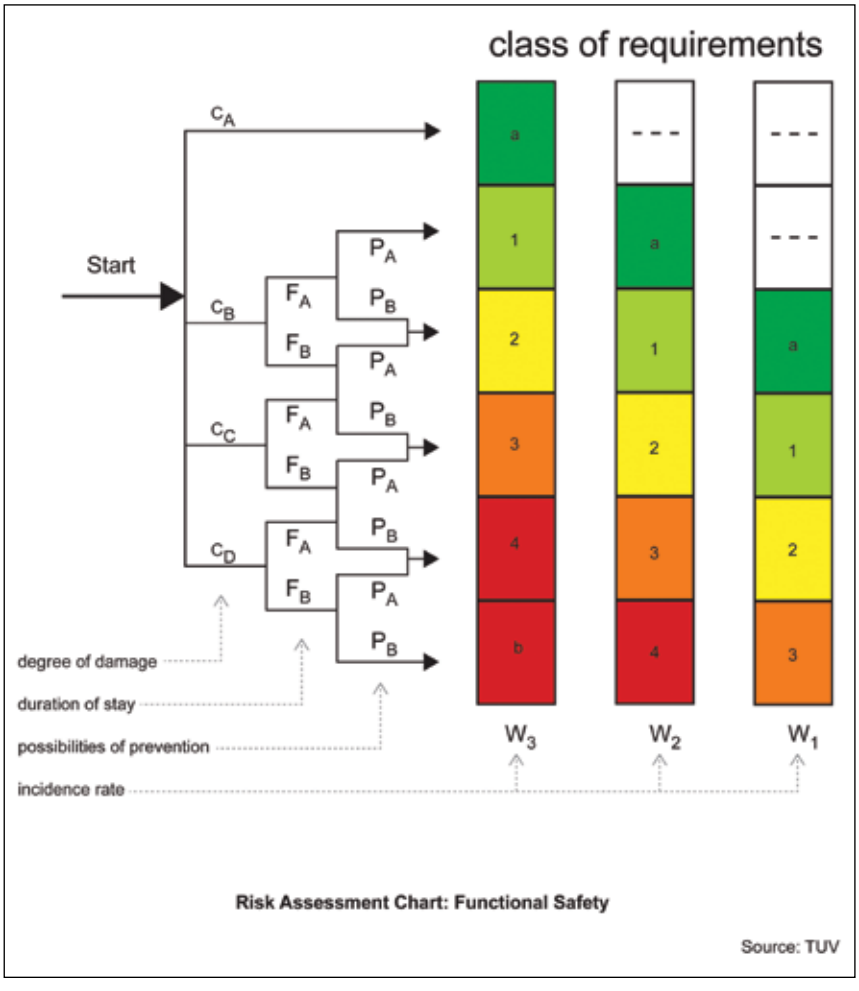
Safety Networks in Auto Manufacturing

As recently as 10 years ago very few safety networks existed in most manufacturing facilities. The systems that did exist often contained proprietary hardware and software, and to understand them required significant knowledge in complicated safety standards. In today's manufacturing environment, we have all types of safety network capabilities that are standardized, certified, and available off-the-shelf. Today we have DeviceNet Safety (CIP Safety), EtherNet/IP Safety, ProfiSafe, AS-Interface Safety at Work (ASi-SaW), EtherCat FSoE, and Powerlink OpenSafety, just to name a few. But the plethora of networks that are available leads to the difficult question of which network to choose. With the many varied features available, making a decision requires significant understanding of machine safety and safety networks.

Machine safety over a network is achieved with redundant or dual-channel systems that monitor for faults and prevent a restart when a fault occurs.



