

# **CIP SAFETY: INNOVATIONS IN PROCESS APPLICATIONS**

Paul Kucharski  
Principal Engineer, Safety Systems  
Rockwell Automation

Presented at the ODVA  
2007 CIP Networks Conference & 12<sup>th</sup> Annual Meeting  
September 18-20, 2007  
Englewood, Colorado USA

## **Abstract**

CIP Safety has typically been used in machine safety applications, where fast response times and stop on a failure are common modes of operation. This paper will describe an upcoming CIP Safety Specification Enhancement which will provide additional services to allow operation in safety applications where longer loop times, fault tolerance and the ability to maintain operation during non-critical errors are required. These applications include, but aren't limited to SCADA, process and wireless.

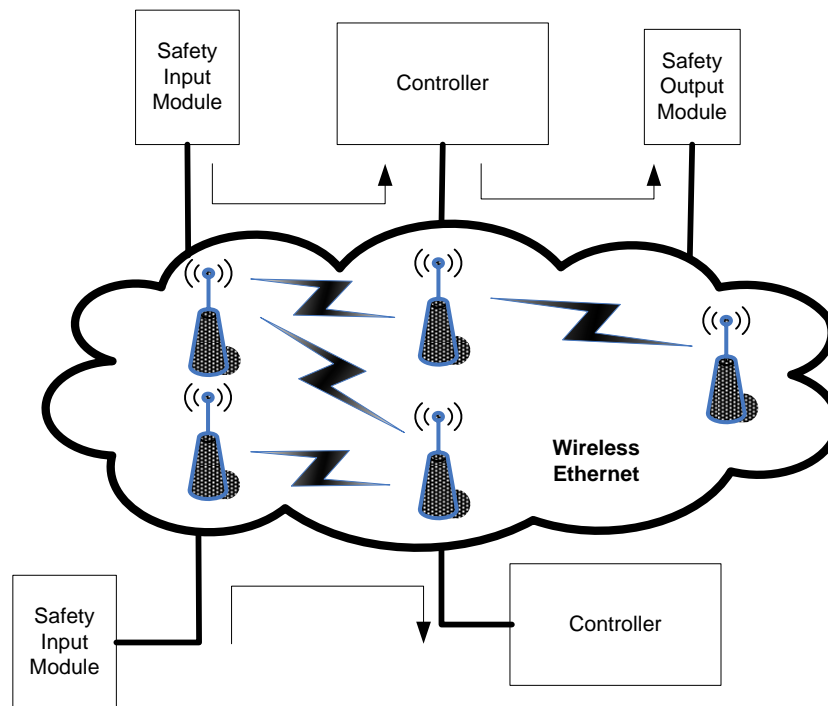
## **Introduction**

CIP Safety is a very compact protocol because its design placed great emphasis on being able to send short data packets over DeviceNet without having to rely on fragmentation. It also has numerous mechanisms in place to detect a wide variety of non-critical errors and in each case close the connection to assure the safety state is achieved in a consistent and timely manner. This behavior is acceptable for machine safety applications since the probability of occurrence for these errors is very low. But closing connections when a non-critical error is detected creates issues for process safety applications regardless of the probability of occurrence. Process safety applications want the same level of error detection, but require that SIL3 Safety Integrity Levels be achievable without having to rely on connection shutdown when the error is not safety critical. These special requirements will be accommodated in CIP Safety with a new connection format that has strengthened detection abilities of non-critical errors to ensure that the connections can continue to be available.

One of the other key aspects needed to achieve better availability is longer safety reaction times. The safety reaction time of a CIP Safety system is proportional to the cyclic packet rate and a parameter called the "Timeout Multiplier". It seems counter-intuitive to call this a benefit since in machine safety, fast reaction times are more important; but for process applications (with slower application response times) the extra time margin can be used to build in tolerance for riding through non-critical system errors and packet delivery delays. Building in tolerance for packet delivery delays also facilitates the use of network technologies such as Wireless Ethernet; where packet delays may be more common. The new format on CIP Safety extends the period that can be tolerated before connections shut down while maintaining SIL3 levels. This is done by extending the range of the Timeout Multiplier.

## Applications

The use of Ethernet as a control network provides a greater opportunity to distribute the control over wider geographic areas than other CIP networks. The use of routers, switches, and wireless technology overcomes distance and physical limitations common in wired networks. It also allows for larger control systems to be interconnected with control connections. The additional network components present more opportunities for delivery delays and new sources of errors. Wireless Ethernet can solve some intractable interconnection problems for many users, but the technology introduces potential for delays and lost packets because of the nature of how it works. CIP does not currently define any guidelines for using wireless protocols with EtherNet/IP; so the technology chosen can have wide-ranging effects on distance and throughput. The new format gives users greater flexibility to extend the timeout periods and also allow the safety protocol to drop packets when errors are generated without having to close the connections. With the new format, users don't have to sacrifice availability to make use of these technologies. Figure 1 shows an example where two controllers are operating a portion of their control over wireless Ethernet. Applications that need to pick up remote points that cannot be reached with cable can connect them to a controller using wireless access points.



