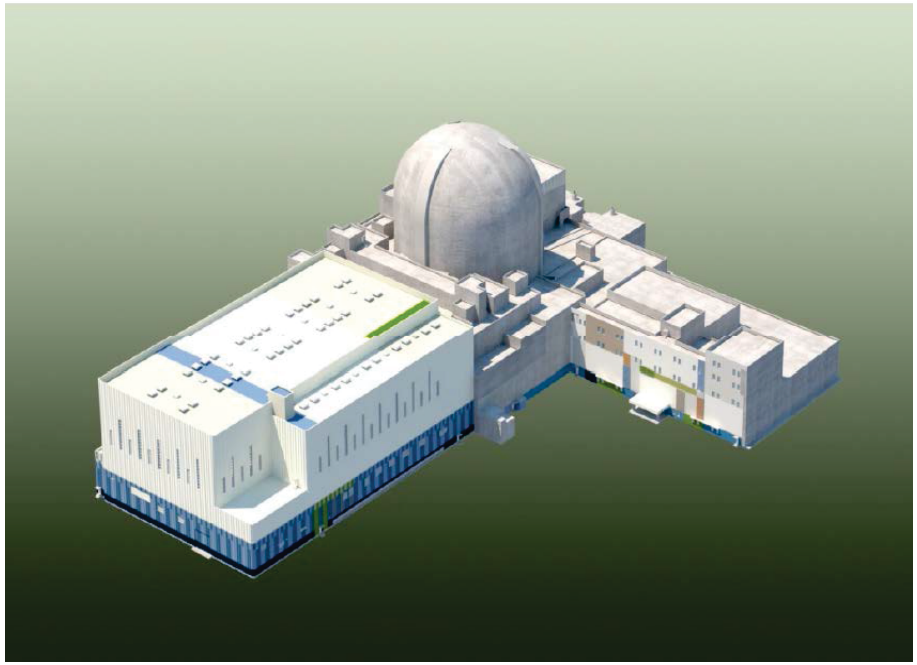
APR1400 Design Certification Review
I&C Topics



KEPCO/KHNP

August 12-13, 2015

Table of Contents

Q1 Prioritization of Control Signal (1/6)

- **NRC Question**

  How are the prioritization of control signals, latch, and reset functions implemented in the component control logic?

- **Response to NRC Question**
  - The priority of the signals from the PPS and HSI in the MCR is provided in the loop controller (LC) as follows:
    - ESFAS signals from the PPS has priority over the signals from component-level MI switches and the ESCM.
    - Signals from component-level MI switches and signals from the ESCM have the same priority.
  - In the CIM, the demands from the DPS and ESF-CCS LC have equal state-based priority.

Q1 Prioritization of Control Signal (2/6)

- **Response to NRC Question**

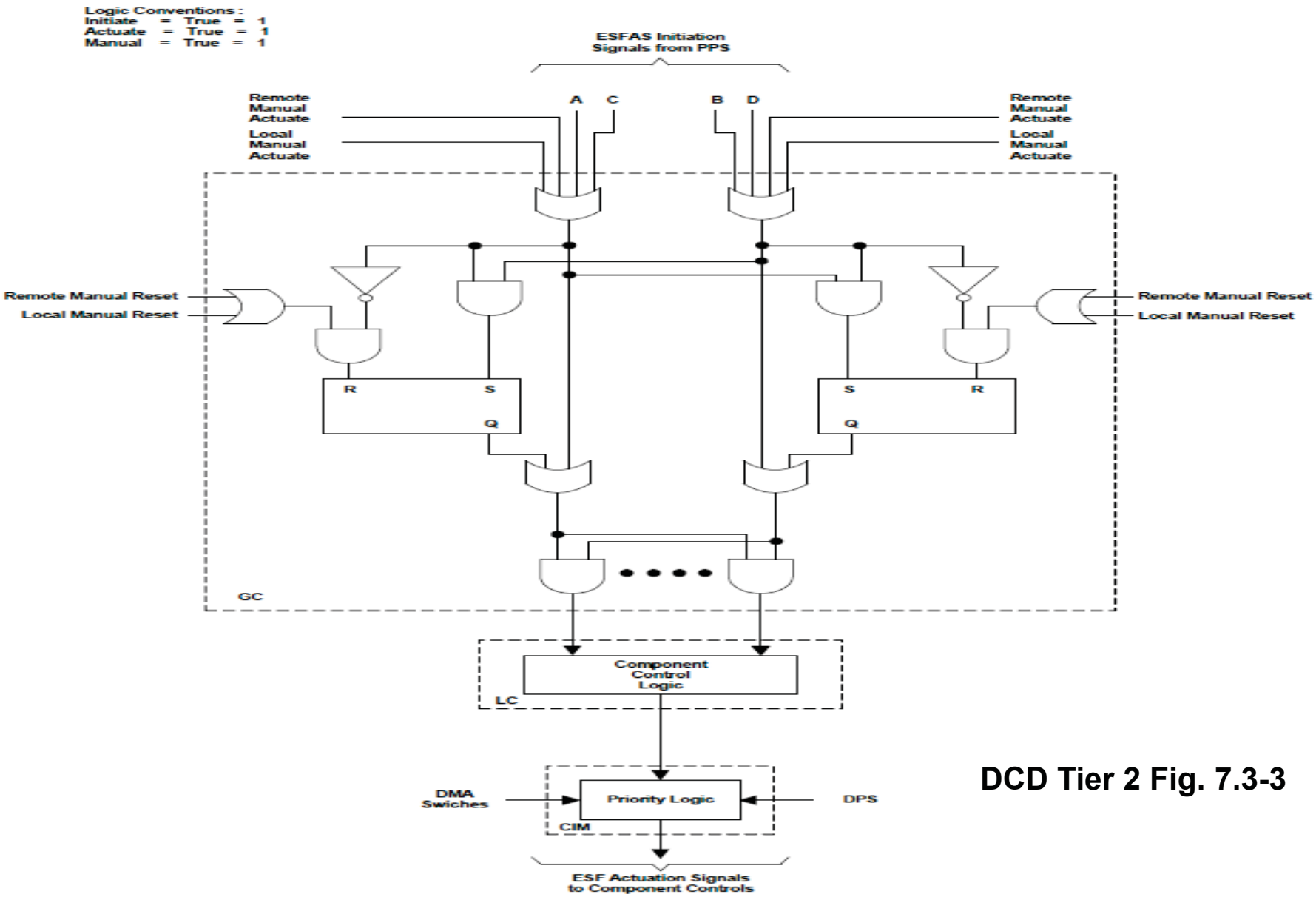
TS

Q1 Prioritization of Control Signal (3/6)

- **Response to NRC Question**
  - The reset and latch functions for the engineered safety features actuation system (ESFAS) signals are implemented in the group controller (GC) logic which generates system-level actuation as shown in DCD Tier 2 Figure 7.3-3.
  - The operation of the reset function and latch function is as follows:
    - The ESFAS is activated only when the ESF initiation signals from two or more PPS divisions are provided to the ESF-CCS.
    - Once an ESF actuation is activated, the ESF actuation output is latched and is not automatically reset even after the ESF initiation condition is cleared from the PPS divisions.
    - The ESF actuation output is manually reset after the ESF initiation condition is cleared.

Q1 Prioritization of Control Signal (4/6)

- **Response to NRC Question**



DCD Tier 2 Fig. 7.3-3

Q1 Prioritization of Control Signal (5/6)

- **Response to NRC Question**
  - At the component control logic in the LC, when an ESFAS to start (or stop) is present from the GC, the opposite control commands are blocked to avoid blocking or overriding a safety actuation.
  - In the component control logic, ESFAS safety command (ESF-1) cannot be overriden until it is manually reset after the ESF initiation condition is cleared.
  - ESFAS safety command (ESF-2) can be subsequently overriden by the operator. Once ESFAS signal is overriden, it is continuously blocked until it is reactivated.

Q1 Prioritization of Control Signal (6/6)

- **Response to NRC Question**

TS

Q2 Qualification of ESCM (1/1)

- **NRC Question**

  How are software and hardware qualifications addressed for the safety-related ESCM?

