

LISTEN.
THINK.
SOLVE.®

Lab 13 - Advanced Safety Techniques for Logix Controllers

Bill Waltz
Rockwell Automation
Mayfield Heights, Ohio

Get familiar with the demo case

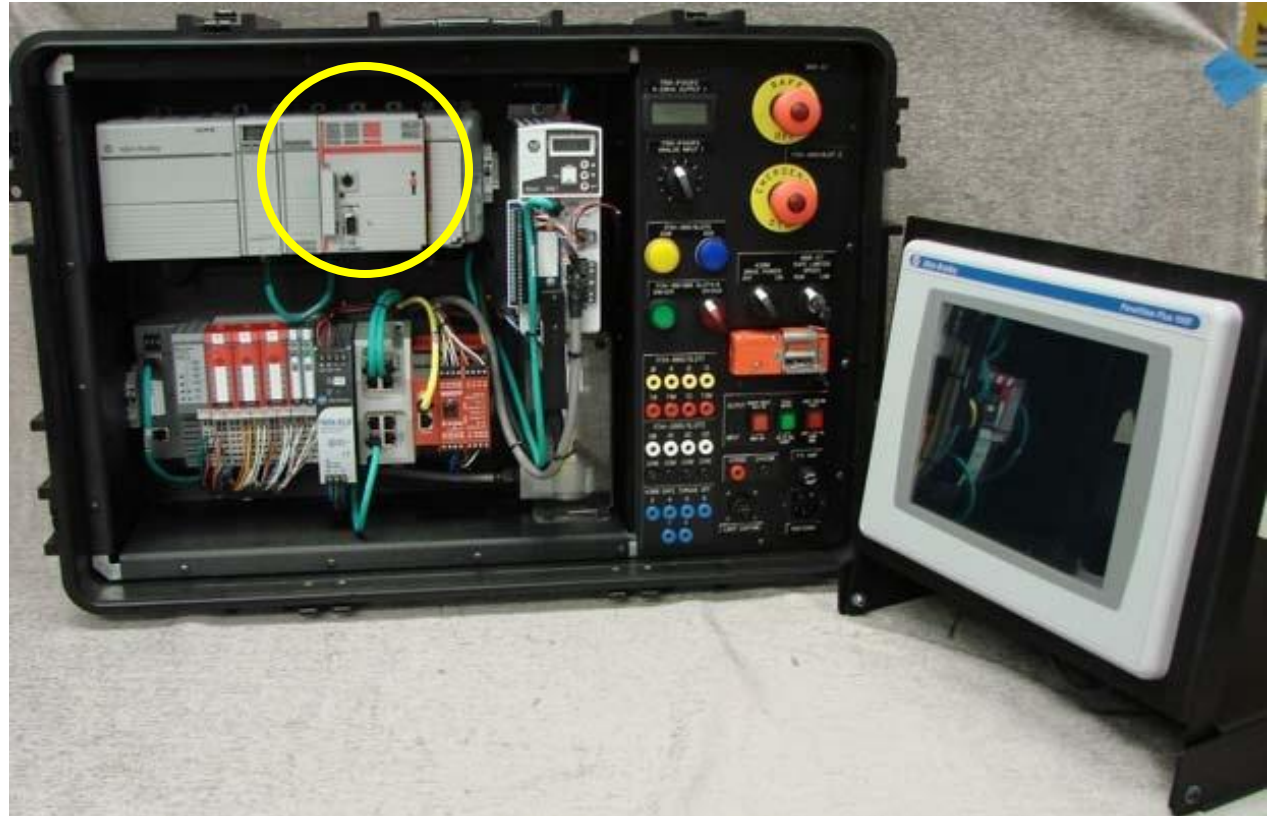


Safety Controller

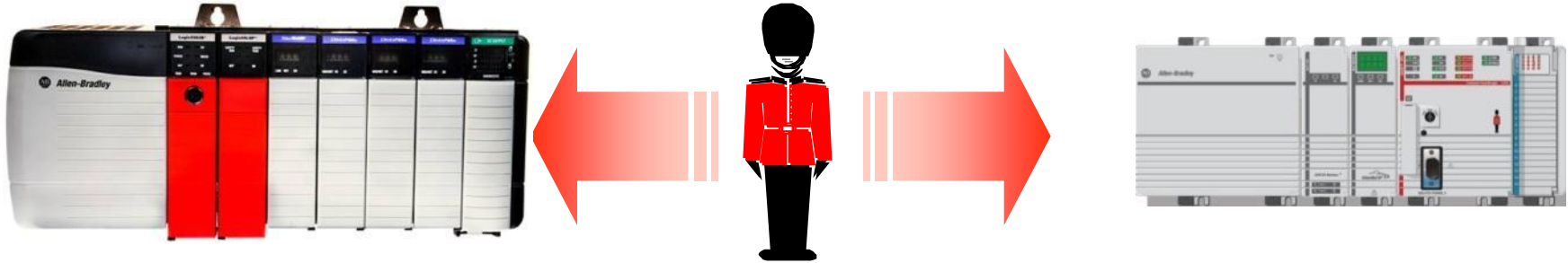
CompactGuardLogix
1768-L43S

Integrated Safety Controller

- Safety
- Standard
- Motion
- Integrated Architecture



GuardLogix® Safety Integration



- **Logix Integrated Safety**

