

ODVA
2007

CIP Networks Conference
and 12th Annual Meeting

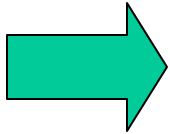
INNOVATIONS FOR PROCESS APPLICATIONS

CIP Safety Enhancements

Technical Track

www.odva.org

Agenda



1. CIP Safety Today

2. New Safety Format Features

3. Examples: Wireless EtherNet/IP

4. Examples: Redundant Safety Controller

5. Summary

CIP Safety

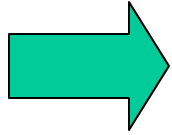
CIP Safety is a compact protocol

- ▶ Emphasis on short data packets for DeviceNet
- ▶ No reliance on fragmentation
- ▶ Mechanisms in place to detect non-critical errors
 - Closes the connection to assure the safety state is achieved in a consistent and timely manner
 - Acceptable behavior for machine safety since the probability of occurrence is very low

CIP Safety

- ▶ Closing connections on non-critical errors creates issues for process safety applications
 - Process safety applications want the same level of error detection
 - Want SIL3 Safety Integrity Levels without connection shutdown on non-critical errors
- ▶ CIP Safety has a new connection format that allows connections to continue to operate with non-critical errors

Agenda



1. CIP Safety Today

2. New Safety Format Features

3. Examples: Wireless EtherNet/IP

4. Examples: Redundant Safety Controller

5. Summary

Safety Reaction Times

- ▶ Extended to serve a wider variety of applications
- ▶ Reaction Time allows systems to ride through system failures
 - Network routing delays
 - Extra time margin can be used to build in tolerance for packet delivery delays
 - » Wireless Networks
 - » SCADA
 - Redundant Control System switchover
 - Fault Tolerance in process applications is defined as detection without shutdown
 - Extra time margin can be used for switchover delays

New Format Features

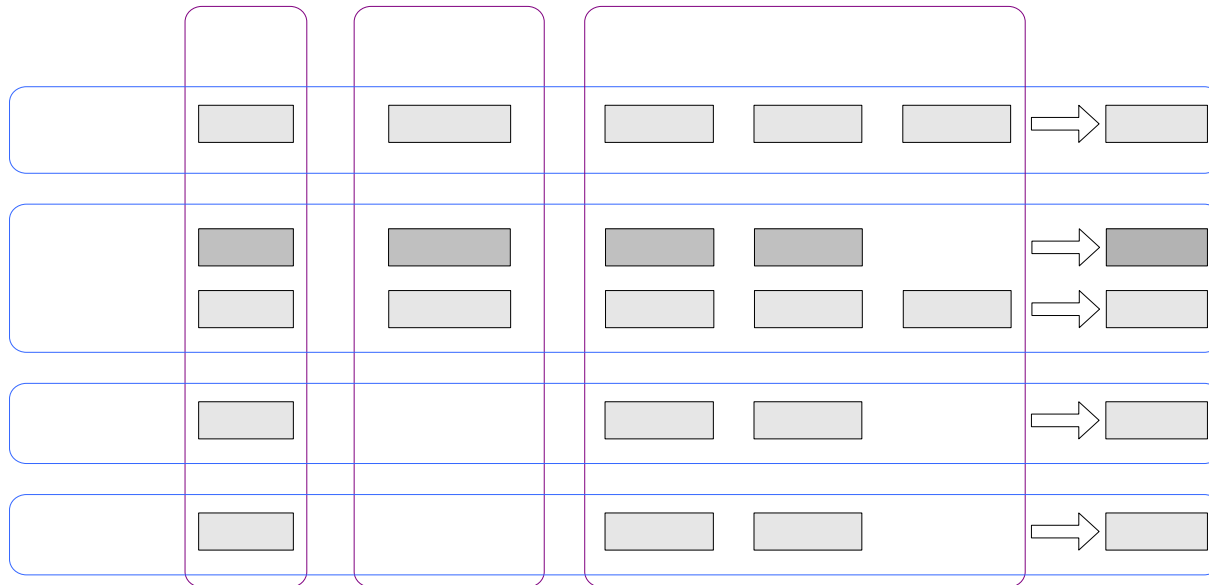
The new format and associated specification enhancements