- **Response to NRC Question**
  - The software and hardware qualifications of the ESCM

Hardware	Display Computer with Touch Screen	Class 1E
	Network Card (SDL, Ethernet)	
	Fiber Optic Modem	
Software	Operating System	Important to Safety (ITS)
	Application Programs	

Q3 Voting Logic (1/5)

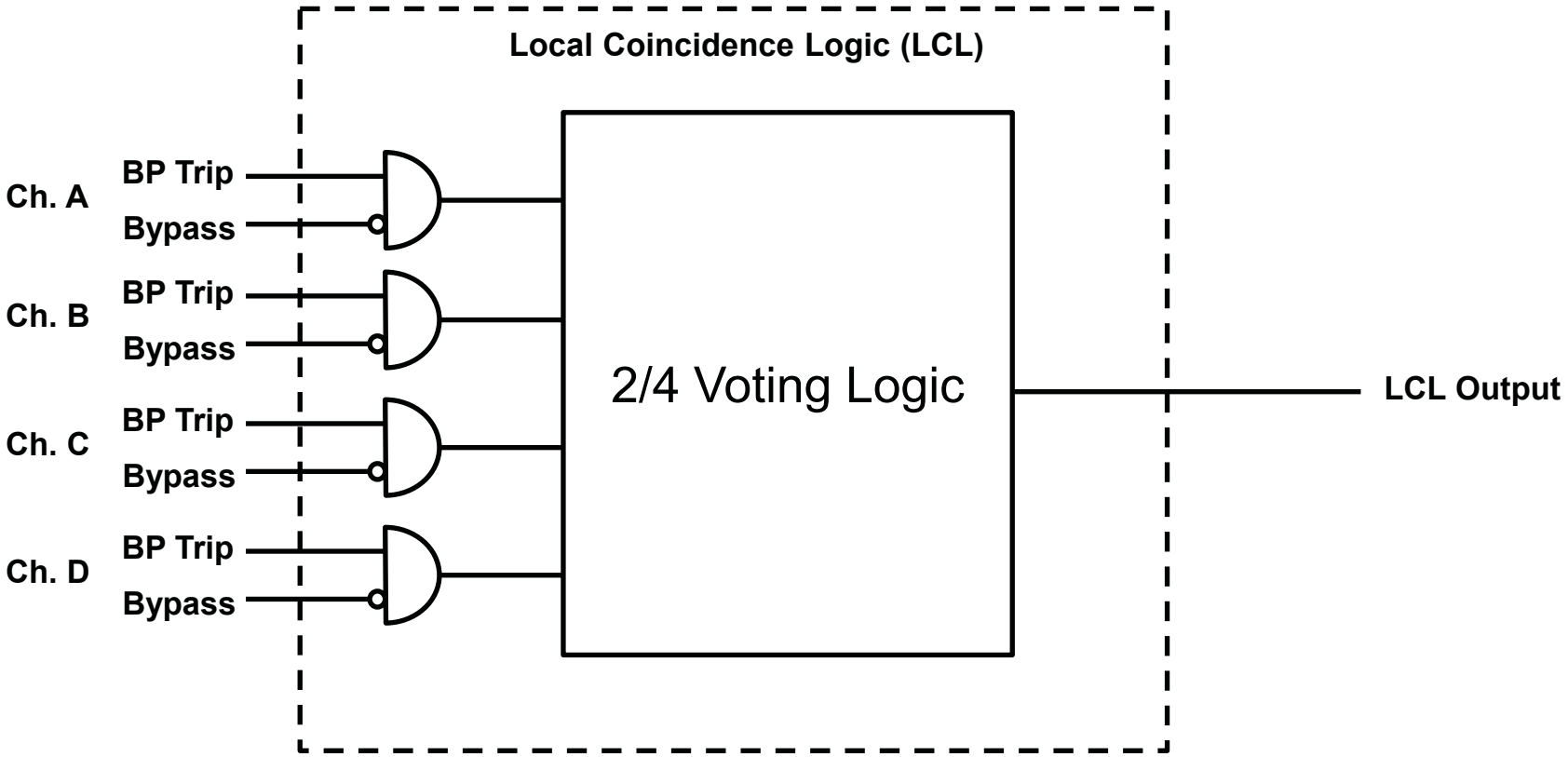
- **NRC Question**

  How are changes made to voting logic when one division fails and another one is in bypass mode?

- **Response to NRC Question**
  - Normal Operation: 4 channel redundancy (2-out-of-4 voting)
  - 1 Channel Bypass: 3 channel redundancy (2-out-of-3 voting)
    - The bypassed channel is excluded from the voting logic as shown in the simplified diagram on the next slide.
  - 1 Channel Bypass & 1 Channel Single Failure: 2 channel redundancy
    - Failure to trip : 1-out-of-2
    - Failure to untrip : 2-out-of-2

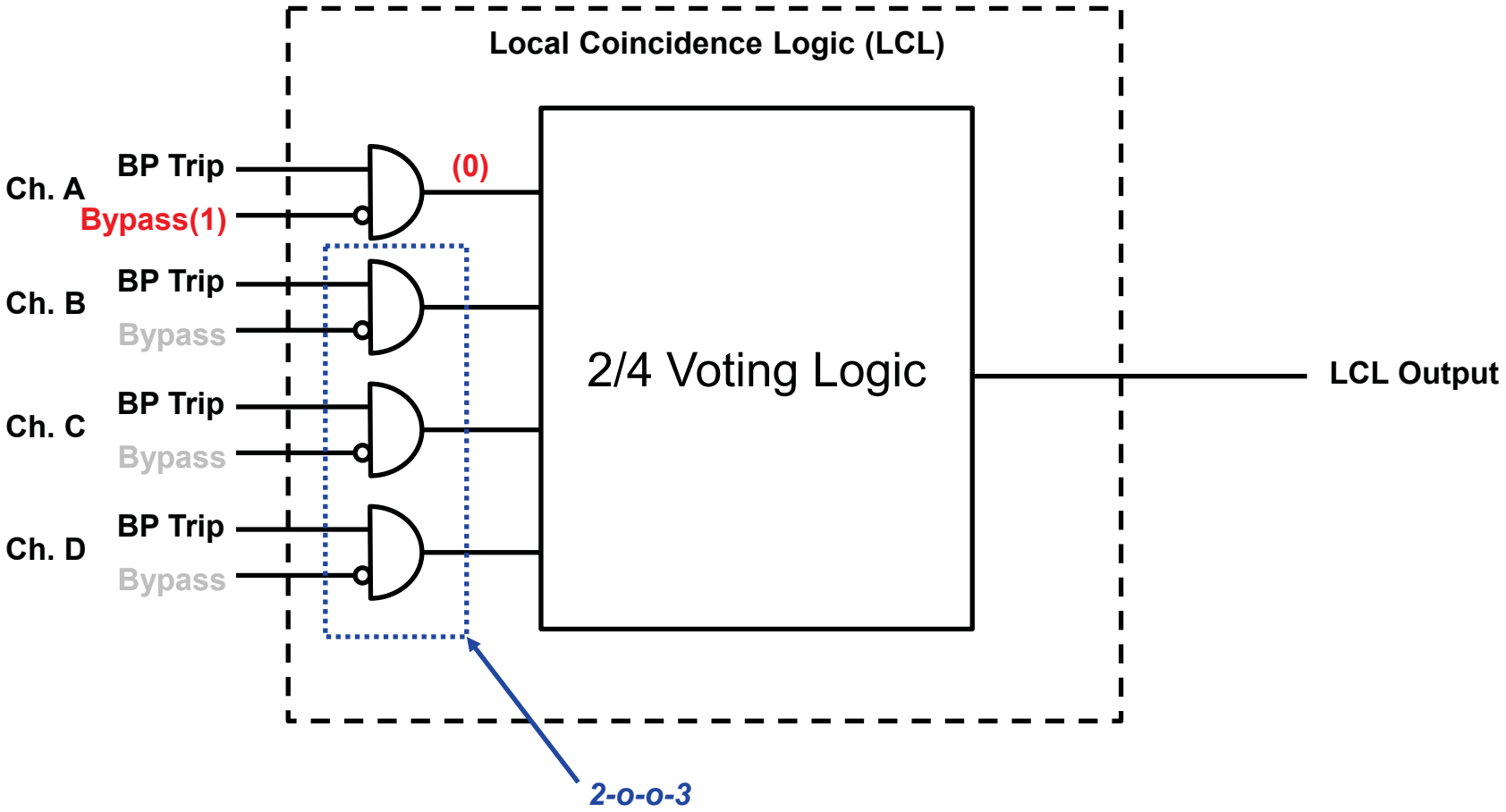
Q3 Voting Logic (2/5)

