

PROGRAMMABLE SAFETY APPLICATIONS ARE ENTERING automation fields that had been reserved for conventional electromechanical technology. Are all industries ready to accept safety systems that rely on bits and bytes? The answer is: Not yet. But that time should not be far off.

For many products and systems, a failure to function can expose people and the surrounding environment to hazards or contribute to

under all the stated conditions, within a stated period of time. IEC 61508 also is the basis for the certification of programmable electronic safety systems.

IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, is a seven-part international standard. It is generic, and applies to safety-related control systems, PLCs, devices, and

SAFETY APPLICATIONS

IN CONJUNCTION

WITH NETWORKS WILL



BE THE FUTURE IN THE

AUTOMATION WORLD

Are We Ready for Digital Safety?

production losses. A standard safety assessment evaluates how much "safety" has to be incorporated into a device or system to achieve the appropriate safety level. Products such as safety PLCs, fire-detection systems, light curtains, or safety bus systems are considered safety-relevant devices.

Although standard fieldbus applications grew dramatically in the past few years, safety functions had to be realized in a second layer. A second layer usually contains safety relays or is implemented within a special safety network. Additional wiring costs for the diagnosis of safety functions often is necessary, and flexibility is limited due to heterogeneous engineering.

The status of safety-oriented parts or layers can be made available to the control system by coupling with the operative fieldbus. Safety applications in conjunction with networks, regardless of their structure, will be the future in the automation world. Openness and interoperability are key factors to expedite the safety automation process. It won't be too far in the future that Bluetooth or WiFi-enabled control pendants will be a part of an overall safety network.

The current experience gathered in safety networking in the operative area of plant and machine controlling paves the road in the right direction. Benefits include reduced wiring, comprehensive diagnostic possibilities, increased flexibility, and a higher level of safety.

When engineering a safety system, its safety integrity must be built in. In other words, the safety integrity of the intended system architecture has to be predicted and evaluated. IEC 61508 is the major functional safety standard that introduces the concept of the safety integrity level (SIL). The SIL represents the probability that a safety system will not satisfactorily perform the required safety functions

components (including sensors, actuators, and operator interface). The four main areas covered by the standard are:

- Measures and techniques for avoiding or controlling faults (hardware and operating system software) during design and development.
- Hardware fault tolerance of systems/subsystems (structure) in combination with "safe failure fraction" and diagnostic coverage.
- Probability of "failure to danger" of the subsystem by reliability modeling techniques.
- Measures and techniques for avoiding or controlling faults during the design and development of application software.

The concept of SIL introduced in IEC 61508 is a concept of classes of safety requirements for components, modules, subsystems, or functions. The SIL indicates target failure measures for the safety function of an E/E/PES system. This method obtains Markov models for probabilistic calculations that make it possible to determine the accurate SIL level.

IEC 61508 is a powerful blueprint for the future. TÜV Rheinland, which has offices in the U.S. and other countries, currently is the only organization authorized to provide an assessment of safety networks around the globe.

In North America, the U.S. Occupational Safety and Health Administration has endorsed ANSI/ISA-S84.01-1996, Application of Safety Instrumented Systems for the Process Industries, as a "national consensus standard" for the application of safety instrumented systems (SIS) for the process industries. S84.01 covers electrical, electronic, and programmable electronic technology, and follows the safety lifecycle, similar to IEC 61508.

Acceptance is growing all over the world. It's only a matter of time before this concept of programmable safety is embraced universally. ●

ANDREW EBERHARD, DIPL. ING.

...is division manager of industrial services at TÜV Rheinland of North America Inc., Pleasanton, Calif. Information is available by e-mailing info@us.tuv.com or by calling 203/426-0888.