**Figure 1 : Distributed Control over Wireless EtherNet**

Unlike EtherNet/IP with switch technology, Wireless Ethernet protocols generally operate in a collision domain and the request-to-send/clear-to-send sequence plus retries and acknowledgement can extend the time it takes to successfully transmit a packet; while other packets wait for access. Multi-cast productions are broadcast and are not acknowledged; so the CIP cyclic rate needs to have enough redundant packets to account for packets lost in wireless transmission. Noise sources in a plant can disrupt communications intermittently and broadcasts will not have the benefit of retries when no acknowledgment is received. Good design practices can alleviate many of the issues with wireless technology, but control system designers still need to be able to anticipate disruptions and throughput limitations and account for them in how safety connections are configured to avoid unnecessary shutdowns of the control system.

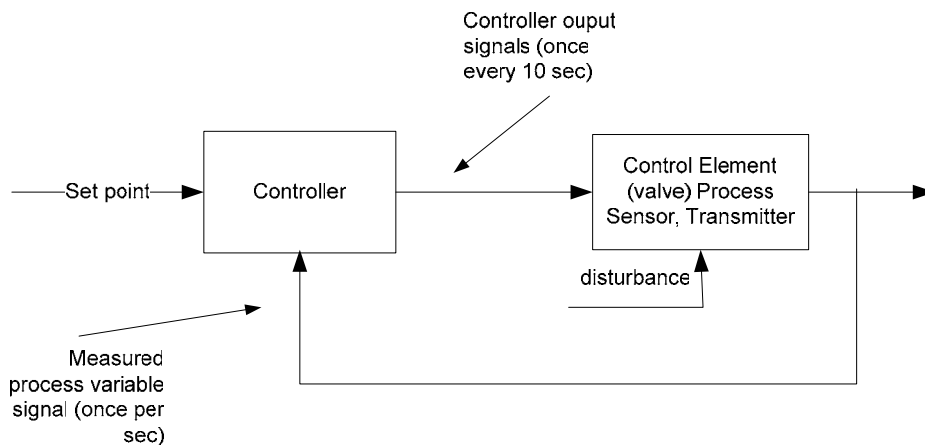
Assume a remote input module is multi-casting the input data to two controllers and there are independent control loops and separate access points all competing for the right to transmit. If we assume the controllers in this example have worst-case safety reaction times of 500 ms, a possible set of CIP safety connection parameters are shown in Table 1. 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.

Table 1 shows that with a timeout multiplier of 5, both the input and output connections allow for a larger number of redundant packets to greatly increase the probability that the age limits will never be reached. The extended range of the timeout multiplier allows a user to build in 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 <sup>1</sup>	344 - 464 ms
<sup>1</sup> 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.	

**Table 1 : Example Wireless Ethernet Safety Connection Parameters**

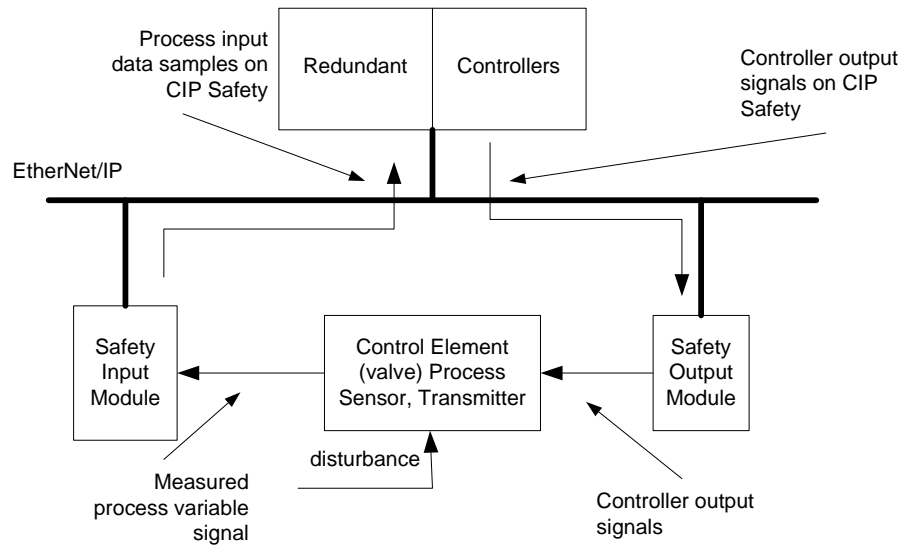
To provide another example, consider a process control application. Assume a generic process control loop like that shown in Figure 2. Assume that this process requires a new control command every 10 seconds and 10x faster input data sampling to maintain good control. Along with some control set point, assume that this system needs to be monitored for SIL3 safety to a separate safety-critical set point. It's reasonable to assume that the time needed to sense a problem and initiate a safety shut down to the Control Element is the same as the time to perform normal control. So the 10 second update rate is the required Safety Reaction Time.