- **Response to NRC Question**
  - **Channel bypass and voting logic**



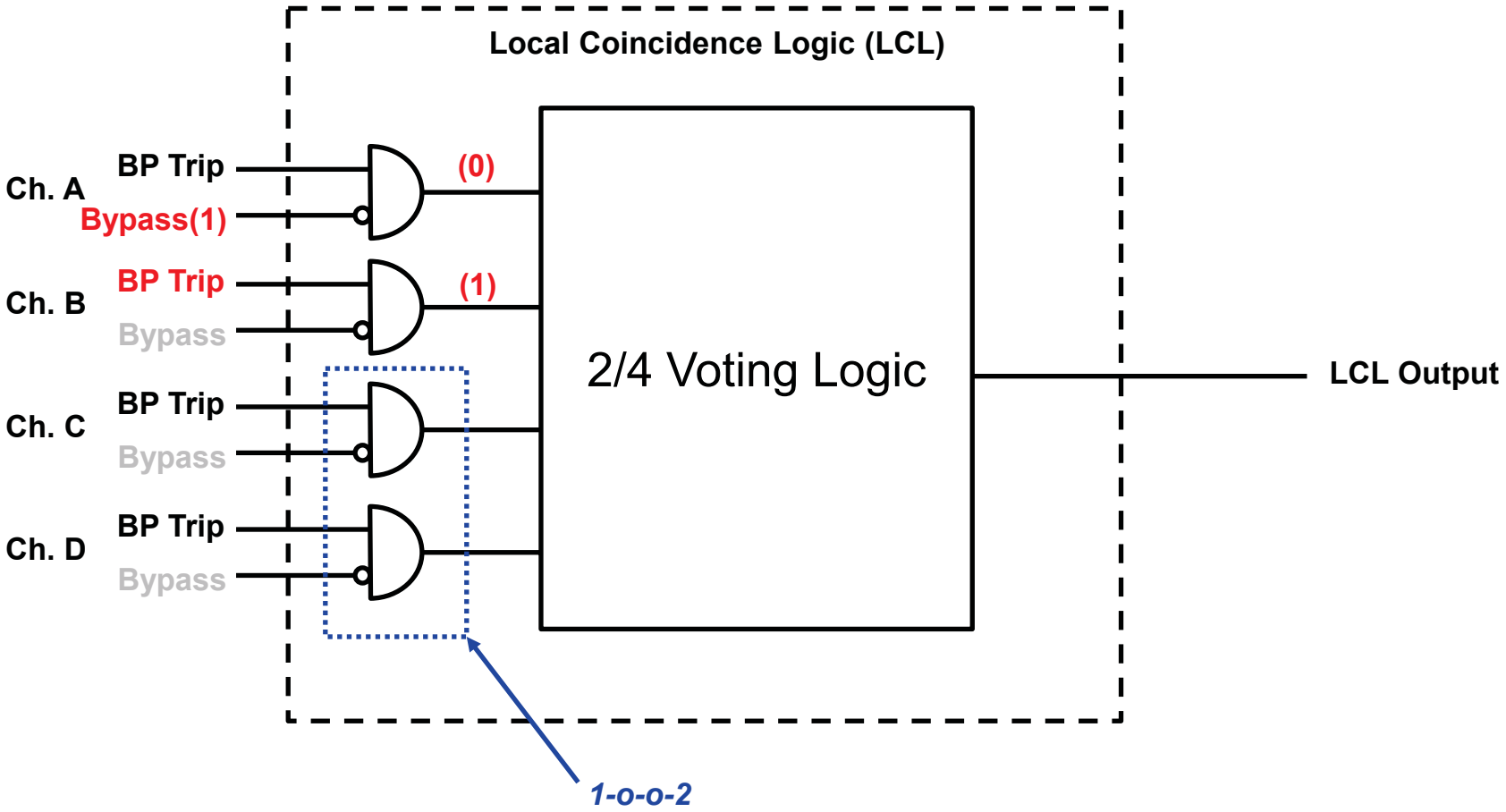
Q3 Voting Logic (3/5)

- **Response to NRC Question**
  - **One channel bypassed (e.g., Ch. A)**



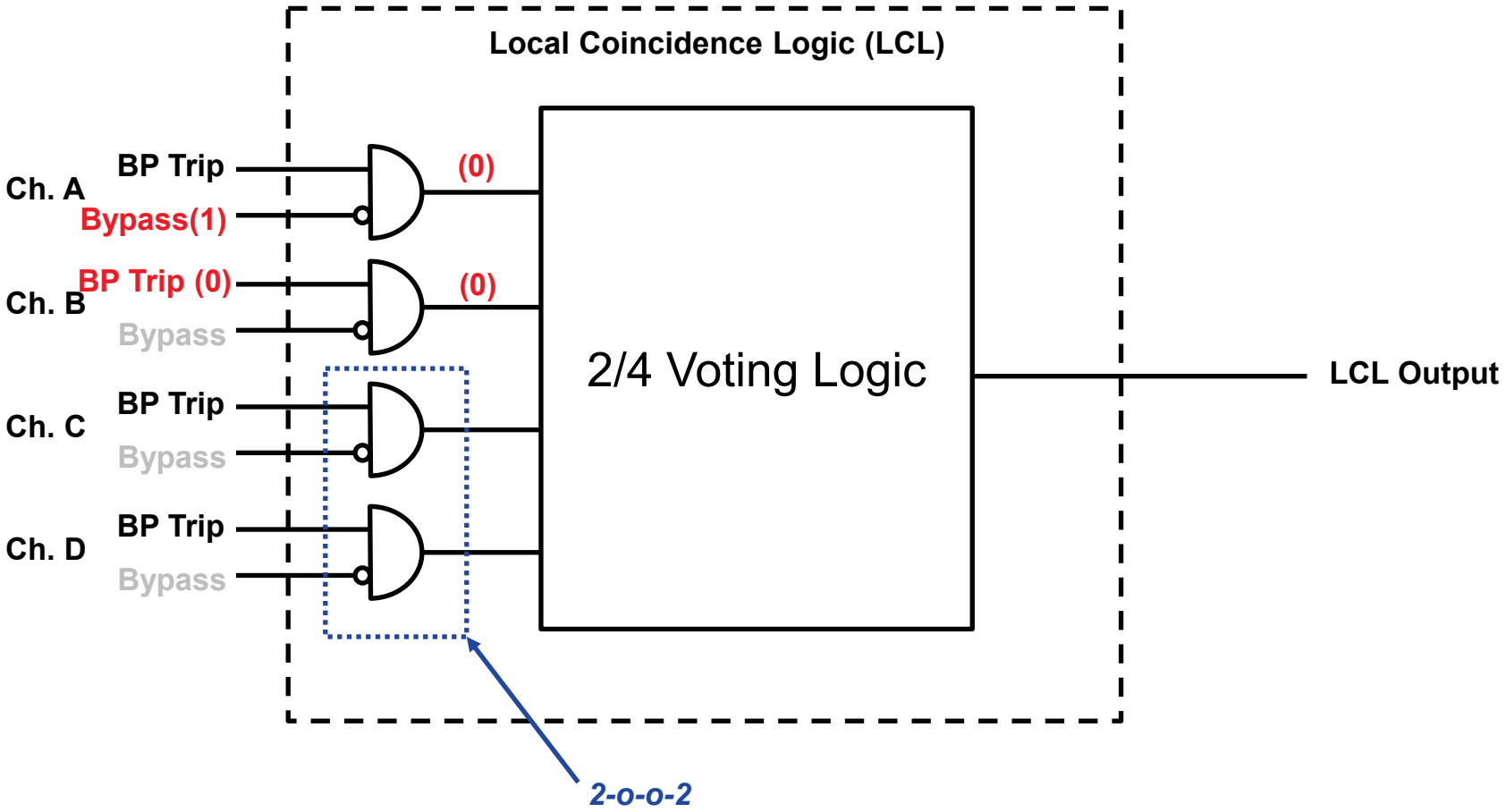
Q3 Voting Logic (4/5)

- **Response to NRC Question**
  - **One channel bypassed & one channel (e.g., Ch. B) failed to trip**



Q3 Voting Logic (5/5)

- **Response to NRC Question**
  - **One channel bypassed & one channel (e.g., Ch. B) failed to un-trip**



Q4 BOP ESFAS 1-out-of-2 Logic (1/3)

- **NRC Question**

  What are justifications or bases for the BOP ESF system which utilize 1 out of 2 logic?

- **Response to NRC Question**
  - DCD Tier 2, Section 7.3.2.1 describes the compliance of the 1-out-of-2 coincidence logic of the BOP ESFAS with the single failure criterion.
  - If the BOP ESFAS signals are produced by spurious actuation of BOP ESFAS, the supply and return air fan in air control unit are actuated. The actuating ESFAS signals do not adversely affect plant safety or reactor trip.
  - Because the BOP ESFAS initiation signals are performed by 1-out-of-2 logic taken twice, the 1-out-of-1 logic of the available division can be actuated by the remaining operating radiation monitor, even if:
    - ✓ one of two radiation monitors in the same channel is placed in bypass for testing and
    - ✓ single failure of the different channel belonging to other division occurs at the same time under the radiation release accident.

Q4 BOP ESFAS 1-out-of-2 Logic (2/3)

- **Response to NRC Question**

TS

Q4 BOP ESFAS 1-out-of-2 Logic (3/3)

- **Response to NRC Question**
  - **1-out-of-2 coincidence logic taken twice meets the minimum required logic function for the single failure criterion of IEEE 603 for BOP ESFAS by changing the logic from 1-out-of-2 to 1-out-of-1 in the channel bypassed.**

Q5 MI Switches (1/2)

- **NRC Question**

  Figure 7.3-1 in DCD Tier 2, Section 7.3 shows that both MI system-level and component level manual switches only. Figure 4-28 in the Safety I&C System Tech. Report also shows the MI switches only. Figure 7.1-1 in DCD Tier 2 shows both MI switches and ESF switches. Figure 4-13 in the Safety I&C System Tech. Report shows the MI switches, ESF switches, and local manual ESF switches. Clarify the differences among the figures for the same ESF control system and also what safety functions those manual switches will execute?

