Elements of a "Fail-to Safe", Control Reliable Inspection System (CRIS) Methodology

For Machine Vision and Barcode Verification Systems

The Key element in the "Fail to Safe" methodology is that the inspection system to assumes that the "Mismatch or Fail" condition is present at the start of each machine cycle. This will initiate the Fail-to-Safe shutdown process on each trigger, unless an overriding positive Match/Pass confirmation signal comes from the inspection device.

Only an authorized and identified operator (RFID Badge) may teach-in, or select from a recipe screen, a new barcode or product to load into the inspection system for a product change. The newly taught or selected code is set into the "Positive Match/Pass" register in the inspection system.

An inspection device communication heartbeat is required to confirm an active communication loop between the inspection device and PLC.

Dual trigger eyes with complimentary outputs should be used. The output from the first eye directly triggers the camera, and the other with inverse logic runs to the PLC. The second eye runs a complimentary signal back to the PLC to back-check the function of the trigger system. This allows for immediate trigger eye failure detection.

The machine cycle process is as follows:

- Product to be inspected triggers both photo eyes, one signal goes high to trigger the inspection device and one signal goes low to the PLC to monitor trigger eye health. The second eye allows for matching trigger count detection should one of the eyes get blocked or misaligned.
- The inspection system triggers and inspects the product. If a barcode is read, it compares it to the match code register "Positive Match Code" If it is image based or OCR the information is compared against a preset "Pass" image.
- Trigger eye signal goes low signaling "End of Inspection Cycle" to camera AND to the PLC.
- If the PLC sees the data from the inspection device and it matches the data in the "Match Code" register, the barcode is confirmed to be a good match and the machine can continue running its process. This also applies to OCR and image compare the camera must see a "Pass" to continue running.
- If the PLC sees "No Match or Fail" data from the inspection device, the barcode is either unreadable or not present and the carton reject signal from the CRIS system is fired. The reject of the carton off the production line MUST be confirmed by a reject confirmation eye tied back into the Control Reliable Inspection System or the production line will immediately be shut down to prevent the unidentified product from exiting the inspection zone. If this "No Match" sequence happens three consecutive times, the machine is shut down.
- If the PLC sees both Trigger Eye Inputs only and no data from the inspection device, the barcode is a "Mismatch" and the machine is immediately shut down. This immediate shutdown would also occur if the camera itself failed or the wiring from the scanner to the PLC became compromised.

763-972-1051 • **888-920-0939** • fax 763-972-1041
507 Kelsey St. • Delano, MN 55328 • www.sensorsintegration.com

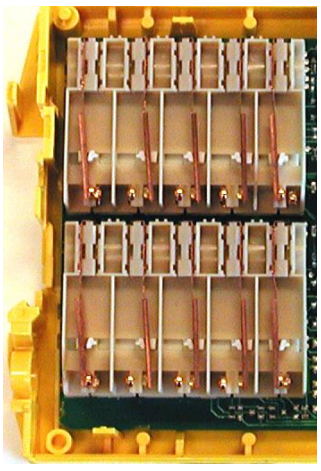
Use of the Safety Relay: For a "Fail to Safe" system, a controlled shutdown command is issued from the PLC to perform a normal controlled stop. As with most safety systems, an E-Stop circuit is run parallel to the controlled shutdown signal. The E-stop relay is fired ONLY after a predetermined time period expires; this time period allows the machine to perform a normal shutdown before opening the E-Stop contacts. The E-Stop circuit runs through a safety relay that allows redundant positively driven contacts to perform the guaranteed machine shutdown function in the event that the controlled shutdown relay contacts weld or any number of other machine stop errors occur. The use of a Certified Safety Relay allows back checking of the safety shutdown circuit back to the PLC. This Fail-to-Safe methodology will detect any single component failure in the shutdown circuit, while still providing a guaranteed safe stop of the machine.