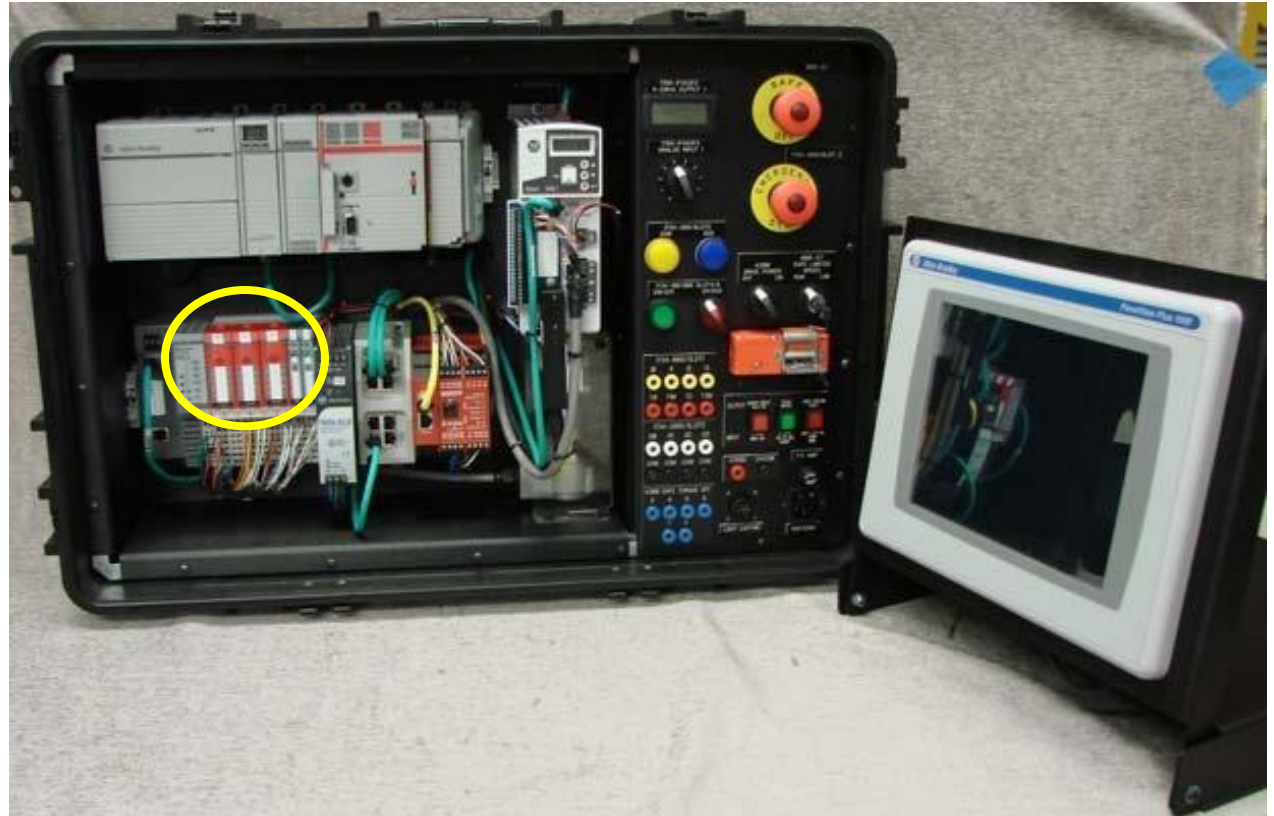
- Dual Processor Solution (1002 Architecture)
 - 1002 is recognized as the best safety architecture
- SIL-3 Certification per IEC 61508
- ISO 13849 Performance Level e (Category 4)
- Programs with RSLogix™ 5000
 - Extensive suite of certified safety application instructions
 - Simplifies design, validation, maintenance
 - Dual Channel suite
 - Muting & Press Suite
- CIP Safety comms for safety rated interlocking or safety I/O on Ethernet



