway)

Sales and support network

- MEN GmbH, Germany
- MEN S.A.S., France
- MEN Micro Inc., USA
- Worldwide distribution

Terry is a seasoned project manager from the industrial automation sector who recently joined a rail transportation manufacturer. With his engineering background, Terry has no problem understanding the technical aspects of the new project he is taking on, related to automatic train protection. Drawing up a project outline, complete with development schedule and budgetary figures, would usually take less than two weeks if he were not stuck. This being Terry's first safety certified project he is grappling with how to get EN 50128 approval at the system level for the hardware and software. Numerous questions swirl around in Terry's head, each threatening to undermine the usual knowledge that Terry has for estimating schedule and budget.

"What hardware platform should we choose to make the EN 50128 certification easier?"

"Which COTS components should we use?"

"What design implications does EN 50128 have on the overall system?"

"How much does certification cost?"

"How do we mitigate the risk of a failed certification attempt?"

"Are there any existing expertise in our development team on the application of the EN 50128 standards?"

"How does the EN 50128 requirement impact the overall schedule? Would it double the project length?"

A Harvard Business Review article surveying a sample of large IT projects showed that on average 45% of the projects run over budget, 7% over time and 56% deliver less value than predicted. Terry never thought these statistics would apply to any project he managed, based on his experience and industry knowledge. Now, faced with a new requirement for functional safety certification, Terry has a fresh appreciation for these numbers.

The Problem

Terry's problem is commonly found in many industries, including railway transportation, power and energy, factory automation, to name a few. Basically any system whose malfunction could lead to damages to human or properties is a candidate for functional safety regulation. There is an increasing adoption of functional safety standards in different markets, resulting in a number of market specific standards. EN 50128 is one such example. Based on IEC 61508, the standard governs the functional safety for heavy and light rail systems. The EN 50128 standard, which was published in 2011, and used in draft before then still confuses many system manufacturers who are unprepared for the implication of certification requirements, basically how such requirements impact project budget and time. A common mistake for less-experienced companies is gross under-estimation of this impact which can lead to market timing errors and lost revenue.

The knowledge level for functional safety and certification is one of the most important deciding factors for project success. Generally speaking, a project with functional safety certification requirements can easily double or triple the time it takes to complete a project without. Efforts invested in certification activities are often greater than efforts in straight development. This magnifying effect of the certification requirements is abated when knowledge level is high and amplified when knowledge level is low. The table below shows a fictitious scenario to illustrate this effect, assuming a development team with fairly good knowledge in safety and certification.

Newcomers to functional safety standards may find this increase in effort level to be inhibitive. However, a closer look at the standards' demand help explain this. Take IEC 61508 for example. The safety integrity levels of IEC 61508 range from SIL 1, the lowest level to the highest at SIL4. To provide a sense of how demanding these certifications are, a system certified at SIL 3 must have a probability of dangerous failure below 1 in 10 million per hour of operation. Achieving such a low risk of failure is non-trivial, to say the least. In fact, it's well-nigh impossible to satisfy these functional safety requirements unless they are baked into the very design of the product. This type of design strategy for safety products is reflected by the increase in both developer head count and activity duration in the table above. Demonstrating the compliance to these requirements, to an independent auditing firm, adds a whole realm of new challenges of its own, which could easily stretch the project duration by more than 100%.

So how do today's system vendors meet the challenge of increasing regulatory pressures for safety standard compliance in the face of increasingly compressed time-to-market windows?

The Solution

The MEN Modular Train Control System (MTCS) is a perfect demonstration of the three aspects of a highly-effective solution to this problem. First, embed functional safety concepts throughout the entire design lifecycle. Second, leverage pre-certified components wherever possible. Last but not least, use modularity to control project scope. MEN was able to deliver this sophisticated product with proven pedigree in functional safety in a timely fashion. In turn, the MTCS product is itself a pre-certified component, a critical ingredient of an effective solution for all railway system builders.