- **Response to NRC Question**
  - **Minimum inventory (MI) switches consist of component-level switches and system-level switches on the safety console.**
    - **System-level switches are manual ESFAS switches to initiate system-level ESFAS actuations (SIAS, MSIS, AFAS, CSAS, CIAS, CREVAS, CPIAS and FHEVAS).**
    - **Component-level switches provide the component manual control for safe shutdown by the MCR operators when the operator consoles are not available.**

Q5 MI Switches (2/2)

- **Response to NRC Question**
  - **Local manual ESF switches are system-level ESFAS switches which are located in the MTP cabinet in the I&C equipment room.**
  - **System-level MI switches and local manual ESF switches are provided for the same purpose to initiate system-level ESFAS actuation.**

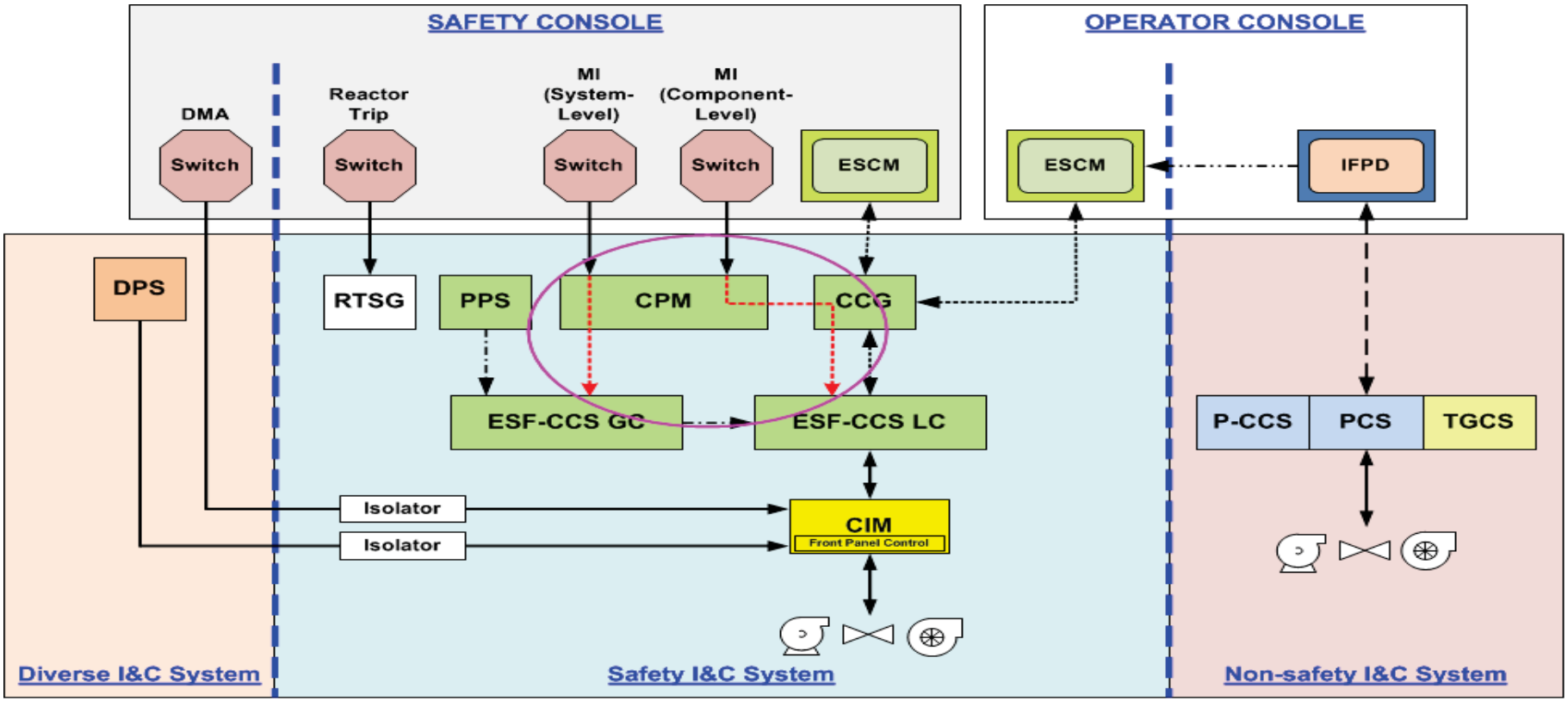
Q6 System and Component level MI Switches (1/4)

- **NRC Question**

  Because both MI system-level and component level manual switches are connected in the same way to the control panel multiplexer (CPM) as shown in Figure 7.3-1 in DCD Tier 2, Section 7.3, what are the logic differences between these two types of manual control commands in the ESF-CCS system?

Q6 System and Component level MI Switches (2/4)

- **Response to NRC Question**



ABBREVIATIONS AND LEGENDS

CCG: Control Channel Gateway
CIM: Component Interface Module
CPM: Control Panel Multiplexer
DMA: Diverse Manual ESF Actuation
DPS: Diverse Protection System
ESCM: ESF-CCS Soft Control Module
ESF-CCS: Engineered Safety Features-Component Control System
FLC : Field Programmable Gate Array (FPGA)-based Logic Controller
IFPD: Information Flat Panel Display
MI: Minimum Inventory
P-CCS: Process-Component Control System
PCS: Power Control System
PPS: Plant Protection System
RTSG: Reactor Trip Switchgear
TGCS: Turbine/Generator Control System

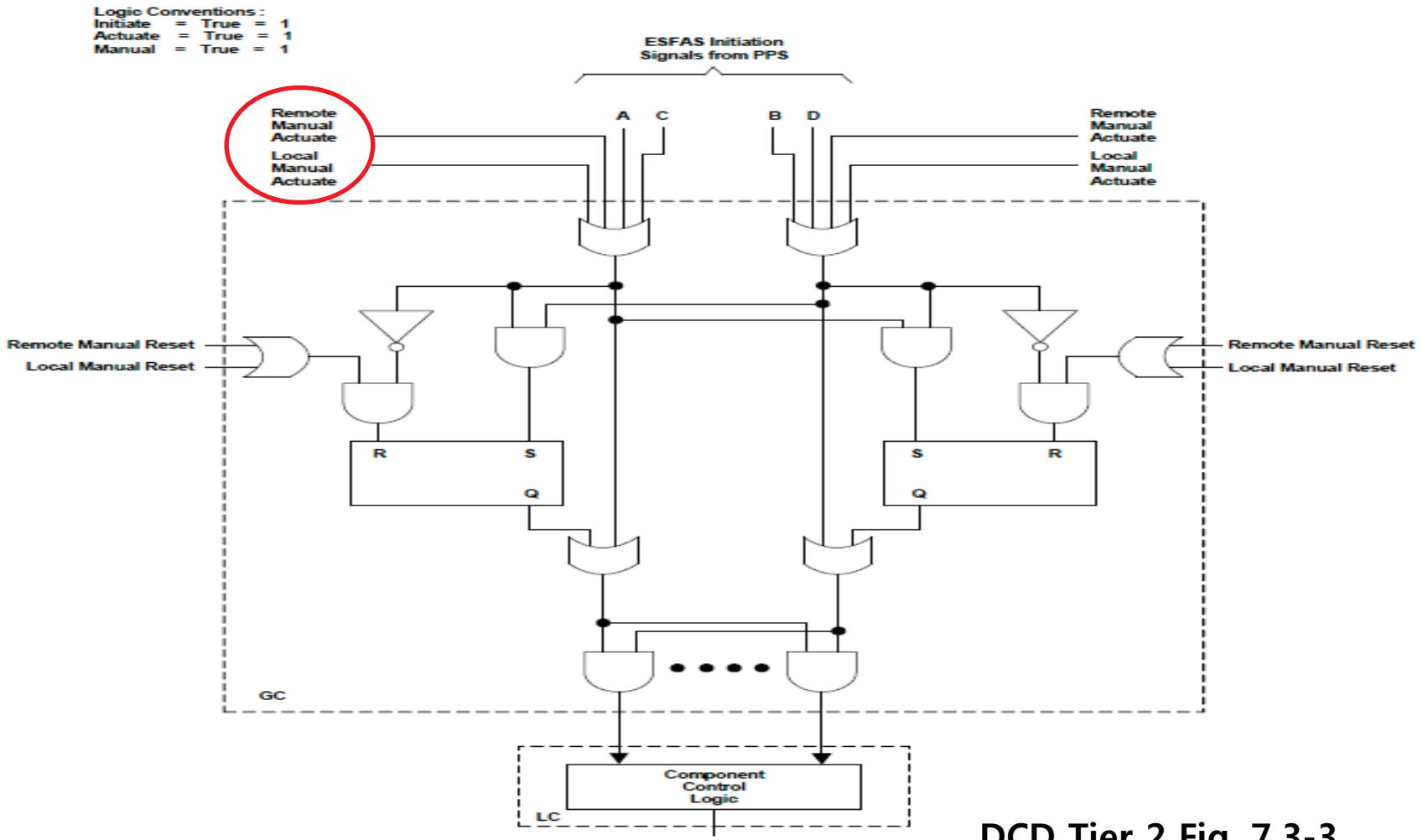
PLC Platform
Hardware Platform
DCS Platform
FLC Platform
Self-standing Platform

Hardwired
Safety system
Data Network (SDN)
Serial Data Link (SDL)
Data Communication Network - Information (DCN-I)
Ethernet

DCD Tier 2 Fig. 7.3-1

Q6 System and Component level MI Switches (3/4)

- **Response to NRC Question**
  - **System-level switch signal**
    - **The signal is inputted to the GC via the CPM, and acquired as the input of 2-o-o-4 voting logic in the GC.**



DCD Tier 2 Fig. 7.3-3

Q6 System and Component level MI Switches (4/4)

- **Response to NRC Question**
  - **Component-level switch signal**
    - **The signal is inputted to the LC via the CPM and CCG, and acquired as the input of component logic in the LC.**

TS

Q7 Local Manual Actuation Commands (1/2)