POINT Guard I/O™

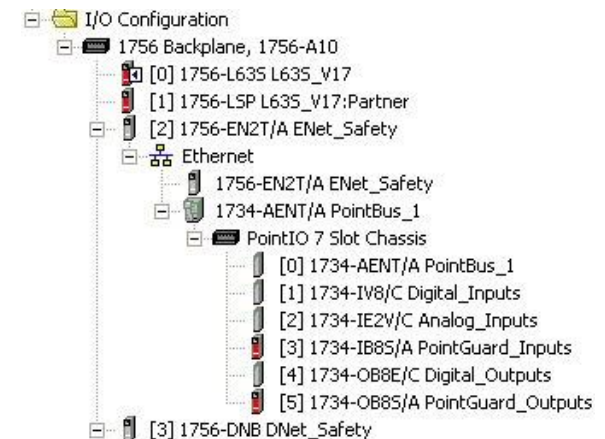
POINT Guard Safety I/O

- 1734-IB8S
- 1734-OB8S



POINT Guard I/O Integrated Safety I/O platform

- Mix & match safe and standard I/O in Point I/O
- SIL3 / PL e / Cat.4, TÜV certified
- POINT Guard I/O
 - 1734-IB8S – 8 Safety Inputs (4 dual)
 - 1734-OB8S – 8 Safety Outputs (1A ea – 4 dual)
 - 1734-IE4S – 4 SIL 3 Analog Inputs (introduced today)
- Connects on EtherNet/IP to GuardLogix & CompactGuardLogix
 - Single Port EtherNet Adapter (1734-AENT)
 - Dual Port EtherNet Adapter (1734-AENTR), supporting Ring & Line topology
 - Wireless EtherNet Adapter by ProSoft Technology



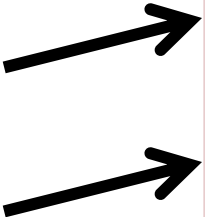

POINT Guard I/O provides for a highly flexible, safe, and standard I/O platform

MSR57

MSR57 Speed Monitoring Relay



MSR57 Functionality

| Safe Speed | GuardLocking |
|---|---|
|  <ul style="list-style-type: none"><li data-bbox="434 539 763 578">Safe Limited Speed<li data-bbox="434 606 821 645">Zero Speed Monitoring<li data-bbox="434 674 801 712">Safe Maximum Speed<li data-bbox="434 741 865 779">Safe Direction Monitoring<li data-bbox="434 808 730 846">Safe Acceleration |  <ul style="list-style-type: none"><li data-bbox="917 539 1356 631">Safe Control & Monitoring of Door Locking Device<li data-bbox="917 659 1278 698">Safe Door Monitoring<li data-bbox="917 726 1193 818">Enabling Switch Monitoring |

