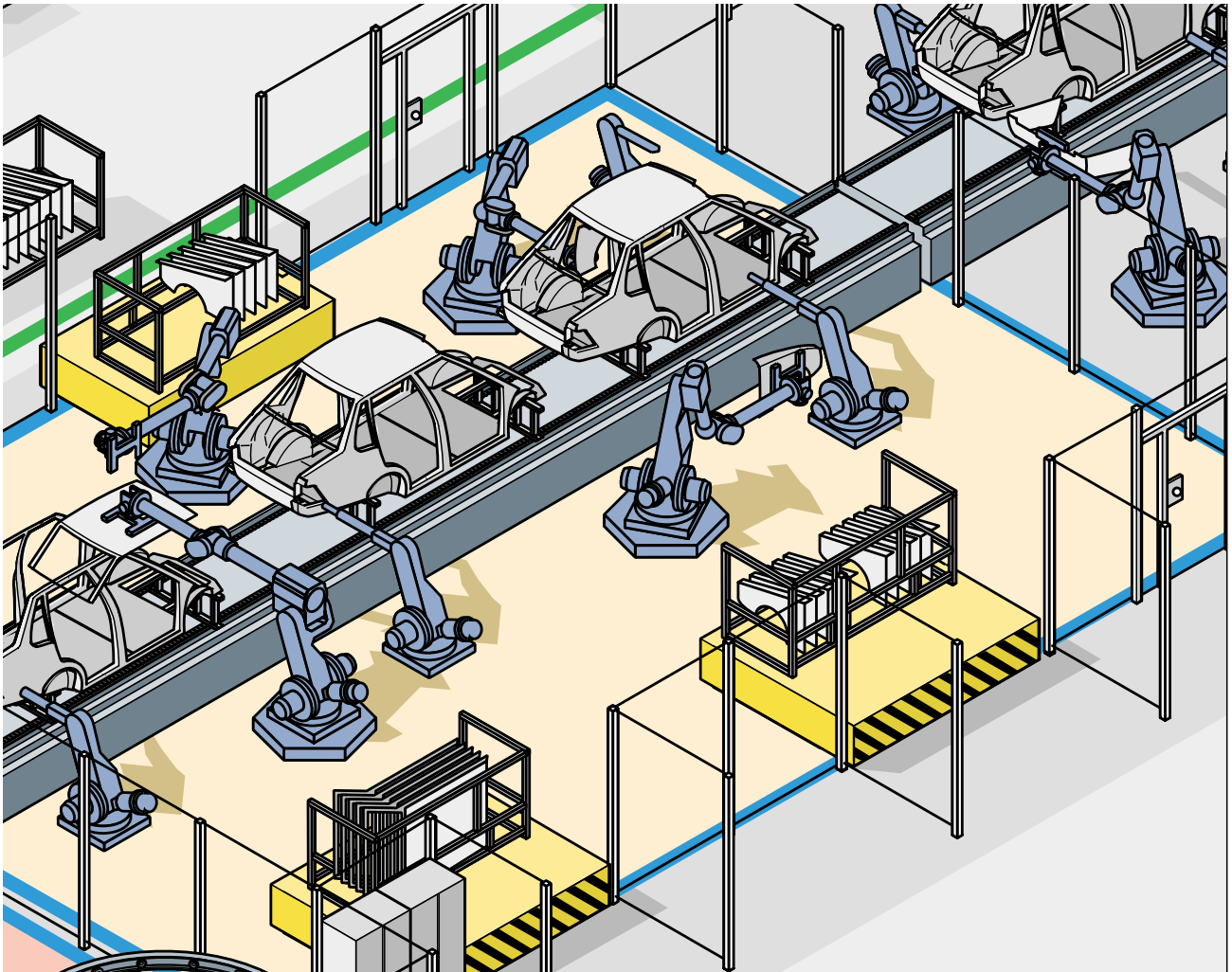


# Safety Networks

Increase Productivity,  
Reduce Work-Related Accidents and Save Money



## Executive Summary

With metal-cutters, blistering hot ovens and swinging robotic arms as workplace companions, safety control systems are vital in protecting factory-floor workers and the machines they operate. Recent modifications to international safety standards are allowing suppliers to introduce a new breed of safety controls and networks that leverage the modern, robust technology found in standard applications. Manufacturers taking advantage of these new offerings are implementing safety systems that increase productivity, reduce work-related accidents and save money. As a result, safety controls and systems aren't just protecting workers and machines anymore — they're delivering a return on investment.