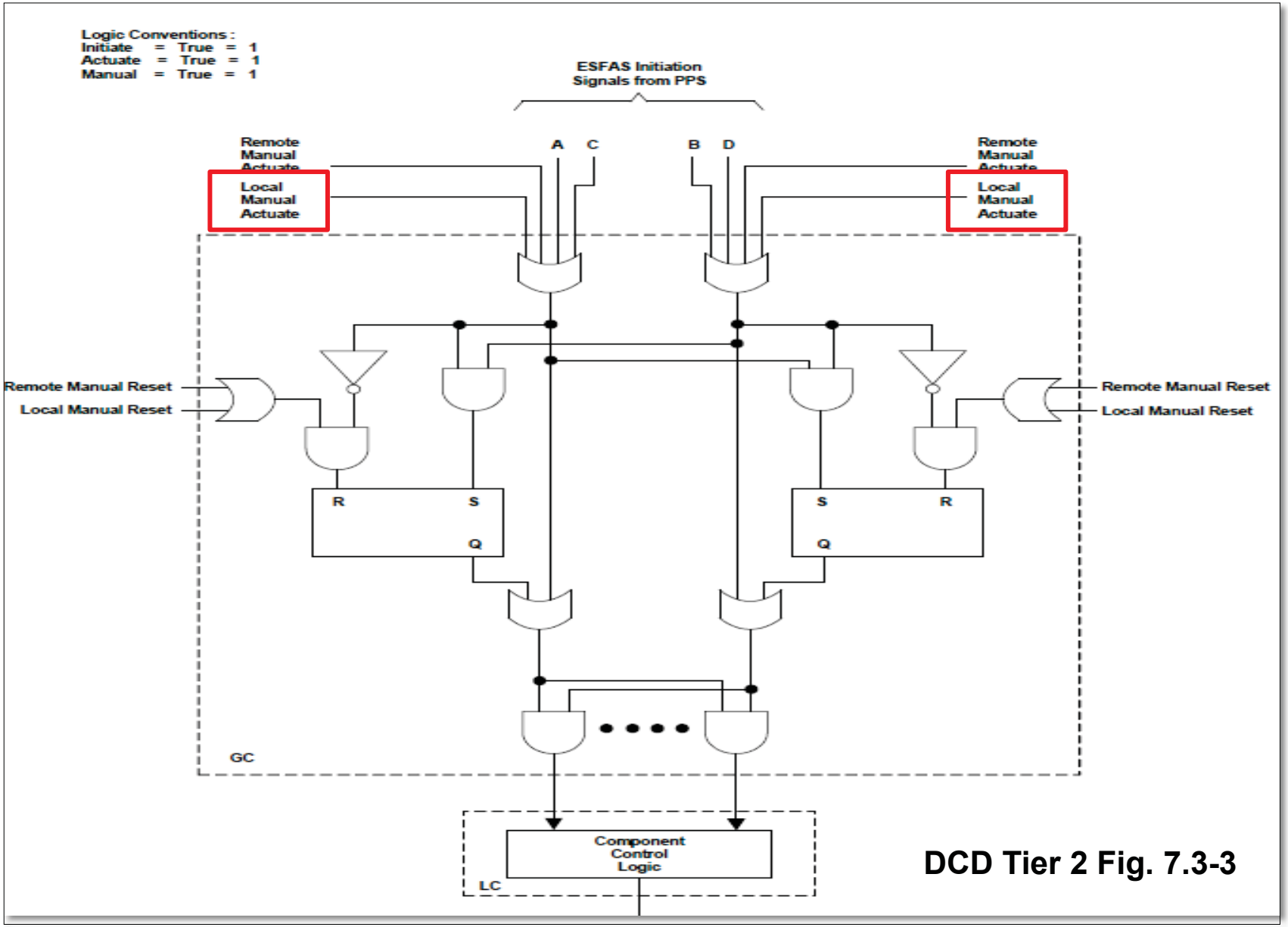
- **NRC Question**

  Besides the remote manual actuation commands, what are the local manual actuation commands at the system level as shown in Fig. 7.3-3?

- **Response to NRC Question**
  - The local manual actuate commands can be initiated from the switch panel of the MTP in the I&C equipment room.
  - While the remote manual actuate commands are transmitted to all ESF-CCS divisions, the local manual actuate commands are transmitted only to the corresponding ESF-CCS division.
  - The local manual actuate commands exist to test and verify that the components of one ESF-CCS division can be actuated at a time.

Q7 Local Manual Actuation Commands (2/2)

- **Response to NRC Question**



DCD Tier 2 Fig. 7.3-3

Q8 Two Division Containment Spray System (1/5)

- **NRC Question**

  The containment spray actuation signal (CSAS) is used to actuate the containment spray system (CSS). The logic diagram for CSAS in Figure 7.3-5 in DCD Tier 2 shows four divisions. However, there are only two containment spray pumps. How is the control logic for the two spray pumps implemented?

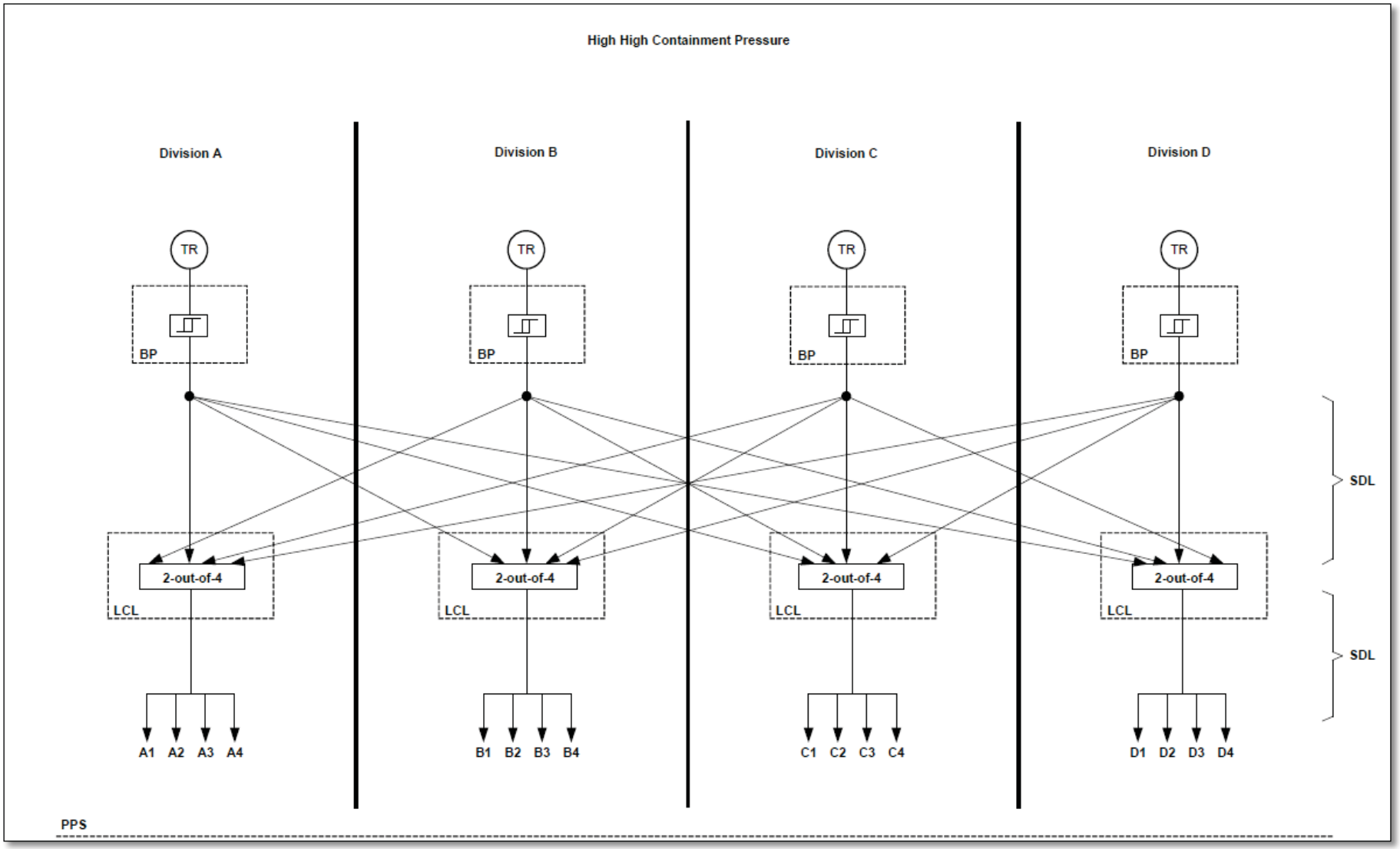
- **Response to NRC Question**
  - **The containment spray actuation signal (CSAS) initiation signal is generated from all four PPS divisions A, B, C, and D, and the initiation signal is transmitted to the group controllers (GCs) in all four ESF-CCS divisions as shown in Figure 7.3-5 of DCD Tier 2.**
  - **The GCs in each ESF-CCS division perform a selective 2-out-of-4 coincidence logic based on the CSAS initiation signal and transmit the actuation signal to the loop controllers (LCs).**
  - **The outputs of the LC in ESF-CCS divisions A, B, C, and D are then transmitted via the component interface module (CIM) to the division A, B, C, and D components, respectively. This is shown in Figure 7.3-5 of DCD Tier 2 and described in Subsection 7.3.1.7 of DCD Tier 2: *"Each ESF-CCS division actuates the ESF components assigned in that division."***

Q8 Two Division Containment Spray System (2/5)

- **Response to NRC Question**
  - As described in Subsection 6.5.2.1 of DCD Tier 2, the containment spray system (CSS) is designed to have two independent divisions, each of which contains one containment spray pump.
  - One containment spray pump is actuated by the CSAS from ESF-CCS division C, while the other containment spray pump is actuated by the CSAS from ESF-CCS division D.
  - The CSAS from ESF-CCS divisions A and B each actuates a shutdown cooling pump when containment spray pumps are not available to actuate.