Kinetix[®] 300

Kinetix 300
Indexing Servo Drive

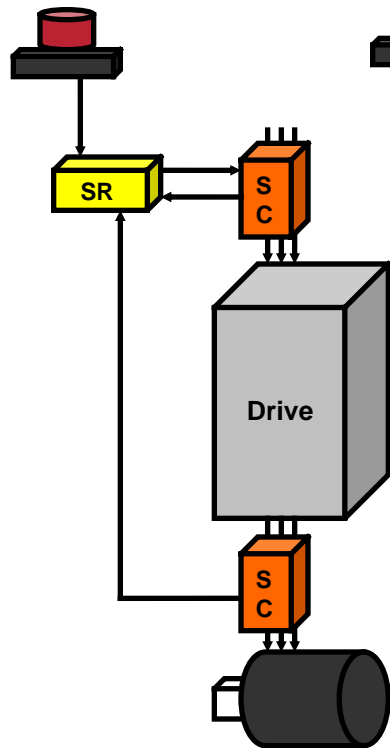
Safe Torque OFF



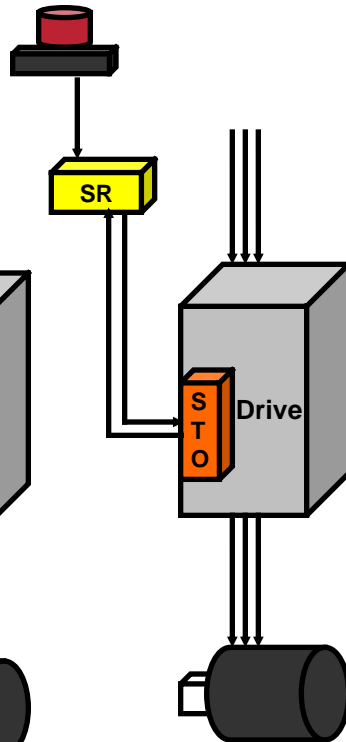
Safe Torque OFF

Basic Solutions

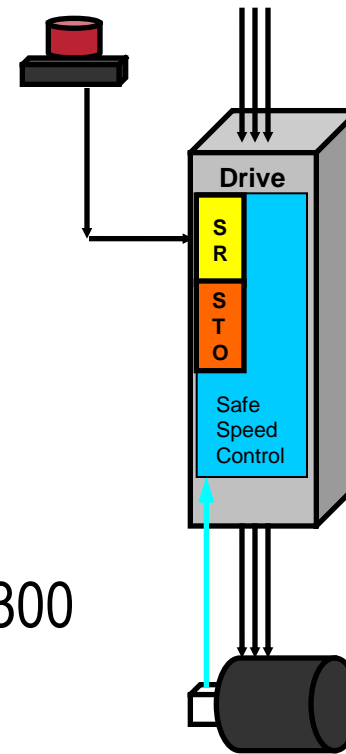
Non-Integrated
“Safe Torque Off”



Integrated
“Safe Torque Off”



Enhanced Solutions



Kinetix 300

SR = Safety Relay
SC = Safety Contactor
STO = Safe Torque Off

“Safe Torque Off” (basic safety) means that the drive will not cause the motor to rotate (IGBT firing circuits are guaranteed off)

