ODVA 2017
Industry Conference
and 18th Annual Meeting

CIP Safety Parameter Data

Kevin Colloton
Rockwell Automation

February 22, 2017

Safety Parameter Data

CIP Safety – Parametric Data

A functional gap in CIP Safety has been identified, the gap is being able to change parametric data in an I/O class safety device (or get data from an I/O class safety device) on-demand (when the need arises) based on safety program execution.

Today, parametric data can only be sent when the device connection is opened, or by embedding parametric data as part of the safety output data assembly.

Sending parametric data in the Forward_Open configuration block is not suitable for program driven parametric data exchange with a safety device. In fact, for a safety device, the configuration block of the Safety Open is part of the Safety Signature and cannot be modified programmatically without violating the devices safety signature.

Using the Output Assembly for on-demand parameter data transfer is both wasteful and a misuse of I/O Connection's intent, not to mention that the number and complexity of the resulting assembly structures would explode.

With no effective mechanism for on-demand programmatic data exchange, CIP Safety systems limit the flexibility customers have for advanced safety applications, especially for motion safety related functions.

Functional Safety - Background

- History
  - Safety sensors
  - Safety relays
  - Failsafe - off = safe state

Functional Safety – PLC's

- Programmable safety
  - Early safety PLC's arrived late 90's (97~99)
    - Significant safety relay mindset
    - Discrete (binary) functions, On / Off
    - Local safety I/O
    - None or limited networked safety capabilities / features

Functional Safety - Integrated Safety

- Introduced in early 00’s (2003~2005)
  - Safety rated automation controllers
    - Programmable control functions (discrete, motion, process)
    - Programmable safety functions (still primary discrete safety functions, On/Off)
    - Local safety I/O modules
    - Networked safety
      - For safety processor interlocking
      - For distributed safety I/O

Integrated Safety Today

- Safety rated automation controllers
  - Programmable control functions (discrete, motion, process)
  - Programmable safety functions (still primary discrete safety functions, On/Off)
  - Networked safety
    - For safety processor interlocking
    - For distributed safety I/O
    - For distributed safety devices (Servo's, Drives, etc)

Safety Devices: Devices that are intelligent, can perform local safety operations/functions, even operate without a safety controller.
Safety capable Servo's, Drives are examples.
For this discussion distributed safety I/O is not considered a device.

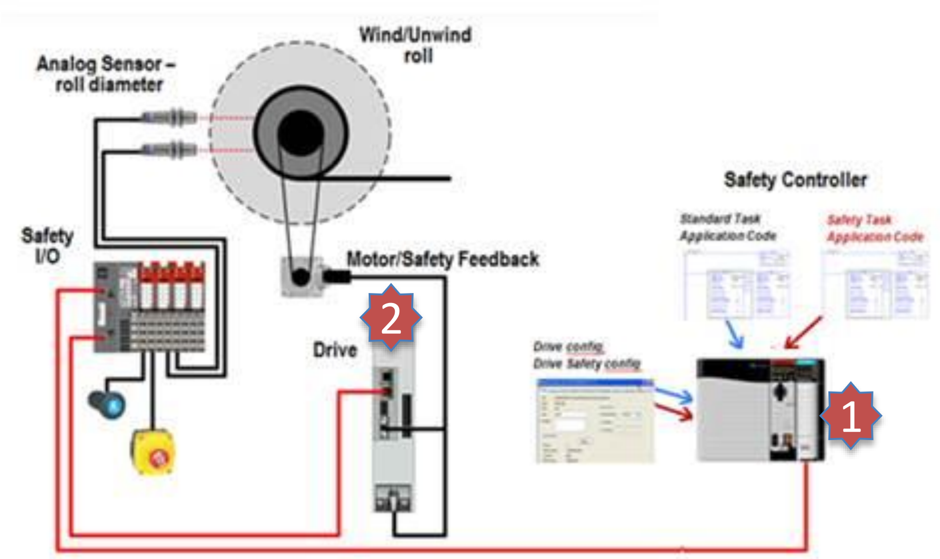
Safety Devices - Today

- Device based safety functions
  - Device safety configuration typically done using a configuration tool
    - High limits, low limits, time setpoints, etc.
  - Device safety features are selected:
    - via configuration tool
    - via bit enable
  - Device safety functions are enabled via safety outputs (bits)
  - Device safety status is monitored via safety inputs (bits)
  - Device safety diagnostics are monitored via safety inputs (bits, or simple error codes)

These intelligent devices typically appear as simple discrete devices in the automation controller, but they are the opposite!