Q8 Two Division Containment Spray System (3/5)

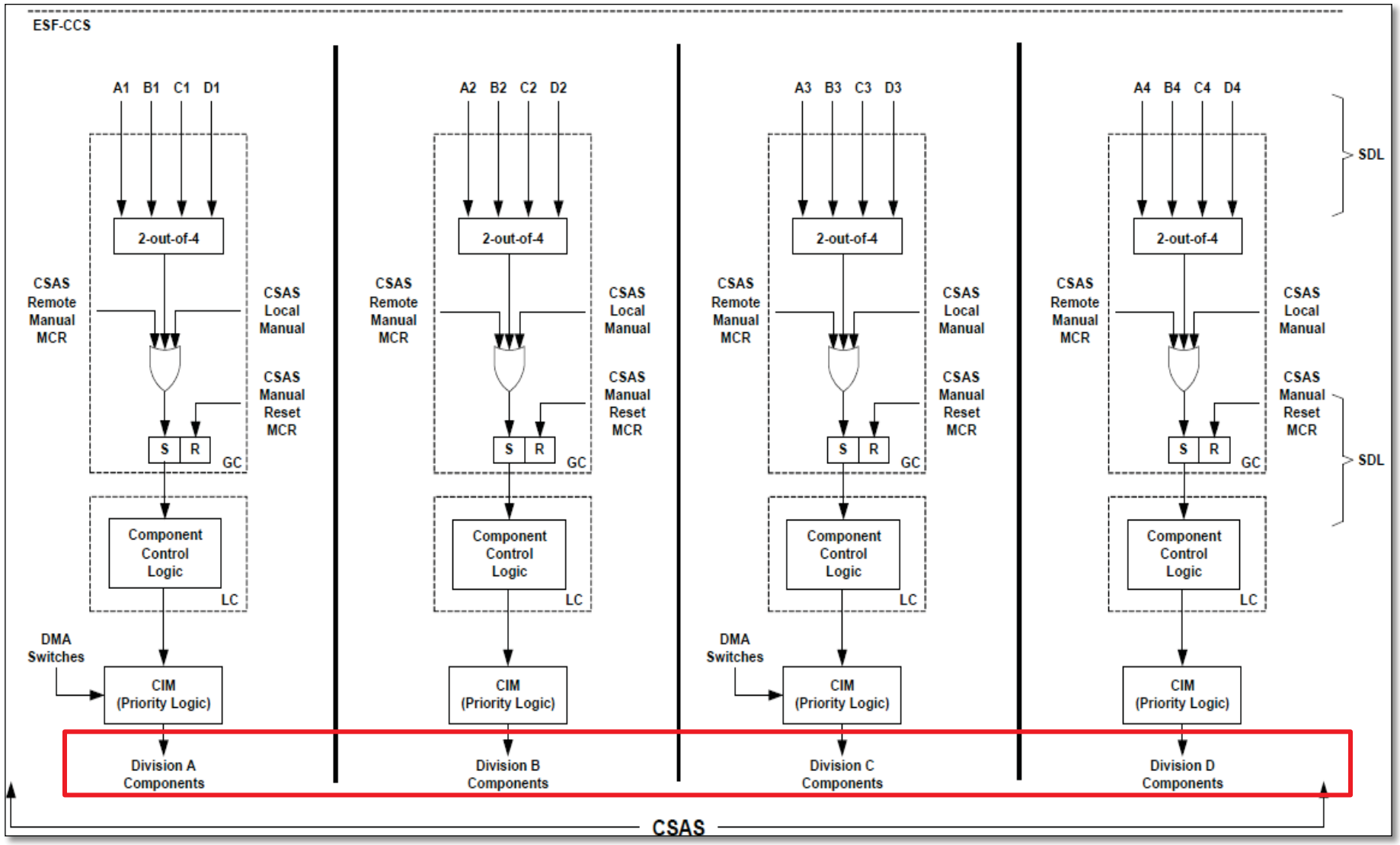
- **Response to NRC Question**



DCD Tier 2 Fig. 7.3-5 ESFAS Functional Logic (CSAS)

Q8 Two Division Containment Spray System (4/5)

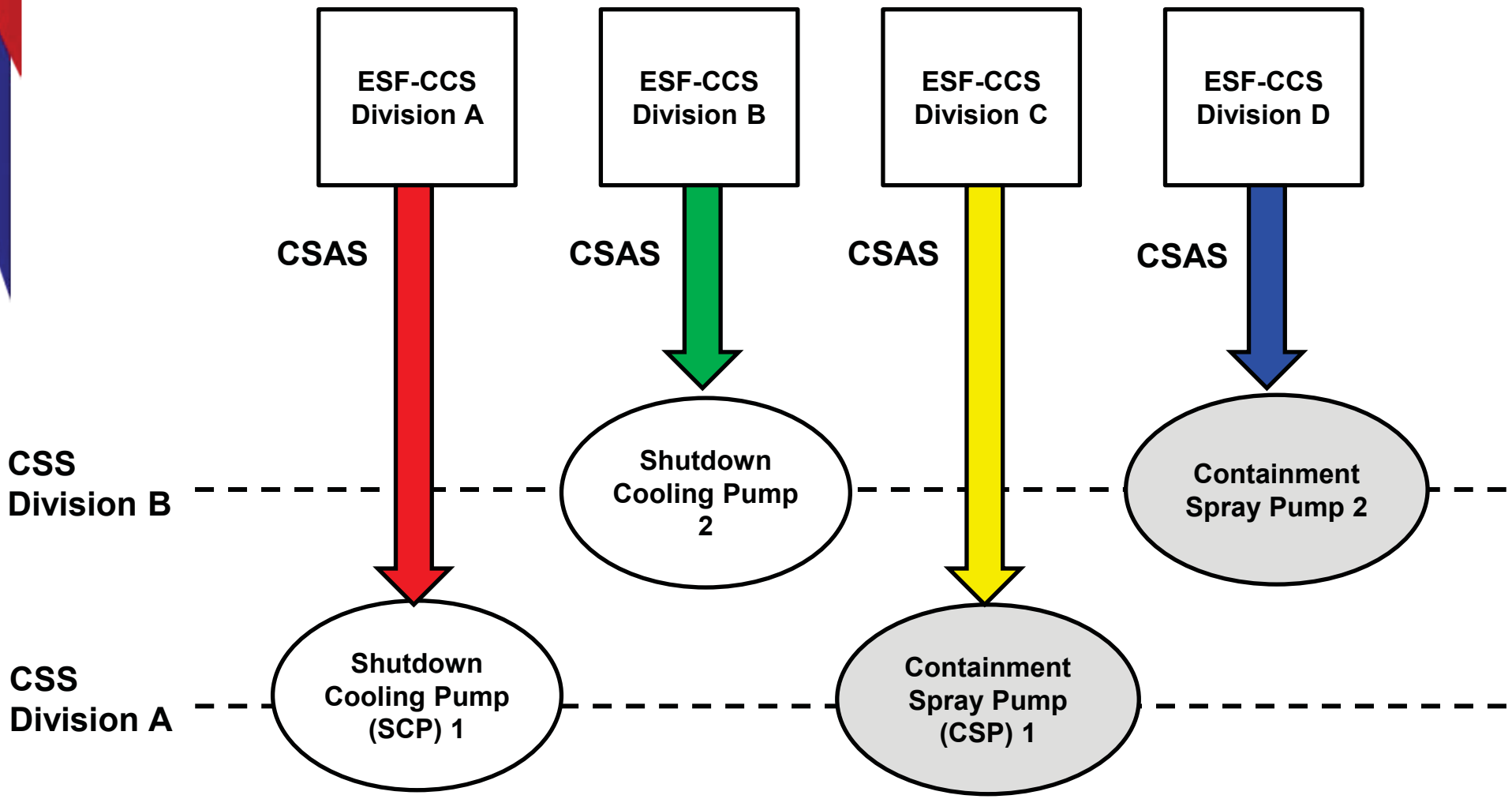
- **Response to NRC Question**



DCD Tier 2 Fig. 7.3-5 ESFAS Functional Logic (CSAS)

Q8 Two Division Containment Spray System (5/5)

- **Response to NRC Question**
  - **Simplified Diagram of CSP and SCP operation**



Q9 CIM Modulating Control (1/1)

- **NRC Question**

  Both Figure 7.3-1 in DCD Tier 2 and Figure 4-13 in the Safety I&C System Tech. Report show the component interface module (CIM) used for the ESF-CCS system.

  Clarify how the CIM is used for modulating control components?