Risk Assessment Chart: Functional Safety

Source: TUV

Curt Christensen
Automotive Program Manager - CNC
FANUC America Corp.
Hoffman Estates, IL

To help understand today's safety market, it will help to take a quick look at where and how safety networks came into play. Safety, in the not too distant past, was normally a totally separate system from machine control. A stand-alone control system performed safety functions, with its own sensors, controllers, and network communications. If a fault occurred, it was the safety system's function to stop the machine and sound an alarm. Although the control system was perfectly capable of performing the same safety functions, the idea was to provide a redundant system in case the main control system failed. However, having a second control system became expensive and difficult to manage. In most cases, machine controls came from one vendor, while the safety system came from another. This added further complexity to engineering, integration, and aftermarket support. Over time, consolidation of safety functions into the machine control systems began to evolve.

Today, safety functions are incorporated into the machine control systems, using safety networks to bring sensor information to the control system. Safety PLCs are fully capable of performing both control and safety functions, while meeting the safety requirements of ANSI and IEC. Machine safety over a network is achieved with redundant or dual-channel systems that monitor for faults and prevent a restart when a fault occurs. And all of this occurs using a single wired channel for communications, an architecture that is recognized and acknowledged in IEC 61508 and other standards. That standard states that redundancy within communications protocols is sufficient to meet the same levels of safety as dual-channel, hardwired systems.

IEC-61508

IEC-61508 is the current standard used in many companies for functional safety of electrical, electronic, and programmable electronic systems (PES). This standard covers PLC and CNC components installed in typical manufacturing systems found in automotive, and it defines Safety Integrity Levels (SIL) as a means of targeting measures adequate to achieve what is known as "Tolerable Risk." Additionally, the standard provides example measures for abatement of hazards and covers the entire safety lifecycle including risk analysis, safety requirements and allocations, design, procurement, system build, system verification, installation and commission, validation, operations, and maintenance modifications.

The key to this standard is that it defines both quantitative and qualitative measures for the development and implementation of a network safety system. Quantitative measures for safety are designed to predict the frequency of hardware failures and compare them with some tolerable risk target. If the target is not satisfied, the design is revised until the target is met. Qualitative measures, on the other hand, are designed to minimize the occurrence of systematic failures (*eg.* software) by applying a variety of defenses and design disciplines appropriate to the severity of the tolerable risk target. All of this has been developed into a Safety Integrity Level (SIL) measurement that is designed to provide clarity to the "risk" of a system. However, the SIL level determination is actually application specific and really has nothing to do with the safety system—it is the risk assessment which is used to identify the SIL level of the specific application.

Basic Safety Integrity Levels

There are four basic levels of SIL in the machine safety specification, and these levels are tied directly to the probability of a dangerous failure. The levels are as follows:

Safety Integrity Level 1 (SIL1) is the lowest safety level and therefore is the easiest to achieve, providing that ISO 9001 practices were applied throughout the design process. Functional Safety Capabilities must also be demonstrated within the design of the system. Functional Safety Capabilities are covered in IEC 61805, and there are two basic assessments that are required: an assessment of management procedures (similar to an ISO 9001 audit) and an assessment of the implementation of the procedures. Adequate competency for Functional Safety Capability includes the following factors:

- Technology knowledge
- Safety engineering knowledge
- Legal/regulatory knowledge
- A link between magnitude of consequences and rigor of competence
- A link between SIL and rigor of competence
- A link between design novelty and rigor of competence
- Relevance of previous experience
- Relevance of qualifications
- Need for training to be documented

Safety Integrity Level 2 (SIL 2) is incrementally higher than SIL 1, and still requires that ISO 9001 practices be applied. SIL 2 requires more review and testing, and therefore adds additional cost, however, it is not difficult to achieve.

Safety Integrity Level 3 (SIL 3) involves a significantly higher degree of effort and competence than is the case from SIL 1 to SIL 2. Development costs and time will be significantly increased, and the choice of qualified vendors will be

SAFETY LEVEL	PROBABILITY OF DANGEROUS FAILURE (per hour)
SIL Level 4	1 in 1 billion
SIL Level 3	1 in 100 million (highest level for most industrial applications)
SIL Level 2	1 in 10 million
SIL Level 1	1 in 1 million

much more limited. SIL 3 is the current level with which most automotive companies require their safety networks comply.