## Safety Systems Pick up the Pace

This extended role is a significant achievement, as safety technology has traditionally lagged behind standard controls in adopting programmable technology. To illustrate, let's review the major automation milestones of the past few decades. Thirty years ago, manufacturers used relay-based control for all of their manufacturing operations. Relay panels were expensive to build and maintain and difficult to reconfigure. To remedy this, the industry switched to programmable logic controllers (PLCs) and other smart controls. These devices required less hardwiring and were therefore much less expensive to install and maintain. PLCs also were more adaptable to the evolving needs of the production process, with condition-based control among their capabilities.

Then came the age of open, digital networks. Although smart controls were capable of supplying users with monitoring and diagnostic information, it took a digital network to quickly facilitate the control, configuration and collection of that data. Open networks introduced the benefits of multi-vendor interoperability, and further slashed the number of connections as they replaced hundreds and thousands of individual wires with a single communications cable.

Unfortunately, the prescriptive standards in place at the time meant that safety control systems could not easily benefit from this migration. In fact, most manufacturers are still using the same expensive, inflexible controls for their safety system that they deemed archaic long ago for their standard control systems. The good news is that safety technology is catching up – the byproduct of an increased demand for flexibility, efficiency and ease-of-use from users of safety components. With advances such as safety laser scanners for perimeter guarding, isolation systems with millisecond tag outs, and safety PLCs with dual-CPU's and fast response times, safety applications can now match the performance and flexibility of PLC systems in the rest of the factory.

Now, with more flexible standards and a new mindset toward safety, manufacturers are ready for the next round of productivity gains. In the same way the standard control industry moved from relays to PLCs in the 70s — and from hardwiring to digital networks in the 90s — safety control systems are now taking the next evolutionary step.

## Safety Networks Introduced

The development of safety networks represents a major step forward in the overall migration of safety applications. Similar to its everyday counterpart, a safety network is a fieldbus system that connects devices on the factory floor. It consists of a single cable that allows for quick connect/disconnect of replacement devices, simple integration of new devices, easy configuration and communication between the devices, delivery of diagnostic data (as opposed to just on/off status updates), and a wealth of other features to help workers maintain a safety system more efficiently. But unlike standard networks, which also provide this functionality but are designed to tolerate a certain number of errors, a safety network is designed to trap these errors and react with pre-determined safe operation.

Companies can choose to deploy a safety network for the significant wiring savings and ease-of-installation, or they can use it to their full advantage by capitalizing on the network's diagnostic capabilities, enhancing the underlying performance of the manufacturing process. When an error occurs today, for example, a hardwired safety system responds by shutting off the power to all the PLC outputs — essentially shutting down the entire application. Regardless of the problem, the response of the system is the same. This reaction negates a hazardous situation, but at a substantial cost. Once an entire application is powered down, it takes a significant effort to get it up and running again — time and energy that equates to significant profit loss and broken commitments to customers.

With a networked system, on the other hand, the safety controller can make a narrower decision as to what needs to be shut down and what can continue operating. If, for instance, a misaligned safety sensor is impacting a robotic arm in a cell located at the far end of the facility, the shutdown can be limited to that particular cell. Not having to cut power to an entire area or machine when a safety event occurs translates

into greater productivity. The key to this ability is the advanced diagnostics designed into the controller, networks and I/O devices, as well as both firmware and application software-level response to those diagnostics.

At first it may seem risky to rely on communications and software to change a system’s behavior in such a way. However, the protocol inherent in a safety network takes measures to ensure a high level of integrity within the application. These measures, such as message redundancy and cross checking, ensure that safety messages are reliably transmitted from one device and received at another in the predetermined time and with the integrity of the data content maintained.

## The End Justifies the Means

**IEC 61508** — the International Electrotechnical Commission (IEC) standard for functional safety in programmable electronic systems — defines the functionality of safety networks. This seven-part standard defines the requirements of a safety system to comply with the appropriate safety integrity level (SIL).