- **Response to NRC Question**
  - **The CIM manages the priority of different actuation signals, and sends signal which results from application of the priority management to a given plant component.**
  - **The signals for modulation control also are combined in the same manner as for any other components in the CIM (i.e., using state based priority).**
  - **Accordingly, the CIM receives component control signals including modulation control from the ESF-CCS, and sends the demand signal to the component.**
  - **The modulating function is implemented in the ESF-CCS LC.**

Q10 Class 1E Switchgear for Safety Component (1/2)

- **NRC Question**

  How is the I&C function implemented for the incoming and outgoing breakers of the Class 1E switchgears used to provide sources to power ESF components and other safety systems?

- **Response to NRC Question**
  - Various input signals come to the ESF-CCS related to incoming and outgoing circuit breakers of the Class 1E switchgears.
  - The I&C functions are implemented with these signals in the ESF-CCS and close/ trip operation of the power circuit breaker (PCB) is performed. The ESF-CCS also gives output signal to related electrical logics (such as alternate feeder breaker, EDG, AAC gen., alarm, and etc.) as an input signal.
  - The ESF-CCS has an interface with Class 1E PCB, as shown on the next slide.
  - The ESF-CCS LC performs the logical control function for close or trip operation of the PCB according to the predetermined conditions in the control logic diagram.

Q10 Class 1E Switchgear for Safety Component (2/2)

- **Response to NRC Question**

TS

Q11 Non-safety Control Signals in Loop Controller (1/4)

- **NRC Question**

  What are the justifications for the non-safety control signals used in the safety-related loop controllers as shown in Figure 4-13 in the Safety I&C Tech. Report?

- **Response to NRC Question**
  - **The functions, purpose, and evaluation results for non-safety signals are described in Section 4.9 of the Control System CCF Analysis TeR (APR1400-Z-J-NR-14012-P).**
  - **The P-CCS sends a few control signals to the ESF-CCS. However, the control logic in the ESF-CCS is designed so that non-safety control signal can only be actuated to safe mode (e.g., close the valve). Therefore, the non-safety control signal cannot cause spurious opening of the valves at any time.**

Q11 Non-safety Control Signals in Loop Controller (2/4)

- **Response to NRC Question**
  - Table 4.9-1, Control System CCF Analysis TeR

TS

Q11 Non-safety Control Signals in Loop Controller (3/4)

- **Response to NRC Question**
  - **Table 4.9-1, Control System CCF Analysis TeR**

TS

Q11 Non-safety Control Signals in Loop Controller (4/4)

- **Response to NRC Question (**

TS

CLOSE

Q12 Backup HSI (1/3)

- **NRC Question**

  What HMI is primarily used to control safety-related and non-safety equipment during normal, abnormal, and accident conditions?

  What HMI is used as backup if the primary HMI fails?

Q12 Backup HSI (2/3)

- **Response to NRC Question**
  - **Primary and backup HSIs**

TS

Q12 Backup HSI (3/3)

- Response to NRC Question

TS

Q13 Common Q Tool Connection (1/2)

- **NRC Question**

  Section 5.6.10 of the Common Q Topical Report states that "When the reboot occurs, the Windows operating system is started up in order to be able to use the tool that connects to the AC 160 for maintenance. When this occurs, all AF 100 variables are marked invalid by the safety function processor (PM646A) in the AC 160, and all Ethernet datalink activity which would be monitored by the non-safety system is halted. When the tool is connected and the execution of the application program in the safety function processor is halted in order to change software then..."

  Clarify whether the tool that performs software modifications is normally physically disconnected from the safety I&C systems.

Q13 Common Q Tool Connection (2/2)

- **Response to NRC Question**
  - **AC160 PLC S/W loading and maintenance in the APR1400**
    - **The MTP is not used for maintenance and SW loading.**
    - **Serial cable is connected to the dedicated program port of PLC processor module (PM) temporarily.**
    - **Loading cable is disconnected on each end to prevent inadvertent programming during normal plant operations.**
  - **Compliance to DI&C-ISG-04, Section 1, Position 10 in the Safety I&C System TeR (APR1400-Z-J-NR-14001) states that :**
    - **"... the software is loaded into the PM by a serial connection between the portable workstation and the PM."**
    - **"This loading cable is always disconnected on each end to prevent inadvertent programming during plant operations."**

Q14 CCF Indication (1/2)

- **NRC Question**

  How exactly do they know when a software CCF has occurred within the safety system, including the PPS or ESF-CCS?

  Are there any indications or annunciators that let the operators know of a software CCF condition?

  What indications prompt the operators to use the DAS?

Q14 CCF Indication (2/2)

- **Response to NRC Question**
  - There are no CCF-specific alarms or indications. A software CCF may not be detected until the periodic testing on the safety systems is performed, because no alarms or indications are provided by the safety systems upon a software CCF.
  - If a software CCF and a DBE occur concurrently, the DPS is automatically actuated and the alarms and indications are provided in the MCR, enabling the operator to be aware of safety system CCF.
  - As described in Subsection 7.8.3.2 of DCD Tier 2, during the software CCF, the data passed to the IPS from systems other than the PPS and ESF-CCS are processed for display and alarm.
  - As described in Subsection 7.8.3.1 of DCD Tier 2, the DIS and DMA switches provide means for the operator to take manual actions necessary for the mitigation of AOO and PA concurrent with software CCF in safety systems, to place the plant in a safe shutdown condition, and to monitor and maintain the critical safety functions. The safety functions remain intact.
  - Further information is provided in the CCF Coping Analysis TeR (APR1400-Z-A-NR-14019-P).

Q15 100% Testable CIM (1/5)

- **NRC Question**

  KHNP claims that the CIM is a non-software-based qualified nuclear safety grade module. However, the CIM may not be composed of analog circuitry and hence there's firmware associated with it. KHNP needs to substantiate their claims and if not, then show that the CIM is 100% tested and proven not to be susceptible to a software CCF condition.

Q15 100% Testable CIM (2/5)

- **Response to NRC Question**

TS

Q15 100% Testable CIM (3/5)

- **Response to NRC Question**
  - **Base Section**
    - **Provides interface to controlled component: power switching, status feedback (e.g., limit switch).**
    - **Provides power switching monitoring with output interface to Diagnosis Section.**
    - **Employs only conventional hardware devices (e.g., field effect transistor).**
    - **Is used by all control demands: ESF-CCS, DPS, DMA switches, front panel control (FPC), etc.**
    - **Will be "100%" tested (i.e., all input combinations).**

Q15 100% Testable CIM (4/5)

- **Response to NRC Question**
  - **Priority Logic Section**
    - **Combines control demand inputs through priority logic from all control sources: ESF-CCS, DPS, DMA switches and FPC.**
    - **Provides output interface to Diagnosis Section.**
    - **Employs only conventional hardware devices (i.e., CMOS or TTL).**
    - **Is used by all control demands: ESF-CCS, DPS, DMA switches, and FPC.**
    - **Will be "100%" tested (i.e., all input combinations).**
  - **Diagnosis Section**
    - **Monitors operability of Priority Logic Section and Base Section via high impedance inputs with no short circuit potential.**
    - **Receives status inputs only from those sections and provides no outputs to those sections.**
    - **Employs FPGA. The FPGA of the Diagnosis Section is developed in accordance with RG 1.152 and BTP 7-14. V&V is performed in accordance with IEEE-1012 SIL-3, because FPGA is for monitoring only (no safety function).**
    - **Is not required for 100% test of the functions.**

Q15 100% Testable CIM (5/5)

- **Response to NRC Question**

  - The component feedback signals are sent to the ESF-CCS LC via relay output in the CIM with bypassing the diagnosis section. These signals are only monitoring purpose.
  - The diagnostic result signals of the Diagnosis Section are sent to the ESF-CCS LC for the maintenance purpose.
  - Any failures of the CIM are regarded as single failure of the component because the Base Section and Priority Logic Section performing safety actuation function in the CIM have no software.
  - All sections are designed and manufactured as Class 1E devices under 10CFR50 Appendix B.

Q16 CEA Position Processor Failure (1/5)

- **NRC Question**

  For the APR1400 FSAR, Tier 2, Revision 0, Table 7.2-7, "Failure Mode and Effects Analysis for the Plant Protection System," single failure entry item 2-14, b), provide detailed design descriptions that would explain the failure terms:

  a. *Unrecognized software malfunctions,*
  b. *Erroneous control element assembly (CEA) position transmission and indication,*
  c. *Improper CEA position.*

  In addition, also describe how improper CEA position renders a core protection calculator (CPC) channel inoperable and changes the logic to 2-out-of-2 coincidence.