**Figure 2 : Generic Process Control Loop**

If a safety control system and CIP Safety network were used to control this process and to monitor it for SIL3 safety shutdown, it would communicate the input samples and the output commands over the network and the system might be represented as shown in Figure 3.

Process control applications often use redundant control systems that can detect and respond to control failures and execute system switchovers to avoid shutdowns. Typically these switchovers can take seconds to complete and during that time, safety connection data flow is disrupted. Controller redundancy switchovers require network protocols which can ride through the switchover process. During a controller switchover, output connections stop producing data and the consumers need to have sufficient timeout margin to keep the connections active during the time when data isn't being updated. Safety input connections continue to produce data during switchovers, but also expect the consuming controller to provide time coordination packets to keep the safety time clocks synchronized. There needs to be sufficient tolerance in the input data producers to keep the connections alive when time coordination packets aren't being received.



**Figure 3 : Networked Generic Process Control Loop**

There are two loops in this system, the control loop and the SIL3 safety monitoring loop; each with different set points. The SIL3 monitoring loop is what's of interest here. The process input data could be sampled by both the safety loop and control loop. The inputs would be remotely sampled and communicated at some cyclic rate and the controller would run its safety algorithm at a rate that assures the safety reaction time can be met. So the question is what rates to set for the input and safety task/output connections and what timeout multipliers can be used to assure the reaction time is met and still allows sufficient tolerance for network errors, controller switchovers, and/or packet delays?

Every safety control system will have different equations for calculating Safety Reaction Time, but Table 2 shows a possible set of values that could work for this system using CIP Safety and the new format. The combination of the cyclic rate and timeout multiplier allow the connections to tolerate delays up to 5 seconds, yet the 10 second safety reaction time requirement is met. The safety control algorithm would only run once per half-second and would send an output command at the end of each run.

The new CIP connection format extends the range of the timeout multipliers so tolerance can be made for packet delays, dropped packets or controller switchovers. CIP Safety connections use the age of data to determine when a connection needs to be closed. The safety controllers monitor the age of the safety input

module data and in this case if the safety input data is older than 5.18 seconds, a safety output command will be issued to shut down the process.

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 Time <sup>1</sup>	5.5 - 10 sec
<sup>1</sup> 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.	

**Table 2 : Example Process Control Safety Connection Parameters**

With a 500ms input data update rate, the 10x input sample rate is met for the control algorithm; but with 2x packet redundancy to assure the process gets sufficient samples for good control. The safety output module with this set of parameters will shut down the process if it detects the age of its last received command to be older than 5.03 seconds. The expanded range from larger timeout multipliers allow a larger tolerance for dropped or delayed packets. This is primarily facilitated by the process itself having a relatively slow process time constant.

## New Format Features

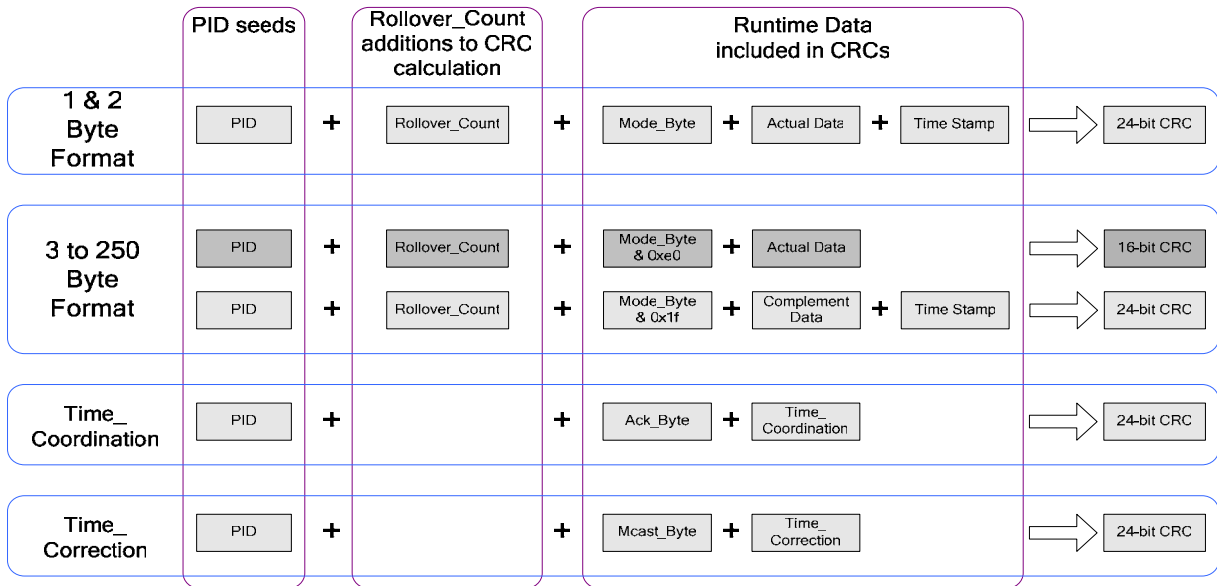
The new format and associated specification enhancements can be summarized as follows:

