MATS KJELLBERG

Display it safe

IN RESPONSE TO THE NEW STANDARDS FOR MACHINE SAFETY, A HIGH-PERFORMANCE DISPLAY COMPUTER THAT MEETS SIL2 WILL BE PRESENTED AT INTERMAT 2009

FIGURE 1: **Safe display computers are needed in industrial vehicles**

A new, high-performance display computer that meets safety integrity level 2 (SIL2) requirements will be presented at Intermat 2009 by CC Systems, the Nordic-based control system specialist.

Onboard computers with graphical displays are becoming common in industrial vehicles. The displays are used as the main interface between the driver and the vehicle control system, while providing possibilities for information processing, such as data collection for system diagnostics and prognostics, and communication with external systems that are today becoming more closely integrated with the vehicle control system. OEMs are also being challenged by legislative requirements such as EU Directive 2006/42/EC, requiring the onboard electronics to conform to safety standards such as IEC61508 (*Figure 1*).

CC Systems is complementing its range of advanced display computers with the CC Pilot XLS, a high-performance onboard computer for safety-critical systems. This comes with a 10.4in or 6.5in touch-screen display and a slim yet robust aluminium enclosure that offers IP67 sealing. The 1.6GHz Intel Atom CPU runs Windows or Linux – a very powerful platform for running non-safety-related system parts – and three additional processing units are used for safety-related functionality. This integrated concept saves space and is more affordable.

How to address safety

A safety-critical system involving a graphical human machine interface (HMI) requires a careful analysis and architectural design to clearly separate safety-related functions from non-safety functions. The next step is to select appropriate system components, to which safety-related functions can be apportioned and separated from other functions. Safety-related subsystems and components must be robust in design and incorporate many diagnostic and redundancy measures. Finally, an overall demonstration that the desired safety integrity level is met must be produced. The problem, however, is that such a solution requires many parts and results in a less integrated system. This drives cost and hinders smooth integration and interaction between the HMI and the control system – two aspects that are very important to manage in modern vehicles.

The CC Pilot XLS offers an integrated safety solution that responds to these needs. The internal architecture is based on a main CPU, a CPU for safety-related functions, an FPGA for highly parallel functions and a system supervisor for internal monitoring and supervision. This architecture makes it easy to implement both safety functionality and advanced, non-safety-related functionality (*Figure 2*).

It is realistic to expect that most functionality is non-safety critical in an HMI system. That functionality should therefore be executed on a platform offering high computing performance and the best development environments. Simplifying the implementation of high-level, customer value functionality, the main CPU is therefore Intel Atom, running Windows or Linux.

The Atom CPU is very suitable for vehicle systems as it combines low power consumption with high performance. The low power means that less heat is generated and thereby enables a wide operating temperature range for the device, which is an important factor in most vehicle applications.

As the Atom CPU hosts the graphical user interface (GUI) application (*Figure 3*), it needs to address some safety issues. Certain graphical objects, such as a speedometer or state indicators for vehicle functions, might need to be classified as safety critical. Pre-defined checksums for these objects are calculated and used by a special algorithm for checksum comparison in the safety-related subsystem for validating the information displayed on the graphical display.

The graphics controller and graphical memory in the CC Pilot XLS are implemented in an FPGA (field-programmable gate array). The FPGA communicates with the Atom CPU via the digital video interface LVDS. Being the link to the graphical display, the FPGA has a key role in the safety architecture.

Another functionality of the FPGA is the handling of analogue video streams from rearview or other surveillance cameras on the vehicle. Video input is processed digitally and superimposed on the digital picture. This enables integration of camera images in the GUI. Because the analogue video stream may include safety-critical information, the high speed of the FPGA circuitry makes it suitable for this task, rendering video images with virtually no delay.

The parts of the system that are classified as safety critical are allocated to a separate safety CPU in the CC Pilot XLS. This CPU is in itself safety classified. The software developer can choose to implement safety functionality either without operating system support, or with a safety-classified operating system such as VXWorks or Integrity. This gives vehicle manufacturers and system designers flexibility and freedom of choice as to the implementation of safety functions.

An example of a safety feature in this CPU is the comparison of pre-defined and actual checksums for safety-critical graphical objects. As long as the checksums match, the safety-critical graphical object is correct and the information can safely be shown on the graphical display.

Another example of a safety feature is protection against frozen image on the TFT display. For a safety-critical function it is essential that the image on the display is not frozen. Should this occur, it is detected by the safety CPU and the display is taken to the safe state.

A system supervisor CPU handles internal monitoring and supervision in the CC Pilot XLS, thereby ensuring the integrity of all parts of the display computer. The power supply within the unit is managed by this CPU. In a safety-critical system it is essential that power is managed in a way that ensures safe states at all times. Monitoring of internal temperatures, supervision of internal oscillators and control of the display backlight is also carried out in this CPU. In addition, the system supervisor performs sequence checking – a very important aspect in safety systems.

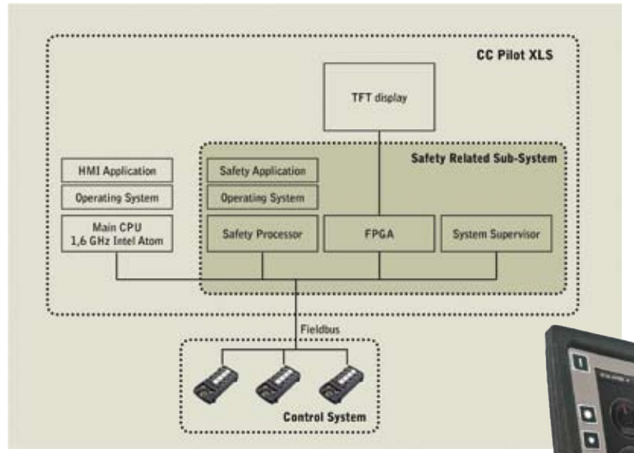

FIGURE 2 (LEFT): **CC Pilot XLS architecture**

FIGURE 3 (BELOW): **Graphical user interface running on CC Pilot XLS**

Safety for all

The new standard for machine safety, ISO 13849, will come into force in December 2009. Standards specific to certain segments such as earthmoving (ISO 15998) and agriculture (ISO/DIS 25119), are also evolving and will be established during the next few years. For safety in electronics and software the new standards refer to or inherit main parts of the IEC 61508 that specifies safety in different safety integrity levels, SIL1-SIL4.

Many industrial vehicle manufacturers are now preoccupied with ensuring that their machines, including electronics and software, will meet the new regulatory framework. Hazard analyses have to be made, as well as assessments of which safety functions are required, and the level of safety must be specified. Then comes implementation of safety functions and finally verification that the machine meets the specification. This can be quite a challenging task and will require a fair amount of engineering time and safety competence to get through the process smoothly.

To what extent a machine and system needs safety classification is very specific to each machine and application. The CC Pilot XLS is already being applied in safety-critical systems. One example is an application where SIL2 rating is required for the display of certain graphical objects, such as speed information. Another example is SIL rating of the display of video streams in real time, where a delayed or frozen picture could potentially lead to a to hazardous situation.

The CC Pilot XLS is a very powerful on-board display computer that enables the implementation of advanced non-safety systems for controls, surveillance and diagnostics. Through its internal architecture and design, it also offers OEMs great flexibility when addressing safety requirements that involve a graphical user interface. Better to be safe than sorry! **iVT**

Mats Kjellberg is marketing & sales manager at CC Systems, which he joined in 2000 after working in ABB's power-generation business

CONTACT
www.cc-systems.com
info@cc-systems.com