Safety Integrity Level 4 (SIL 4) involves state-of-the-art practices including "formal methods" in design. Development costs and time will be extremely high, and finding qualified vendors and suppliers would be extremely difficult. This level of SIL is normally avoided in automotive manufacturing as the costs currently far outweigh the benefits.

Risk Assessment

In the final analysis, safety integrated systems are designed to minimize the risk of personal injury due to a system failure. While no system can be perfectly safe, risk assessment is a tool that is used to determine what level of risk can be considered acceptable. One model of risk assessment is shown on the first page of this article.

Once again, SIL is directly related to the risk. The severity, probability, and frequency of a safety-related failure must be weighed to determine the exact level of risk that a specific system has inherent in normal operations, as well as maintenance, support, and other functions within the production system. This analysis is complex and requires significant time and effort to achieve; however, once determined it can be the basis for future systems.

Which Network for Safety

With all of the intricacies associated with safety and communications, it is easy to see why many industries have avoided the network safety discussion altogether. In today's modern manufacturing world, network safety is a foregone conclusion—it is here to stay. So the question then becomes which network structure is going to be the best, both for today and into the future.

Ethernet/IP is arguably the fastest-growing deterministic field bus network available today. The backbone of Ethernet/IP is the Common Industrial Protocol (CIP) and along with that comes the Common Industrial Protocol (CIP) Safety. The Common Industrial Protocol (CIP) is designed to allow different networks to be used with a common protocol. Since it is designed to be media and data-link independent, it allows for expansion to future networks. CIP Safety is the TÜV-approved extension to standard CIP. CIP Safety extends the standard application layer of the Ethernet stack by simply adding CIP Safety. Because the safety application layer extensions do not rely on the integrity of the underlying standard CIP and data link layers, single-channel hardware can be used for the application layer functionality. Additionally, Ethernet/IP Safe can coexist on the same wire as standard Ethernet/IP and common Ethernet (TCP/IP).

The routing of Ethernet/IP safety messages over this network is possible because the end device is responsible for ensuring the integrity of the data. If an error occurs in the transmission of the data or in the intermediate router, the end device will detect the failure and take the appropriate action. Additionally, all CIP Safety data is produced with a CIP Safety Validator, which is responsible for detecting nine different types of communication errors. The CIP Safety Validator uses five different measures, including time stamp, production ID, safety CRC, cross-check redundancy of CRC, and the CIP safety protocol, for detecting any errors.

Single-Cast Versus Multi-Cast

There has been debate regarding single-cast (or uni-cast) versus multi-cast communications. The primary difference between them is that in single-cast the piece of information is sent from one specific point to another specific point. Multi-cast is the term used to describe communication where a piece of information is sent from one or more points to a set of other points. In this case there may be one or more senders, and the information is distributed to a set of receivers. The receiver that needs the information receives it, while the remaining receivers simply ignore the information. The primary benefit in multi-cast is when it is used in a corporate environment where all routers are multicast-enabled, it can save a significant amount of bandwidth. CIP safety has the capability of providing both types of connections, single or multi-cast.

As the manufacturing world continues to move forward, new technologies will continue to emerge and challenge our methodology and practices. And with these changes comes an even greater focus on the safety liabilities of these processes. This is why it is of paramount importance that we continue to define and refine the standards—to ensure that safety technology grows with the equipment it monitors. The key to the success of any system relies heavily on the system's seamless integration and simplicity of operation. In manufacturing plants throughout the world, the integration of multiple machines and applications will continue to produce challenges for manufacturing and for the networks that must be put in place to support the system. At the end of the day, it is only logical that safety networking be implemented to not only protect the production process, but to ensure the safety of the most important component of any manufacturing system—its people.

The routing of Ethernet/IP safety messages over this network is possible because **the end device is responsible for ensuring the integrity of the data.**