Recently introduced, IEC 61508 redefined the way safety systems are assessed, switching from a prescriptive rules based approach to a goal-oriented approach. This change has been instrumental in allowing the development of advanced safety control systems and, in particular, in the growing use of safety networks as an alternate to hardwired circuits. Prior to IEC 61508, a vendor demonstrated that its components and solutions were designed in accordance with block diagrams prescribed by the assessors. Now users and vendors together perform risk assessments to examine potential failures, documenting the consequences and probability of occurrence. This analysis determines the SIL that must be achieved by the protective system, which in turn defines the maximum allowable Probability of Failure on Demand (PFD).

The top-most integrity level (SIL 4) is applied to such critical equipment as that used on aircraft and in nuclear power plants. SIL 3, meanwhile, is the highest-level found in traditional manufacturing and process applications.

Safety Integrity Level	Mode of Operation	
	<i>Average Probability of Failure on Demand – Per Hour</i>	
	Low Demand	High Demand or Continuous
SIL 4	> 10 <sup>-5</sup> to < 10 <sup>-4</sup>	> 10 <sup>-9</sup> to < 10 <sup>-8</sup>
SIL 3	> 10 <sup>-4</sup> to < 10 <sup>-3</sup>	> 10 <sup>-8</sup> to < 10 <sup>-7</sup>
SIL 2	> 10 <sup>-3</sup> to < 10 <sup>-2</sup>	> 10 <sup>-7</sup> to < 10 <sup>-6</sup>
SIL 1	> 10 <sup>-2</sup> to < 10 <sup>-1</sup>	> 10 <sup>-6</sup> to < 10 <sup>-5</sup>

With this goal-oriented approach, the end result is more important than the equipment used to achieve it. So essentially, the new standard questions whether a system is safe rather than if it “looks” safe. Once this determination has been made, the decision of whether to use a network is the same as deciding on networks in standard applications, such as improved diagnostics, lower cost or the need for a distributed system.

## Selecting a Safety Network

Now that the IEC standards framework no longer excludes safety networks, several vendors and/or organizations are rapidly developing multiple networks to meet the expected demand from end users. Due to the general nature of guaranteeing safety, these networks will most likely share basic features, such as pre-determined safety states, determinism and dual-CPU designs.

Most importantly, safety networks must be designed to allow devices to enter a pre-determined safe state when a communication error occurs. A safe state for one device, such as the swinging robotic arm, could be immediate “power off.” The safe state for an exhaust fan, meanwhile, could be “power on” ensuring harmful substances cannot accumulate and if present are dispersed.

Second, a safety network must be deterministic to ensure all safety messages are transmitted in a predefined and predictable amount of time. A safety network allows customization for each device to have its own periodic response time. This is scaleable to a single device or a chain of associated safety devices. From this, safety devices have guaranteed expectation of message delivery. Some safety messages include a timestamp, which is checked to ensure that it arrives within the defined time expectation. Safety messages arriving beyond the time expectation will cause the affected connection and associated device(s) to go to its safe state.