MTCS is a platform designed for safety-critical train applications like train control, automatic train operation (ATO), automatic train protection (ATP), and positive train control (PTC)/enhanced train control (ETC). These applications range in certification requirements from ATO typically at a EN 50128 SIL2 level to signal interlocking requiring a EN 50128 SIL4 certification. Available in an EN 50128 SIL 4 pre-certified configuration, the MTCS provides safe control of single functions as well as for complete train control. By changing its configurable setup, the MTCS can control anything in the train that requires functional safety – under SIL 4, SIL 3 or SIL 2 requirements. MTCS is developed according to EN 50128 and EN 50129 standards.

	Project without Certification Requirements	Project with Certification Requirements
Developer Head Count	12 people	18 people
Key Activities Duration (lapse in time)		
System Design	5 weeks	8 weeks
Detailed Design	3 weeks	5 weeks
Coding	4 weeks	5 weeks
Testing	6 weeks	12 weeks
Certification	–	20 weeks
Total Budget	$1.2 M	$3 M
Project Duration	8 months	24 months

Table 1: Project Comparison – Certified vs. Non-Certified Product

Using pre-certified components lower overall risk to system manufacturers through proven and reliable technologies. One of the most vital components in complex platforms consisting of hardware and software is the real-time operating system. A pre-certified operating system (OS) offers a high level of reliability and risk reduction for safety-critical systems that has been independently validated. It would be difficult to imagine a certified industrial control application without a pre-certified OS. This is an additional dimension to the build-or-buy decision for system manufacturers. Some companies have legacy home-grown components including operating systems. In most cases, the cost of certifying these home-grown components will outweigh the price tag of a pre-certified solution, simply due to the economy of scale factor. Hardware is a different story. Pre-certified hardware is difficult to find and hardware certification is a frequently-asked question from system manufacturers. By including their customer-designed hardware in the scope of certification, MEN has effectively solved this problem for their customers. The QNX Neutrino RTOS (realtime operating system) is certified to IEC 61508 Safety Integrity Level 3 (SIL 3), and offers a very high level of reliability and risk reduction for safety-critical systems. It plays a major role in building secure, survivable embedded systems. By adopting the QNX pre-certified RTOS, MEN effectively shortened the project by approximately two years, reduced project cost by about $2 million and eliminated any certification risk on the OS level.

To control project scope, which translates to project cost, modularity is the key word. At the heart of the MTCS lies the F75P – the central computing part of onboard applications like Train Management Control Systems or Train Protection Systems.

The F75P is a COTS safe computer with onboard functional safety that unites three CPUs on one 3U CompactPCI® PlusIO card. Two independent control processors (CP) with independent DDR2 RAM and Flash and a supervision structure provide safety (the board becomes a fail-safe subsystem, certifiable up to SIL4). An I/O processor completes the board with I/O connectivity. With its clear separation of safe and non-safe subsystems the F75P can replace multiprocessing systems with CPU redundancy and I/O by a small-footprint, low-power solution that is flexible for different types of application scenarios. The communication protocol of the third CPU was developed in accordance with EN 50159, which targets safety relevant communication in transmission systems. This ensures safe communication in the area known as the black channel, located between the control unit and I/O, for comprehensive, safe communication throughout the system. The diagram below is a good illustration of the modular characteristic of the MEN design.

The modularity concept is also reflected in MEN's choice of realtime operating system. The QNX Neutrino RTOS is a based on the microkernel architecture that enforces strong boundaries between software processes to prevent any process from affecting the performance and behavior of other processes. Processes can damage one another intentionally (via malware) or unintentionally (via bugs); the QNX Neutrino RTOS provides mechanisms to prevent such damage and to keep the system in a healthy state. Furthermore, the adaptive partitioning technology found in the QNX Neutrino RTOS provides this level of separation for CPU bandwidth. A modular design at the system level is only possible if it is built on a platform that supports this.