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

## Virtual 32-bit Time Stamp

The new format supports a method by which the time stamp continues to be transmitted as a 16-bit value while having a virtual 32-bit range. It is called virtual because the upper 16-bits of the time stamp is not transmitted (See Figure 4) and does not take part in the run-time calculations for time synchronization. This allows safety nodes to use a single method for calculating correction values regardless of run-time format.

Yet the virtual 32-bit range greatly increases the ability of the format to detect message insertions of packets. This added detection ability greatly enhances the protocol error detection ability in process safety applications with long reaction times. Even though the upper 16-bits are not transmitted, as shown in Figure 4 the Rollover Count value is used as part of the CRC calculation of the packet along with the producer id (PID). So if the producer and consumer do not use the same upper 16-bit value and/or PID, a CRC error will occur at the consumer. With the new format, these packets are dropped and the connection is maintained.



**Figure 4 : CRC Calculation Order for New CIP Safety Format**

## Single 24-bit CRC

The current CIP safety packet format embeds two different 8-bit CRCs in data transmissions; each covering different parts of the packets. The use of 8-bit CRCs allows the packet format to be very compact while the CRC diversity allows the compact packets to achieve SIL3 integrity levels. SIL3 levels can also be accomplished with larger CRCs, but doing that while maintaining the compact form is challenging. Figure 4 shows the new format using a unique 24-bit CRC that provides the necessary compact format for 2-byte data packets while providing the SIL3 bit error detection. This CRC is also used for the Time Coordination and Time Correction packets in new format connections. When the data is greater than 2 bytes, the 24-bit CRC is combined with the existing 16-bit CRC. Another feature of this new format is that the single 24-bit CRC covers both the data and the Time Stamp; this change is another reason why a single CRC can be used.

## Extended Timeout Multiplier

Because of the added PFD (probability of failure on demand) strength of the new format, connections using the new format can support larger timeout multipliers. The effect of a larger timeout multiplier is to increase the delays tolerated by the protocol before a consumer would declare the connection faulted.

## Dynamic Format Determination

One of the things that complicate the introduction of a new format is how to determine how it gets incorporated into safety systems that may have a mix of capabilities. To minimize the impact to existing devices and systems, the specification enhancement includes new EDS keywords, new object attributes in originators, and new logic requirements to dynamically determine the capability of targets.

## Summary

CIP safety has added a new format that is especially suitable for the availability requirements of process control. It is also suitable for other 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.

---

DeviceNet, DeviceNet Safety, CIP, CIP Motion, CompoNet, CIP Safety and CIP Sync are trademarks of ODVA. EtherNet/IP is a trademark of ControlNet International under license by ODVA. Other trademarks are property of their respective owners.

The ideas, opinions and recommendations expressed herein are intended to describe concepts of the author(s) for the possible use of CIP Networks and do not reflect the ideas, opinions, and recommendation of ODVA per se. Because CIP Networks may be applied in many diverse situations and in conjunction with products and systems from multiple vendors, the reader and those responsible for specifying CIP Networks must determine for themselves its suitability and the suitability of ideas, opinions, and recommendations expressed herein for intended use.

Copyright ©2007 Open DeviceNet Vendor Association, Inc. (ODVA). All rights reserved.  
For permission to reproduce excerpts of this material, with appropriate attribution to the author(s), please contact ODVA on:

TEL	+1 734-975-8840
FAX	+1 734-922-0027
EMAIL	<a href="mailto:odva@odva.org">odva@odva.org</a>
WEB	<a href="http://www.odva.org">www.odva.org</a>