Topics

1. MSR57

2. Certified Safety Instructions

3. Falling Edge Manual Reset

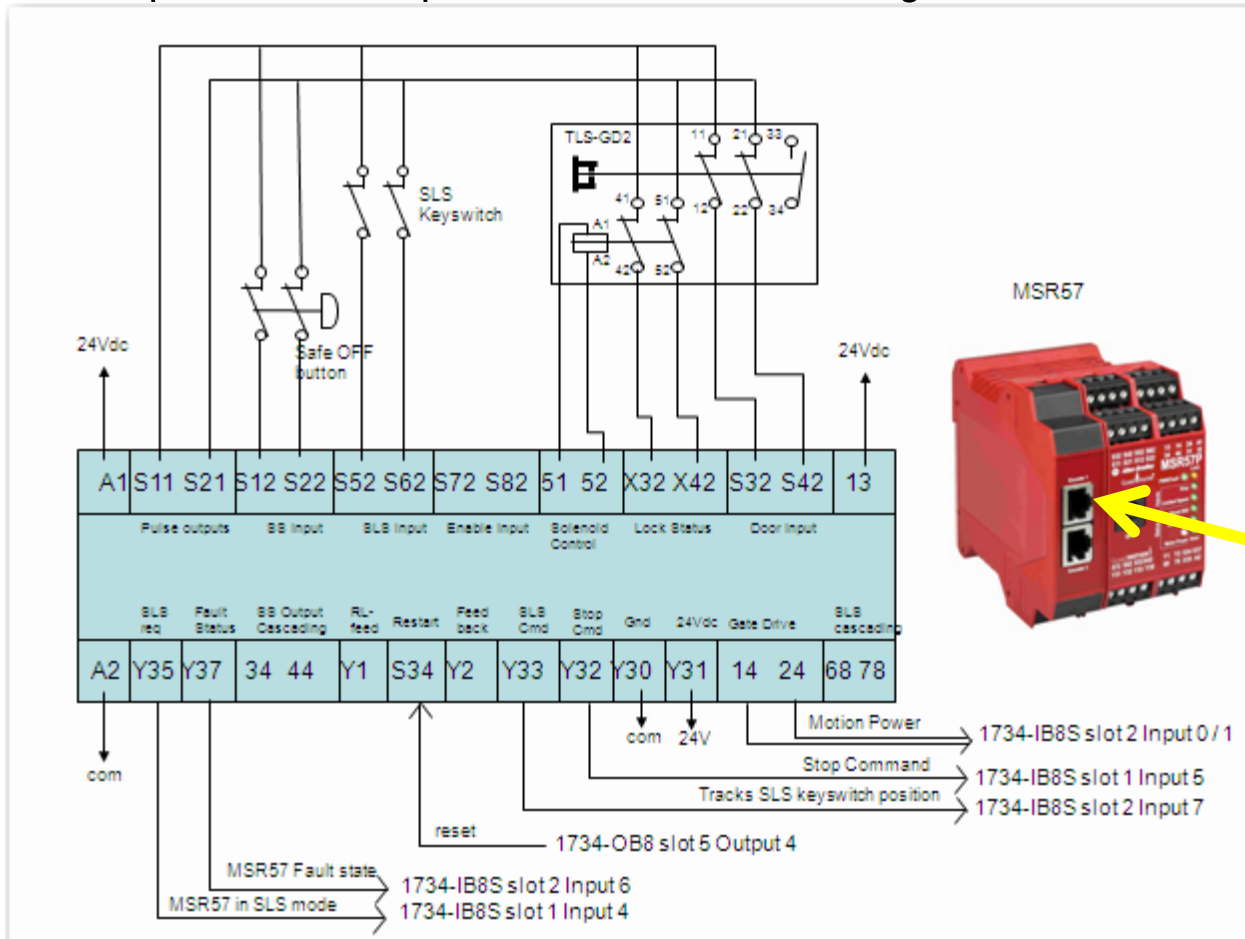
4. Safety Add-On Instructions (AOIs)

5. CIP Safety

MSR57 Wiring in CMSS demo case

- Motor speed is controlled by potentiometer labeled Analog Input 1
 - MSR57 does not control speed, it monitors speed
 - If SLS is requested, and speed is below limit, then gate can be unlocked