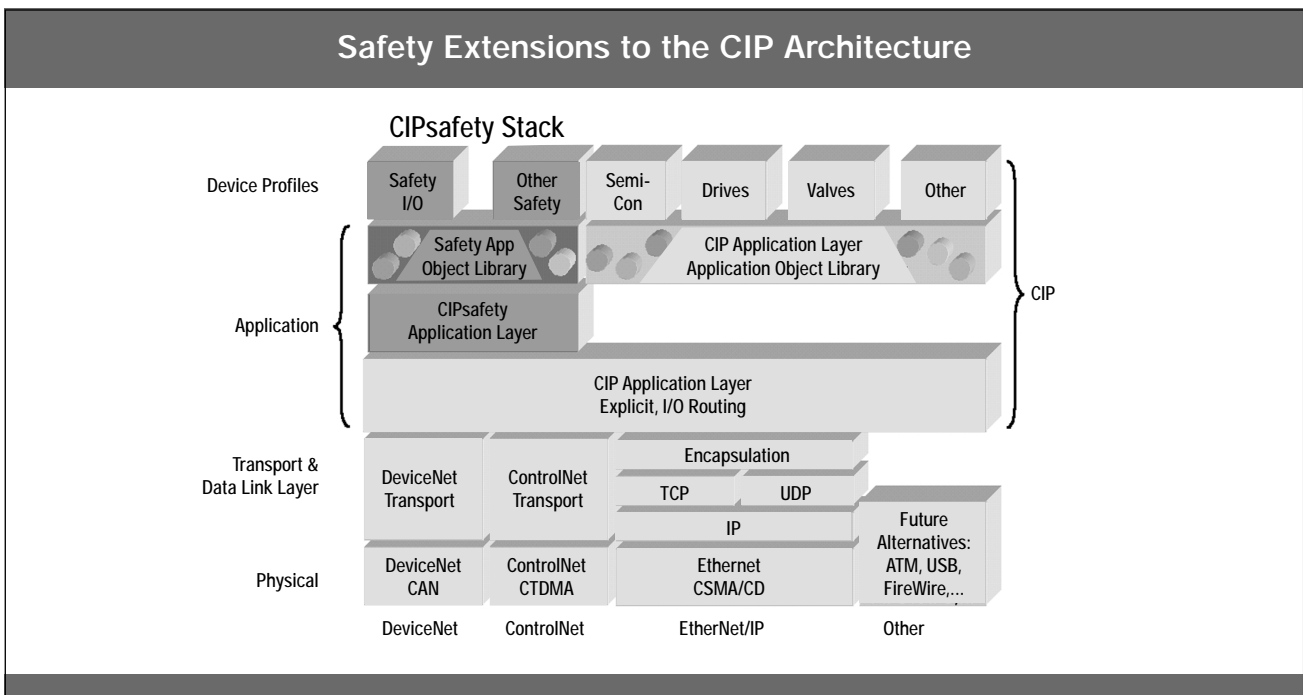
Devices on a safety network require a dual channel design for crosschecking of safety messages as they arrive. The safety network protocol requires that all safety data be transmitted twice; once normal and once with the data inverted. Because data redundancy is built into the network protocol, the dual channels will each pick up messages and cross check one another's results to guarantee accuracy.

Beyond these building blocks, there are many features that will differentiate safety networks. One network that stands out is DeviceNetsafety™, which provides the most efficient method for closing a safety loop and is designed to offer the benefits of a multi-link architecture as part of the CIP Architecture.

### Vendor Community Introduces CIPsafety™ Extensions

In October 2002, ODVA and its member companies received concept approval from TÜV Rheinland for CIPsafety. ODVA's approach is unique, as it supports the only safety protocol that is media-independent. Safety extensions to the Common Industrial Protocol (CIP) – on which DeviceNetsafety™ is based – can be applied to other CIP-based networks like ControlNet™, EtherNet/IP™ and other future technologies. This allows for the seamless transfer of safety I/O messages from any point in the multi-segment architecture to one or more points in the same architecture using either point-to-point or multi-cast connections.

DeviceNetsafety will meet the requirements of SIL 3. When the network becomes available in 2004, manufacturers with safety applications can take advantage of the cost savings and flexibility inherent to a standard DeviceNet™ connection.



## DeviceNetsafety Advantages

In addition to the producer/consumer architecture, which allows devices to synchronize for precise system performance, DeviceNet has many attributes that make it ideal for safety systems. These include:

- Robust media, which has been tested in high noise and other challenging environments
- Automatic checking for duplicate node addresses
- Built-in retries at the data-link layer
- Priorities established by configuration
- Bit error rate of  $\leq 10^{-7}$  under stress (i.e., approximately one error transmitted every 150 years on a fully loaded system)
- Error counters for each connection to the network
- Connection based messaging so both producer and consumer can identify data failure

Also, standard DeviceNet media and topology requires no changes when used in safety implementations. That means current DeviceNet users can continue to use existing wiring to implement a safety system by just adding DeviceNetsafety devices to the existing network. In fact, end users will be able to integrate standard and safety controls on a single network. This feature has a significant pay-off, as safety devices that are usually hardwired to a safety controller can now be directly connected on an existing DeviceNet, sharing the network with other safety and standard devices.