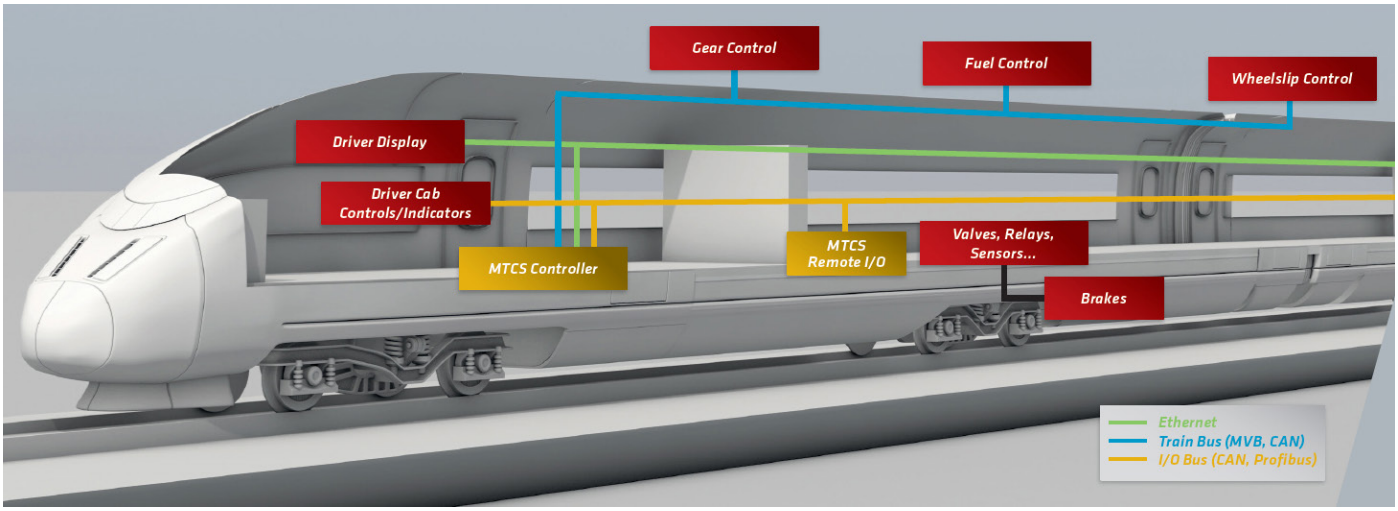

Figure 1: Modular characteristic of the MEN design

Conclusion

The MEN Modular Train Control System offers a pre-integrated, ready to install platform that combines the ideal operating system from QNX Software Systems for reliability and easier programming of safety critical applications with the F75P solution, representing an extremely compelling offer to address regulatory pressures and cost effectiveness challenges.

In addition to pre-certification credentials, MTCS offers high level of flexibility for system integrators, resulting in significant cost and time savings during computerization of the train. The combined solution allows users to quickly create new solutions which take advantage of the latest industrial safety and processing speed and real-time automation technology while allowing them to reuse or adapt existing automation algorithms.

So, for Terry, many of his concerns can be addressed with the selection of a reliable, pre-certified component such as the MTCS. This approach largely removes the unknowns in project planning, both in time and budget. Adoption of such a pre-certified COTS system also represents the most effective solution for many companies, freeing up internal resources to focus on true competitive differentiators. Last but not least, choosing a supplier with good knowledge in functional safety and certification sometimes provides the shortest path to access that knowledge in the most relevant manner.

About QNX Software Systems

QNX Software Systems Limited, a subsidiary of BlackBerry, is a leading vendor of operating systems, development tools, and professional services for connected embedded systems. Global leaders such as Audi, Cisco, General Electric, Lockheed Martin, and Siemens depend on QNX technology for vehicle infotainment units, network routers, medical devices, industrial automation systems, security and defense systems, and other mission- or life-critical applications. Founded in 1980, QNX Software Systems Limited is headquartered in Ottawa, Canada; its products are distributed in more than 100 countries worldwide. **Visit www.qnx.com**