- ▶ Single 24-bit CRC
- ▶ Virtual 32-bit Time Stamp
 - Upper range encoding
- ▶ Extended Timeout Multiplier
- ▶ Dynamic format determination

New 24-Bit CRC

- ▶ Current CIP safety packet format embeds two different 8-bit CRCs in data transmissions; each covering different parts of the packets.
 - 8-bit CRCs allows compact packet format
 - CRC diversity provides SIL3 integrity levels
- ▶ New format uses a single unique 24-bit CRC
 - Provides the compact format for 2-byte data packets while providing the SIL3 bit error detection.
- ▶ CRC also used for new Time Coordination and Time Correction packet formats
- ▶ When the data is greater than 2 bytes, the 24-bit CRC is combined with the existing 16-bit CRC
- ▶ Single 24-bit CRC covers both the data and the Time Stamp

Virtual 32-Bit Time Stamp



- ▶ New format extends the range of the Time Stamp
- ▶ The extended range is not transmitted
 - The upper range is used to seed the CRC
 - Producer and Consumer must agree on value

**PID
seeds**

**1 & 2
Byte
Format**

PID

Virtual Time Stamp cont.

- ▶ The virtual 32-bit range greatly increases ability to detect message insertions of packets
- ▶ Added detection greatly enhances protocol error detection in safety applications with long reaction times
- ▶ With the new format, packets can be dropped and the connection maintained

Extended Timeout Multiplier range

- ▶ New format connections can support larger timeout multipliers
- ▶ Larger timeout multipliers increase the delays tolerated by the protocol before a consumer would declare the connection faulted
 - Allows longer Network Reaction Times

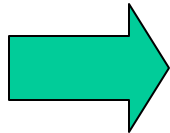
Dynamic Format Detection

- ▶ Integration of a new format requires a simple way to detect format support
 - Networks of devices with mixed levels of support
- ▶ Specification enhancement includes
 - New Originator algorithms to dynamically determine the capability of targets
 - New EDS keywords
 - Configuration Software can determine capability
 - New object attributes in originators

Agenda

1. CIP Safety Today

2. New Safety Format Features



3. Examples: Wireless EtherNet/IP

4. Examples: Redundant Safety Controller

5. Summary

Wireless EtherNet/IP Example

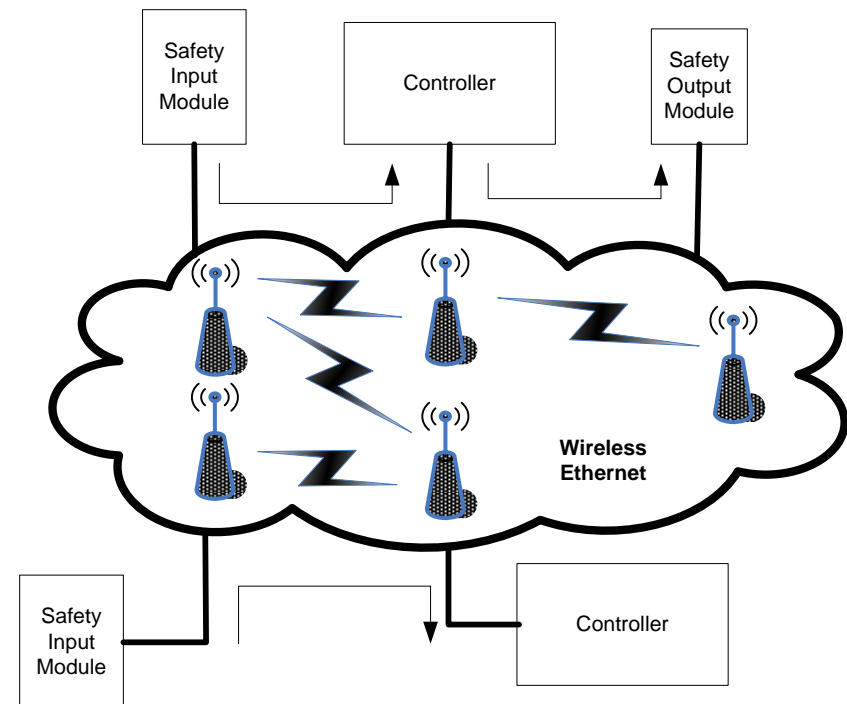
- ▶ Ethernet provides an opportunity to distribute the control over wider geographic areas
- ▶ Routers, switches, and wireless technology overcomes distance and physical limitations
- ▶ Larger control systems can be interconnected with control connections
- ▶ Additional network components present more opportunities for delivery delays and new sources of errors.