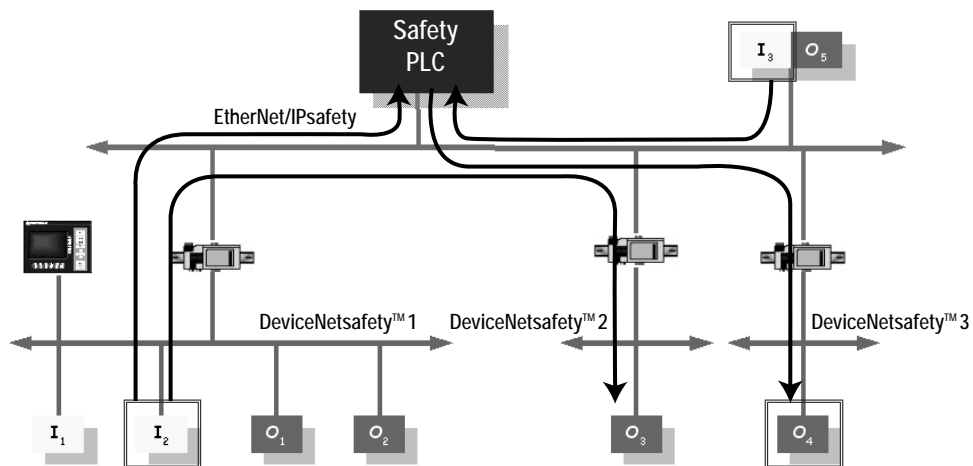
The DeviceNetsafety Protocol ensures that standard devices do not interfere with the function of the safety devices and vice versa. With other safety protocols, however, manufacturers are forced to run a separate network just for safety controls, adding an unnecessary level of complexity to a system. In addition, a separate network not tightly integrated into the standard control system architecture often precludes systems from responding uniquely to each type of fault.

When dealing with multiple networks, it is important to consider how safety loops are closed. There are two approaches for closing a loop between an input and output device. The first is the controller-centric approach, which mandates that all safety loops go through a safety PLC. The second is the safety network controller approach, which doesn't require a safety PLC to be part of the safety loop. The latter method could be categorized as a conventional relay replacement and is typically used for very tight loop closures. Both approaches have advantages and are not mutually exclusive, which means manufacturers can use a combination of both. A DeviceNetsafety system supports both approaches by allowing any device to talk to any other safety point on the same segment or another segment in the network architecture.

With DeviceNetsafety, diagnostics go beyond the status checking of individual nodes connected to the network by allowing the application to test the integrity of the full loop. Input and output modules can have features such as "pulse test", which verifies that the input or output circuit is functioning and not shorted, and "data echo," which uses feedback to check that an output module has received and acted on a command. Advanced diagnostics can even check the external load to verify that voltage is applied to the actuator, and input or output modules have the capability to detect open or short-circuit wires and loss of power.

Because CIPsafety is an extension of standard CIP, it automatically inherits the bridging and routing capabilities enjoyed today by users of EtherNet/IP, ControlNet and DeviceNet. Therefore, from a plant wide perspective, DeviceNetsafety users benefit from a multi-link architecture. A single DeviceNetsafety network can contain as many as 64 devices, but as DeviceNetsafety is based on a seamless, multi-link architecture, the maximum device count is virtually unlimited. Multiple DeviceNetsafety segments can be interconnected using a high-speed EtherNet/IP backbone, with all the nodes communicating as seamless as if they are on the same segment.

## CIPsafety - Routing Capabilities



When designing a safety system, not only must the number of sensors and actuators be considered, but also the maximum response time from sensors to actuator. This will frequently result in an engineer minimizing the number of nodes on a single segment to maximize the network bandwidth available to each node. This becomes even more significant as the number of sensors that can be connected to a single node is much smaller on safety networks than on standard networks due to the safety protocol overhead. As a remedy, engineers can break DeviceNetsafety solutions into separate networks, with each network configured to provide the precise response time needed, while transmitting only required information to the other networks, therefore maximizing bandwidth. In addition to separate networks, the multi-loop feature and safety controllers also help ensure performance.

This feature allows OEMs to design standalone machines each with its own separate subnet, ensuring that safety loops on one machine can be accessed but not negatively impacted by other machines. From an OEM's standpoint, the ability to ensure and take responsibility for a performance output, such as their machine's safety exclusion zone, is critical. An end user, meanwhile, also benefits because multiple machines can be cross-interlocked using an EtherNet/IP backbone without risking the set parameters or performance integrity of any individual machine.

Combined, these features set CIPsafety apart from the competition.

