Safety Buses

By Dick Caro, CEO, CMC Associates, Acton, MA

In 1998, Pilz introduced SafetyBus-p at Hanover Fair. Since then, there have been several announcements and product releases of safety buses. All of this has raised many questions like: What is a safety bus? Do I need one? How "safe" does a safety bus need to be? How is "safety bus" related to "safety systems?"

The primary purpose of a safety bus is to allow ESD (Emergency ShutDown) devices to share common bus wiring with conventional I/O devices. For discrete parts manufacturing, ESD devices are typically that big old red button that says "Emergency Stop", but it may also be a floor mat safety switch, a light curtain, or an infrared personnel detector – all of which are designed to prevent personal injury when people or parts of people are detected in the path of moving machines. These safety devices are designed to detect hazardous conditions, which are part of the normal operation of mechanical processes, and are not to be confused with the more drastic "lock-out" mechanisms such as a padlock or car-seal on the electrical breaker used to allow technicians to repair machinery. ESD devices are provided to both cause emergency shut down, and to allow the control system to log and track these actions. Safety lockouts are only to protect maintenance personnel.

Common practice has been to hard-wire ESD devices to form part of the electrical interlocks necessary to operate the hazardous machinery. With increasing frequency, interlock logic is being embedded into machine controllers, or is part of the PLC set up to operate and schedule the machine. This means that the hard-wire terminates into a controller with programmable interlock logic. At the same time, use of a digital fieldbus has become popular for

interconnecting I/O with controllers. Why not simply make the ESD device another I/O point on the fieldbus?

IEC 61508 is the standard for programmable safety systems published by the International Electrotechnical Committee in 1999. It requires that I/O associated with safety be separately wired, UNLESS the network can be proven to support the Safety Integrity Level (SIL) desired for the safety function. Therefore, validating the network for the use of safety I/O devices is what the topic "safety bus" is all about. To say it in other words, IEC 61508 requires that the safety signal be delivered to activate the shutdown, OR that the system be shut down if a failure of the I/O device or the fieldbus is detected. Detection of device and fieldbus failure must be added to any bus technology for which the term "safety bus" is claimed.

Make My Bus Safe

To make a CAN bus safe, Pilz decided to create a safety protocol that will work on any CAN based bus. The safety controller polls each safety device on a timed basis and assures that there is a response within a time limit. If there is no response, the shutdown action is taken. If the safety device indicates that shutdown should be taken, the machine is also shut down.

Profibus masters poll all slave units on a regular schedule anyway. ProfiSafe is a small additional protocol element added to Profibus to make it a safety bus, and has proven to be very popular and effective in machine control applications.

DeviceNet has also added a safe profile, but has taken an additional step to also make the bus less likely to fail. While DeviceNet protocol, provides bit-wise bus arbitration to avoid collisions, the collision avoidance actually used for DeviceNet is master/slave polling. With every station polled on every cycle, failure detection is rapid and simple. When a safety device is connected with DeviceNet, it will not operate unless the scanner (master station) sends it a "clear to operate" signal. With the release of the DeviceNet safety specification, ODVA (Open DeviceNet Vendors Association also has released a specification for a redundant DeviceNet bus that provides high availability when required to avoid shutdowns due only to single bus failure.

Although Foundation Fieldbus is not used for machine control operations, it too must be considered as an adequate safety bus. The only missing element is not a bus hardware or even

software issue, but only an application or bus management issue. Currently, there is no "safety bus" management function for Foundation Fieldbus. The Application Layer Management Entity does provide access to the bus "alive list" and exception reports when a member of the alive list has a fault. Currently, this is not defined to be a safety function, but it certainly is an equivalent of the bus monitoring in Profibus and DeviceNet. Obviously, a redundant Fieldbus makes process shutdown unnecessary if the fault is a failure of only a single bus.

We are still groping and feeling our way to improved machine and process safety as standards are issued and mature. Many advocates do not trust buses at all, and believe that all safety sensors and safety interlocks should be hard wired. Others believe that the diagnostics available with buses and smart devices make buses safer than hard wiring of dumb devices. Eventually, CMC believes that the safety devices must become intelligent to help make sure that machines and processes are shut down if the failure indication is valid, and not shut down if the failure indication is false. Hardwired systems depend upon external logic which itself is doomed to failure, while smart devices tend to be simple, distributed, and less likely to fail.

CMC Associates focuses on product and market strategies to help suppliers succeed in their markets by fully understanding future technology trends, end user needs, and their preferences. We follow the news events and prepare news analyses such as this to raise awareness of market and technology trends for our clients. No inside knowledge was used to prepare this document, and it has not been funded by anyone. If you think that this type of analysis can be of value to your company, supplier or end user, please contact the author, Dick Caro at Dick@CMC.us.