CMSS Case
MSR57 wiring



Encoder

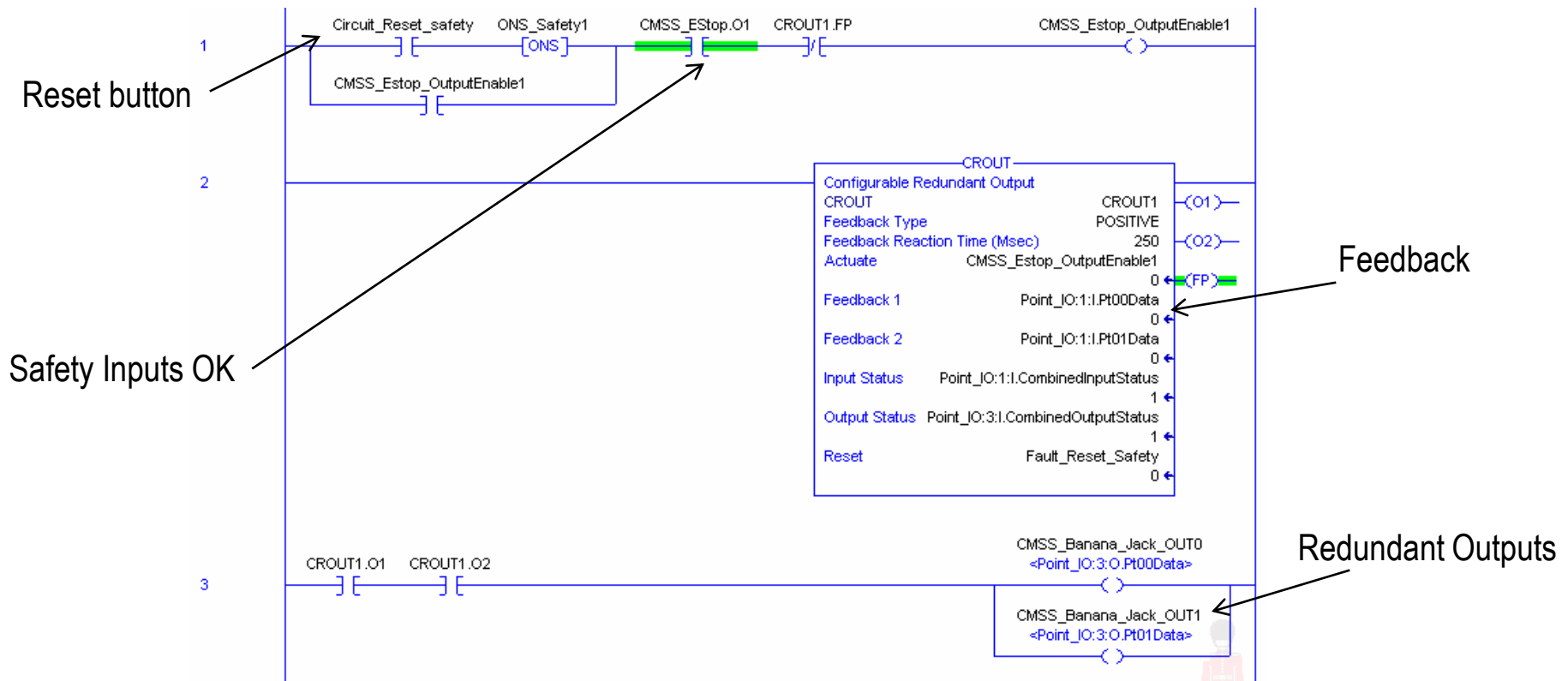
MSR57 summary

- Safe Limited Speed provides both safety and productivity
 - When stopping is an issue, personnel no longer have to decide whether to put themselves into harm's way to do their tasks
- Safe Maximum speed is typically used for machinery protection
- MSR57 Stop Categories
 - Torque OFF is the equivalent of Stop Category 0
 - Stop Category 1 and 2 are also available

Options: 0 = Safe Torque Off with Standstill Checking
(Torque Off)
1 = Safe Stop 1
2 = Safe Stop 2
3 = Safe Torque Off without Standstill Checking
(Trq Off NoChk)

Certified Safety Instructions - Summary

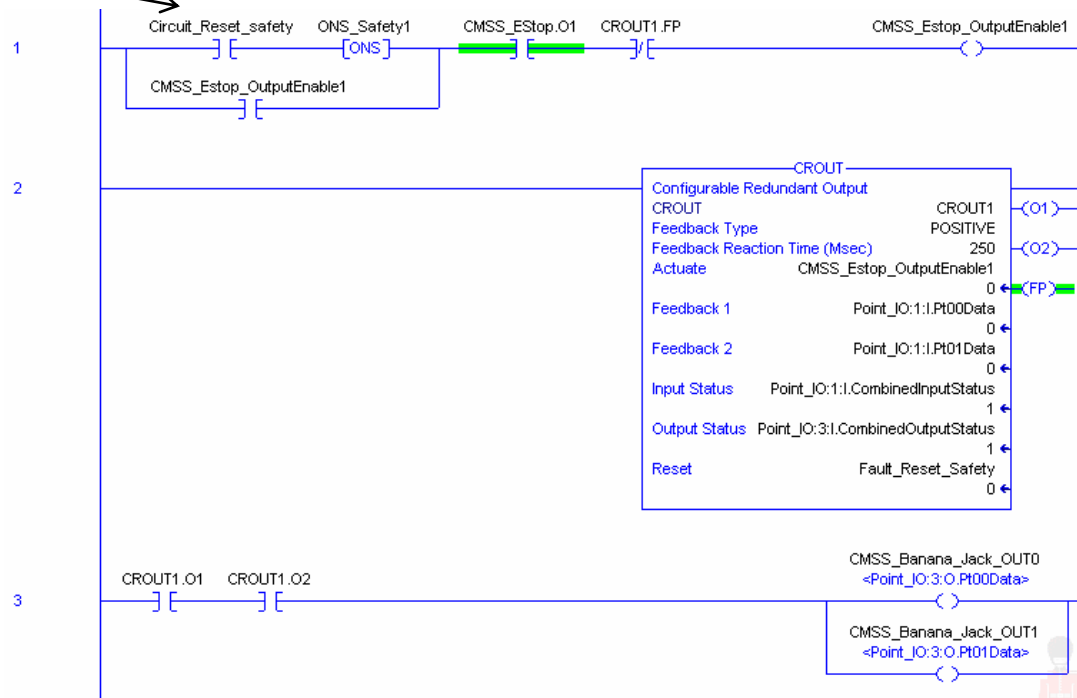
- Only one safety output instruction: CROUT (Configurable Redundant Output)
 - Mimics a safety relay
 - Controls output(s) and uses feedback to monitor whether output(s) operated properly



