Precluding Multiple Spurious Commands from Video Display Units

Why Is This Important

- The safety analysis is based on credible single failures
- If multiple spurious commands cannot be precluded the safety analysis will become unbounded
  - For VDUs controlling only multiple non-safety systems we would need to expand the Anticipated Operational Occurrences
    - Today we analyze only one abnormal control system event at any one time. Multiple spurious commands could result in an unlimited combination of abnormal control system failures.
  - This problem is compounded for multi-channel VDUs
    - Multiple spurious commands could lead to an unlimited combination of safety system failures combined with an unlimited combination of control system failures.
  - This problem is reduced, but not eliminated if we employ only multi-channel SR VDUs
    - Today we analyze spurious actuations in only single trains

Credible VDU Failures

- A spurious control command is a control signal, such as open/close or start/stop, erroneously generated from a VDU with soft controls
- Continuous generation of a single valid spurious control command is credible
  - There are various mitigation strategies, eg.
    - Signal is ignored in controller because two distinct commands are required (enable/action, action/confirm)
    - Once manually detected the failure can be mitigated by disabling the erroneous signal (eg. from the Safety VDU)
      - May affect a single safety or non-safety component, which is bounded by the safety analysis
  - A failure resulting in multiple spurious control commands can be shown to be not credible, based on key design features of the sending and receiving processors

Generating Control Commands

- A control command data set consists of multiple data components, such as
  - VDU tag identification from which the command is originating (e.g. Operational VDU number)
  - plant component tag identification for the component being controlled (e.g. valve number)
  - operation type being commanded (e.g. analog command or on/off command)
  - operational signal (e.g. start, stop, increase, decrease, digital setpoint value or manual demand value)

Generating Control Commands

- The VDU processor assembles these data set components uniquely for each control command, based on a series of operator pointing device actions
  1. Select a monitoring screen that contains an icon for the component to be controlled
  2. Select the icon for the component to be controlled which results in a control pop-up window
  3. Enable the control window by selecting an enable icon
  4. Request action (e.g., stop, start, open, close, new setpoint/demand) in the pop-up window

     or 3 and 4 reversed

  3. Request action in the pop-up window
  4. Confirm action in the pop-up window

Generating Control Commands

- After assembling any control command, the VDU processor adds one or more communication check values to allow the receiver to check the integrity of the complete message
- Common communication check values include
  - Check sum, CRC, hash function
  - Incremented sequence numbers such as “Alive Counters” added to each message in headers/footers

Receiving Control Commands

- The receiving controller independently calculates communication check values.
- Messages are rejected if
  - The calculated and transmitted communication check value are different.
  - The headers and footers are not correct
  - The sequence indicators are not correct.

Receiving Control Commands

- The receiving controller rejects messages that:
  - Do not contain all required data set components, including appropriate delimiters and data lengths
  - Contain unrecognized data set components, including erroneous or unexpected tags or command syntax

Credible VDU Failures

- For systems with these types of design features spurious actuation of multiple control commands would require multiple software block failures that each produce intelligent meaningful data
- Therefore a single failure resulting in multiple spurious control commands is not credible in a system with these types of features
- These features facilitate control of multiple systems - NSR, SR or NSR and SR - in multiple divisions, from the same VDU - SR or NSR
- These features must be maintained throughout the system life cycle