Wireless EtherNet/IP Example Cont.

- ▶ Wireless Ethernet can solve intractable interconnection problems
 - i.e. Safety Condition Monitoring of remote drives
 - But the technology introduces potential for delays and lost packets because of the nature of how it works
- ▶ CIP does not define guidelines for using wireless protocols with EtherNet/IP
 - The technology can have wide-ranging effects on distance and throughput
 - Direct Sequence versus Frequency Hopping
- ▶ The new format extends the timeout periods such that safety control algorithms can tolerate wireless network delays.

Wireless EtherNet/IP Example cont.

- ▶ Two controllers operate a portion of their control over wireless Ethernet
- ▶ Applications pick up remote points that cannot be reached with cable
- ▶ Input multi-cast to two controllers
- ▶ Independent control loops and separate access points compete for the right to transmit
 - Wireless Ethernet protocols operate in a collision domain
- ▶ Noise sources can disrupt communications



Wireless EtherNet/IP Example cont.

- ▶ Assume controllers have reaction times of 500 ms
- ▶ If the control application response time can tolerate it, the way this is done is to allow the connections to operate with greater timeout periods.
- ▶ The input and output connections allow for larger number of redundant packets
 - greatly increase the probability that the age limits will never be reached
- ▶ Extended range of the timeout multiplier allows additional margin for delays or lost packets while maintaining the needed safety reaction time.

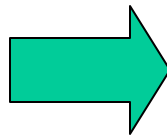
Parameter	Value
Input Cyclic Rate	20 ms
Input Timeout Multiplier	5
Input Safety Data Age Limit	145 ms
Output Cyclic Rate	40 ms
Output Timeout Multiplier	5
Output Safety Data Age Limit	282 ms
Safety Loop Reaction Time ¹	344 - 464 ms
¹ Safety Loop Reaction time is input-to-output. The two values are single-fault and multiple-fault reaction times respectively based on typical safety controllers.	