Manual Reset

- One of the basic safety principles is that a safety output cannot restart automatically
- This is very easy to accomplish using a safety PLC

Reset button



Manual Reset - Summary

- Manual reset shall not diminish rating of relevant safety function

Manual Reset - Summary

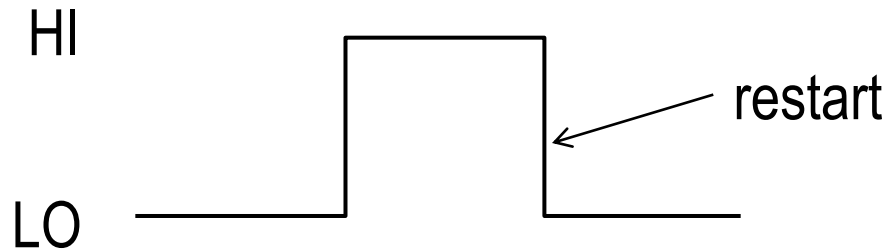
- Manual reset shall not diminish rating of relevant safety function
- How is this accomplished with traditional single channel reset?

Manual Reset - Summary

- Manual reset shall not diminish rating of relevant safety function
- How is this accomplished with traditional single channel reset?
 - If reset does not operate properly, machine simply does not restart (safe)
 - Make sure a single fault does not cause unexpected restart

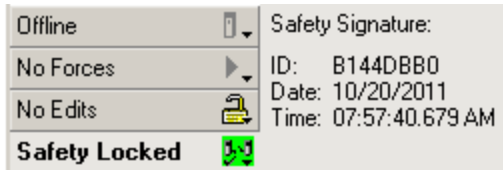
Manual Reset - Summary

- Manual reset shall not diminish rating of relevant safety function
- How is this accomplished with traditional single channel reset?
 - If reset does not operate properly, machine simply does not restart (safe)
 - Make sure a single fault does not cause unexpected restart
 - This is accomplished using HI to LO transition



Add On Instructions

- GuardLogix introduced the concept of a Safety Signature
 - If the signature has not changed, the safety code has not changed
 - If the signature is different, the safety code may have been changed



- The same concept has been applied to AOIs; both standard and safety AOIs
 - It is called a Signature ID for AOIs
- RSLogix 5000 downloads are not 'safety' rated
 - Safety tasks have to be verified, because there is no way to know what memory should be like after the download
 - Instruction memory is known
 - Safety Signature ID is the binary CRC within memory of a safety AOI
 - If Safety Signature ID is correct, the safety AOI downloaded properly

Add On Instructions - Summary

- Do YOU have to be certified to write safety application code?

Add On Instructions - Summary

- Do YOU have to be certified to write safety application code? NO

Add On Instructions - Summary

- Do YOU have to be certified to write safety application code? NO
- Does your safety application code have to be 'certified' ?