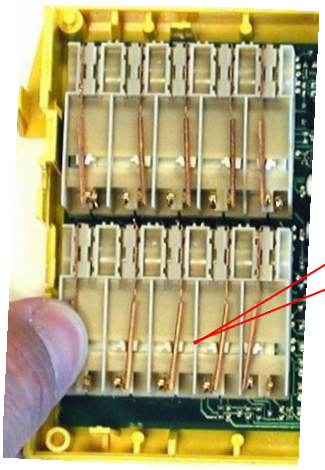
Using the Fail-to-Safe Methodology, we have verified:

- Secure product teach-in, or product recipe selection, by authorized identified personnel only via RFID Badge
- All events, including product changeovers and any component failures, are Time and Date stamped and are available for real time viewing via the onboard Ethernet connection.
- Confirmed a correct matching Barcode or product Pass for each product allowed to pass the inspection point.
- Incorrect product (Good read but mismatch code) with immediate shutdown
- No Read / Unreadable code or Fail product has been confirmed rejected from the production line

A "Fail to Safe" Control Reliable Inspection System (CRIS) system MUST detect within one cycle:

- Failed, unplugged, trigger eye within a single product inspection cycle
- Failed camera with immediate shutdown after one inspection cycle
- Failure to reject bad product from the line must result in immediate line stop
- Failure of one of the two sets of contacts on the Safety Shutdown Relay while still guaranteeing a safe machine shutdown AND the prevention of further machine running until the safety relay is replaced.





Safety Shutdown Relay; Notice the contacts are all linked with a plastic connection bar to be "Positively Driven Contacts"

763-972-1051 • **888-920-0939** • fax 763-972-1041
507 Kelsey St. • Delano, MN 55328 • www.sensorsintegration.com

Testing procedures to determine if an inspection system meets "Fail-To-Safe" criteria for a Control Reliable Inspection System (CRIS)

1) With the system powered but no product passing, Disconnect the inspection device, (scanner or camera) from the system. Within a short time, the lack of Heartbeat signal must be detected, and the system must shut down and not allow a restart until communications with the inspection device can be confirmed. The Human Machine Interface (HMI) display screen must display the detected failure and advise corrective action. (the detection time is configurable, but Default is 30 seconds in a non-triggered state)
2) With products passing the trigger, Disconnect the inspection device, (scanner or camera) from the system. Upon the next product to trigger the system, the system must detect the faulted Inspection device and the system must shut down immediately and not allow a restart until communications with the inspection device can be confirmed. The Human Machine Interface (HMI) display screen must display the detected failure and advise corrective action.
3) Disconnect one of the trigger eyes. The trigger fault must be detected immediately to prevent uninspected products from passing the inspection point. This fault must shut the system down immediately. The HMI must display the detected failure and advise corrective action.
4) Misalign or block the primary trigger eye so that it cannot see the reflector. The trigger fault must be detected within a single product inspection cycles. This fault must shut the system down. The HMI must display the detected failure and advise corrective action.
5) Run a product with no Barcode or Fail product past the camera/scanner with the reject mechanism disabled. The CRIS must detect that the product had not been rejected from the line and must shut the production line down to prevent the product from escaping downstream. The HMI must display the detected failure and advise corrective action.
6) Run a product with the incorrect barcode past the camera/scanner. The CRIS must immediately shut down as the product exits the scanning area. The system must not allow restart until the critical fault of the incorrect carton has been acknowledged and reset by a higher-level key than operator.
7) Jumper the back-checking contact of the safety relay closed (If an inspection system being evaluated has no safety relay, then jumper the machine run contact closed) and test if the system can detect the failure of the contact opening on the next request for machine startup. The machine MUST still perform a stop and not allow the machine to be restarted until a new safety relay is in place. Therefore, we use a redundant contact safety relay. The HMI must display the detected failure and advise corrective action.

763-972-1051 • **888-920-0939** • fax 763-972-1041
507 Kelsey St. • Delano, MN 55328 • www.sensorsintegration.com