Safety Function Execution

- Safety Controller 1
  - User safety logic
- Safety Devices 2
  - Drive based safety functions
- Both
  - Controller
  - Drive



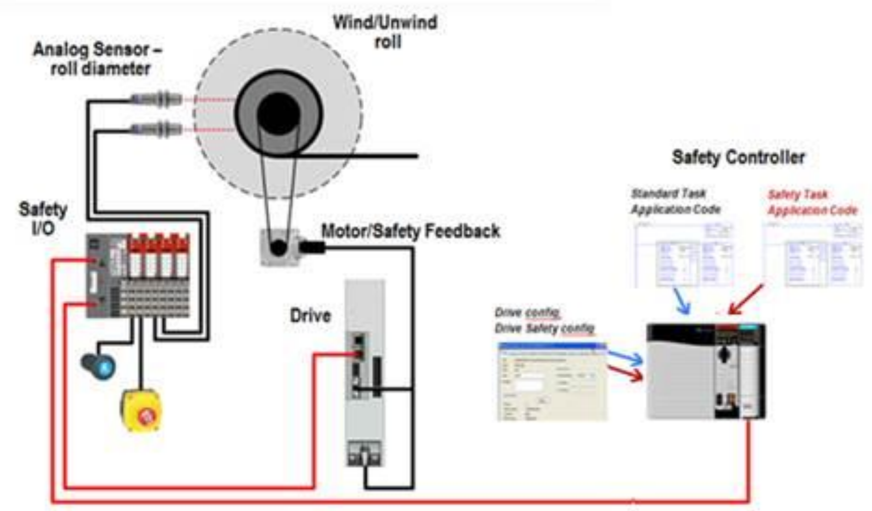
Customer / Market Requests

- More flexibility in changing safety device parameters during runtime
  - Safety logic able to set appropriate parameters based on application needs
    - Speed envelopes
    - Torque limits
    - Timing changes
  - Safety devices currently on the market typically provide 1 – N limits for each supported safety function
    - 1 – 4 speeds
    - 1 – 4 torque
    - 1 – 4 timing

Effectively “hardcoding” these parameters significantly reduces flexibility and increases device management issues for customers.

Variable Safety Data

- Safety Function:
  - SLS of Web (the process)
- Web speed is a function of Motor/Safety Feedback and roll diameter.
- Safety function is executing in the Drive.
- Encoder safety data and Roll diameter safety data used in safety controller to calculate Web Speed.



How does SLS of web get sent to the drives safety core?

Challenge for CIP Safety Devices

- Today there are only two ways to send safety parameter data to a safety device.
  - Safety Forward open
  - Safety Output connection

CIP Safety Forward Open

- There are two primary roles for the forward open
  - Initial configuration of a CIP Safety product / device
  - Establishment of the CIP Safety connection

- Run time problems using forward open process to change device parameters:
  - Safety forward open causes device safe state until configuration process is complete and safety connection is re established.
    - This can’t be used for run time configuration / parameter changes
      - Significant impact to the process/production
      - Major customer aggravation.
      - Restart processes are often not simple

CIP Safety Output Connection

- Real time control of field device
  - Today primarily discrete functions, but Analog devices are supported
  - Not really intended to be used for device parameters, but does provide a functional path for this use.
    - However
      - Output assembly size would grow significantly
      - Potentially large impact to bandwidth
      - Negative impact due to CIP Safety processing at controller and at device
      - Parameter data sent at scan interval
        - » Even though parameter data is rarely changed, and for some applications may never change.

CIP Safety Enhancement

- Enhancement proposal
  - Allow parameters, defined by a devices profile to be changed during runtime
  - Existing CIP Safety connection information would be used between the safety controller and the safety device
  - SIL 3 capable message transport mechanism to be created
  - Rules would be defined for when message can be accepted
    - Device safety core operational (no faults)
    - CIP Safety connection established and operating
    - Parameters that can be changed are defined by safety device vendor (device profile)
      - Restrict what can be changed.
    - No active safety demands

Consider – This type of capability is needed for Process Safety Applications. Where uptime is critical and parameter changes must be made while operating with integrity.

ODVA 2017
Industry Conference
and 18th Annual Meeting

THANK YOU