Add On Instructions - Summary

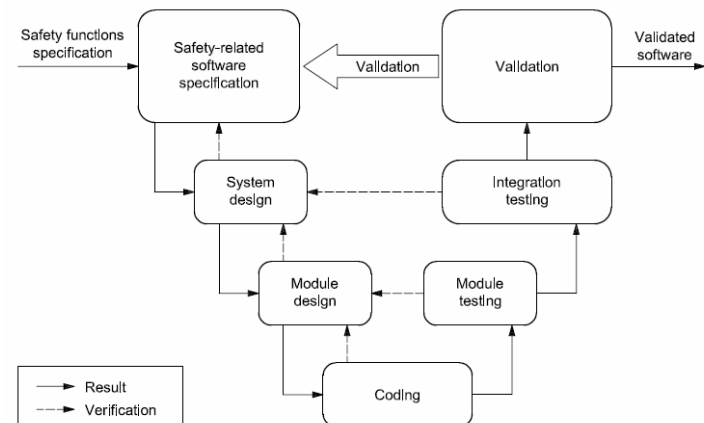
- Do YOU have to be certified to write safety application code? NO
- Does your safety application code have to be 'certified' ? not certified

Add On Instructions - Summary

- Do YOU have to be certified to write safety application code? NO
- Does your safety application code have to be 'certified' ? not certified
 - Your application code must be 'validated', but you can do that yourself
 - If you wish to have your code certified by a third party, they will spend much more time checking your software processes than checking your code.

Add On Instructions - Summary

- Do YOU have to be certified to write safety application code? NO
- Does your safety application code have to be 'certified' ? not certified
 - Your application code must be 'validated', but you can do that yourself
 - If you wish to have your code certified by a third party, they will spend much more time checking your software processes than checking your code.
 - Documented developmental lifecycle according to V-model
 - example: Do you have a SRASW (safety related application software) specification ?
 - Modular and Structured Programming
 - Code shall be readable, understandable, and testable
 -



CIP Safety

Safety Controller

1768-ENBT

Ethernet Cable

Ethernet Switch

1734-AENT

PointGuard

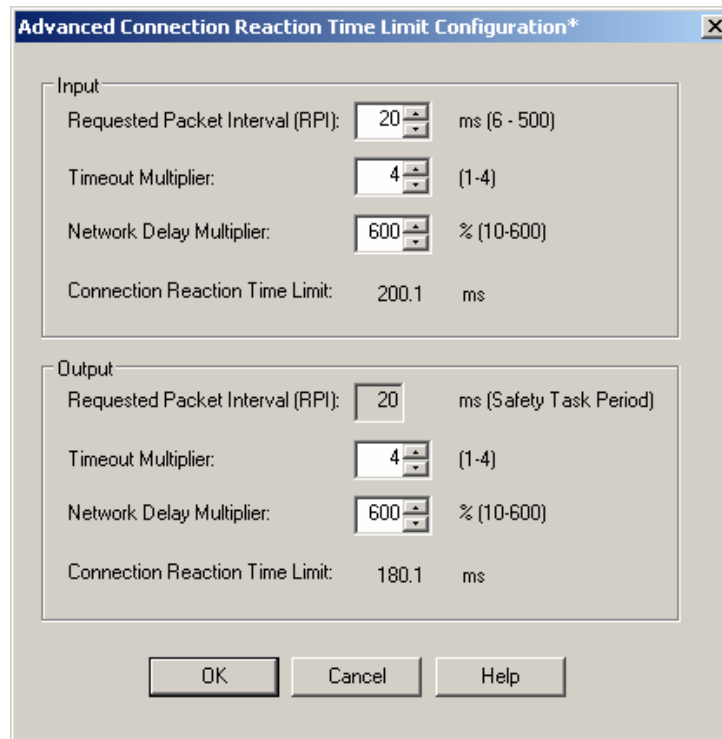


- What makes CIP Safety protocol safe?

- Data sent twice in packet frame (one is inverted)
- Separate CRCs for each piece of data (one is inverted)
- Every packet is timestamped (allowable age of data user configurable by CRTL)

CIP Safety- Summary

- Safety connection loss due to network bandwidth?
 - Increasing CRTL TEMPORARILY to maximum is a good troubleshooting technique
 - If connection loss persists with maximum CRTLs, then issue is likely not bandwidth



LISTEN.
THINK.
SOLVE.®

Questions?