Agenda

1. CIP Safety Today

2. New Safety Format Features

3. Examples: Wireless EtherNet/IP

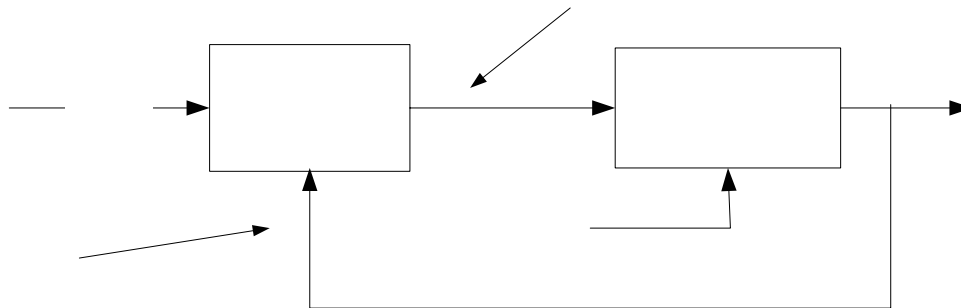


4. Examples: Redundant Safety Controller

5. Summary

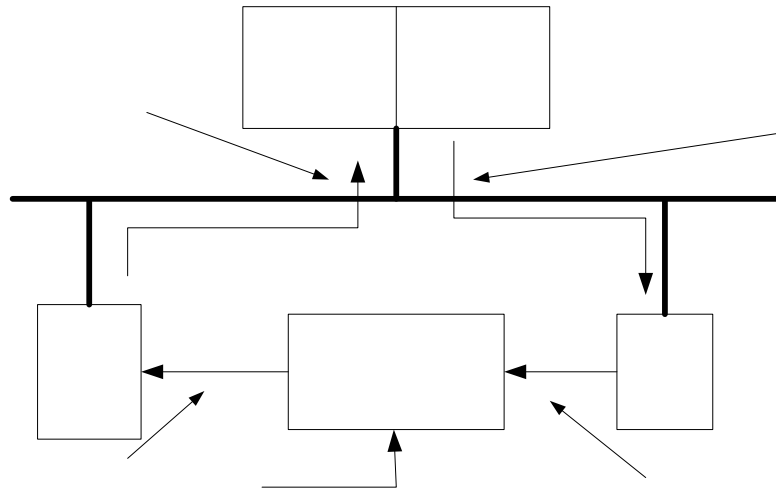
Process Application Example

- ▶ Assume a generic process control loop
 - A new control command every 10 seconds
 - 10x faster input data sampling
- ▶ Assume system needs to be monitored for SIL3 safety by a separate safety-critical set point.
- ▶ Assume the time needed to sense a problem and initiate a safety shut down is the same as the time to perform normal control.
- ▶ So the 10 second update rate is the required Safety Reaction Time.



Process Application Example cont.

- ▶ CIP Safety network used to monitor for SIL3 safety shutdown
- ▶ On switchover, Safety output connections stop producing data
 - Consumers need margin to keep the connections active
- ▶ Safety input connections continue to produce during switchovers
 - Consuming controller provides time coordination packets to keep safety time clocks synchronized.
 - Input producers need margin when time coordination packets aren't being received.



Process Application Example cont.

- ▶ Cyclic rate and timeout multiplier allow connections to tolerate delays up to 5 seconds
 - Yet the 10 second safety reaction time requirement is met.
- ▶ Safety algorithm runs once per half-second and sends output command at the end of each run.
- ▶ Safety controllers monitor the age of the safety input data
 - If the safety input data is older than 5.18 seconds, a safety output command will be issued to shut down the process.
- ▶ 2x packet redundancy assures the process gets sufficient samples for good control.
- ▶ Safety output module will shut down the process if the age of last received command is older than 5.03 seconds.

Parameter	Value
Input Cyclic Rate	500 ms
Input Timeout Multiplier	8
Input Safety Data Age Limit	5.18 sec
Output Cyclic Rate	500 ms
Output Timeout Multiplier	8
Output Safety Data Age Limit	5.03 sec
Safety Loop Reaction Time¹	5.5 - 10 sec

¹ Safety Loop Reaction time is input-to-output. The two values are single-fault and multiple-fault reaction times respectively based on typical safety controllers.

Agenda

1. CIP Safety Today

2. New Safety Format Features

3. Examples: Wireless EtherNet/IP

4. Examples: Redundant Safety Controller



5. Summary

Summary

- ▶ CIP Safety has added a new format that is especially suitable for the availability requirements of process control.
- ▶ It is also suitable for general control applications where there is a need to tolerate larger than normal packet delays such as Wireless Ethernet.
- ▶ CIP safety continues to find innovative ways to bring SIL3 safety to a wider range of applications; to provide customers with the needed high integrity while serving the need for availability.