### But is it Safe to Integrate?

Integration is a definite benefit for standard applications, but some end users may be initially cautious about taking advantage of the feature in safety applications, and rightly so, as there is a need (stated in IEC61508) to maintain standard and safety control systems as independent entities. But too often end users take separation to the physical extreme, which has created the need for technicians who are experts in both standard and safety PLCs. These technicians are scarce. Instead, most companies have engineers with a working-but-not-proficient knowledge of both sides, with the result being poorly configured applications with safety systems that are routinely circumvented due to the bottlenecks they cause — a potentially dangerous scenario.

When it comes to integration, IEC 61508 calls for one of two approaches: physical separation of safety and standard control functionality or logical separation. DeviceNetsafety supports both approaches but is optimized to enforce logical separation. This logical separation ensures safe operation and provides

greater opportunities to improve productivity at a lower cost than implementing physical separation. A single controller platform can be used to enforce logical separation, which simplifies configuration of the safety system and reduces training. Further it enhances the overall safety of the system by minimizing the level of specialist expertise required to maintain the system.

## **Safety Today and Beyond**

The additional flexibility that DeviceNetsafety provides will in turn enhance the speed of system configuration, testing and commissioning for a reduction in total cost of ownership. These gains, already experienced by DeviceNet users, include reducing hardwiring by up to 80 percent, slashing installation time from days to hours, virtually eliminating troubleshooting at start-up, and improving production efficiencies due to valuable advanced diagnostics on machines and individual plant floor devices. But despite these benefits, the migration to safety networks won't happen overnight. The first step for end users is to work with a qualified consultant to perform a risk assessment of their facility. Among other things, this assessment will identify risks, determine appropriate SIL levels and evaluate the benefits of implementing a safety network for their application.

Once the DeviceNetsafety Specification is complete and products are available, early adopters will start to design and implement applications where there is presently significant human interaction with potentially dangerous equipment (for example, machine perimeter guarding). The big gain in these environments will be reducing the risk of injuries and keeping as many operations and areas of the plant up-and-running when a worker enters a zone with operating machines.

Following this, end users will begin taking advantage of the second phase of CIPsafety development, which will allow companies to link distributed DeviceNetsafety segments with standard CIP-based backbone networks like EtherNet/IP. Then, as requirements continue to expand, the CIPsafety protocol will be deployed to EtherNet/IPsafety™ and perhaps other safety network solutions.

As a result of safety network development, manufacturers will implement safety systems that increase productivity, reduce work-related accidents and save money.

## **Questions End Users Should Ask About a Safety Network**

- Does it allow you to put both standard and safety devices on the same wire?
- Does it allow peer-to-peer messaging between safety PLCs and safety network controllers?
- Will it provide the ability to connect a single input device to multiple output devices (multi-cast)?
- Does it have a convenient, main network/subnet architecture? In other words, can you have a safety PLC on Ethernet controlling a number of devices on the safety network?
- Is a logical, rather than physical, connection possible between devices on adjacent device-level safety networks?
- Are plug-and-socket based cable systems available to help install the safety system more efficiently?
- Is it possible to have a safety PLC providing sequential and conditional logical control of the Safety Protection System?
- Is it possible for safety sensors and actuators to communicate directly?
- Is it possible to solve a safety application requiring logic without the need for a safety PLC?
- What is the input to output time for the PLC?
- What is the network cycle time?
- Is it possible to get information from safety devices into standard devices like PLCs and HMIs?
- Does the network have multi master capabilities?



## About ODVA

ODVA is an international association comprised of members from the world's leading automation companies. Collectively, ODVA and its members support network technologies based on the Common Industrial Protocol (CIP™). These currently include DeviceNet™, EtherNet/IP™ and CIPsafety™. ODVA manages the development of these open technologies, and assists manufacturers and users of CIP-based networks through tools, training and marketing activities. In addition, ODVA offers conformance testing to help ensure that products built to its specifications operate in multi-vendor systems. The organization also is active in numerous industry standards bodies and consortia to drive the growth of open communication standards. For more information, visit its web site at [www.odva.org](http://www.odva.org).

For additional information contact [CIPsafety@odva.org](mailto:CIPsafety@odva.org)

*DeviceNet, DeviceNetsafety, CIP and CIPsafety are trademarks of ODVA. EtherNet/IP and EtherNet/IPsafety are trademarks used under license by ODVA.*

*Copyright © 2003 ODVA. All Rights Reserved.*