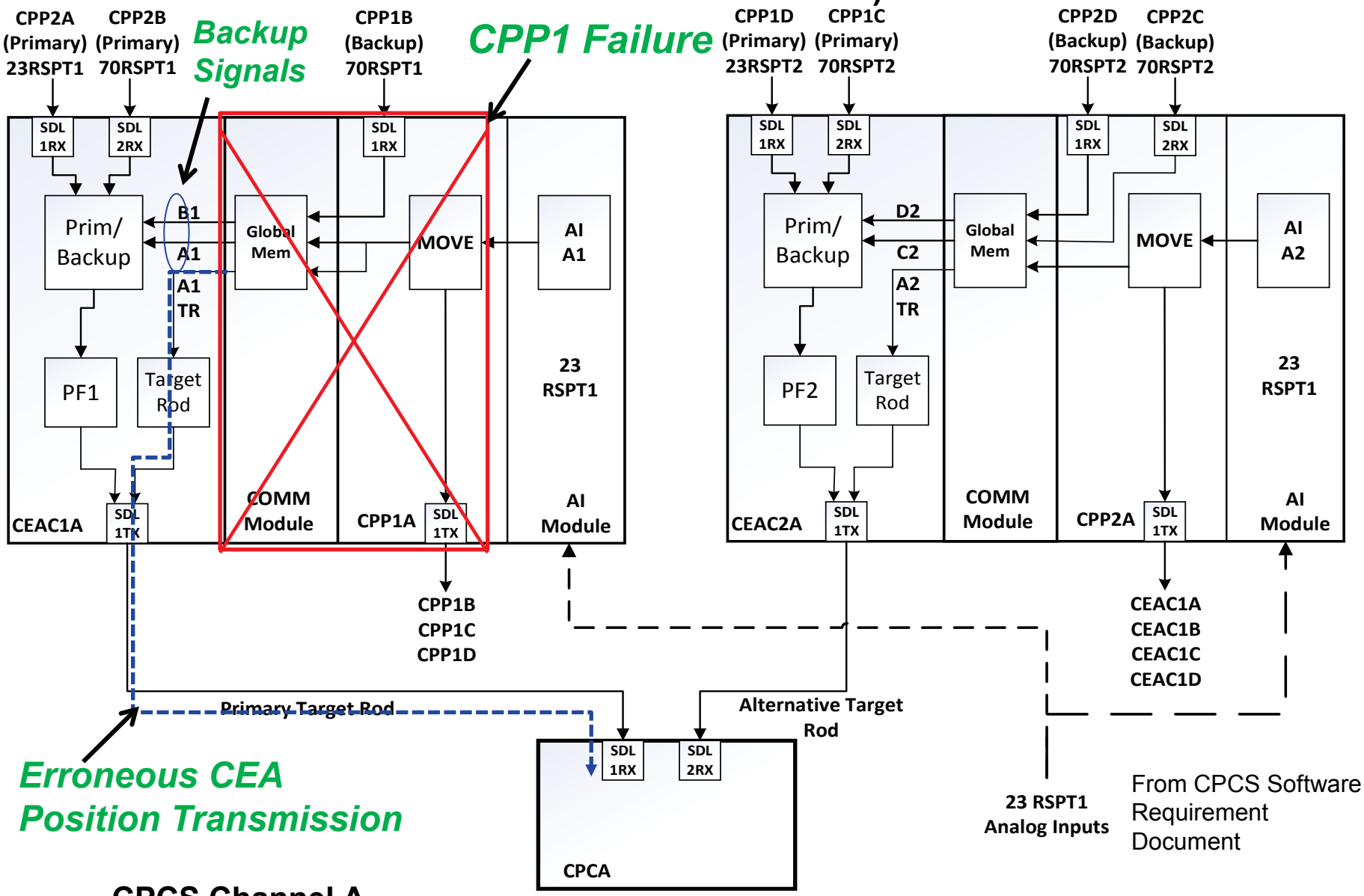
  Provide detailed design descriptions that describe and define the failure terms used of software malfunction, erroneous CEA position, erroneous CEA indication, and improper CEA position. In addition, describe how, upon receiving improper CEA position, a CPC channel would become inoperable and the RPS logic would change to a 2-out-of-2 coincidence logic.

Q16 CEA Position Processor Failure (2/5)

- **Response to NRC Question**
  - **Unrecognized software malfunctions**
    - Software failure which can not be detected by system and application diagnostics
  - **Erroneous control element assembly (CEA) position transmission and indication**
    - The CEA position processor reads the CEA positions and provides these values to the CEA calculator (CEAC) for calculation and to the OM and MTP for display.
    - Erroneous CEA position transmission means providing CEA values which are different from reading values from AI modules to the CPP, CEAC, and CPC processors.
    - Erroneous CEA indication means providing CEA values which are different from reading values from AI modules to the OM and MTP.
  - **Improper CEA position**
    - Erroneous CEA positions which can not generate the DNBR/LPD trip

Q16 CEA Position Processor Failure (3/5)

- **Response to NRC Question**
  - **CPP1 Failure in Tier 2 Table 7.2-7 Item 2-14 b)**



Q16 CEA Position Processor Failure (4/5)

- **Response to NRC Question**
  - **CPP1 Failure in Tier 2 Table 7.2-7 Item 2-14 b)**

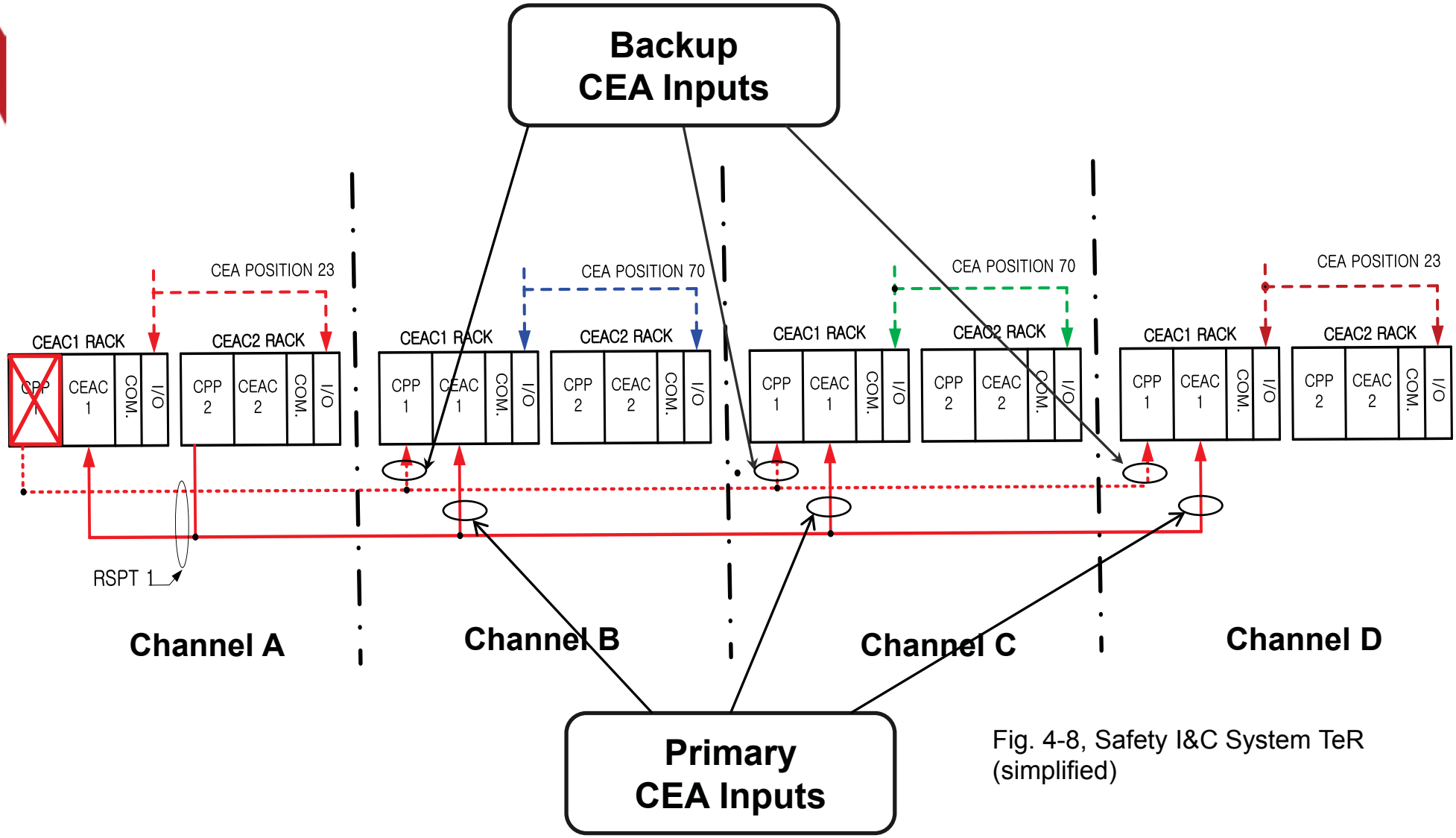


Fig. 4-8, Safety I&C System TeR (simplified)

Q16 CEA Position Processor Failure (5/5)

- **Response to NRC Question**
  - CPP1 in channel A and B is the primary source for target CEA in the CPC.
  - Recognized failure
    - If any of the CPPs and/or communication sections has detected failures, the redundant feature in the channel takes over the safety functions.
    - No effect on the PPS (2-out-of-3 voting logic)
  - Unrecognized failure
    - Failure to trip status : 1-out-of-2 voting logic
    - Failure to un-trip status : 2-out-of-2 voting logic (FMEA considered)
      - ✓ Declare CPCS channel A as inoperable.
  - CPP1 in channel A and B is the alternative source for non-target CEA position in channels B, C, and D.
    - No effect on PPS channels B, C, and D (previous slide).

Q17 Failed RSPT (1/2)

- **NRC Question**

Section C.5.1.3.7, "DI&C-ISG-04 Staff Positions," of the Technical Report "Safety I&C System" APR1400-Z-J-NR-14001-P, Revision 0, states that:

> *If four or more RSPT1 signals are failed and four or more RSPT2 signals are failed, CEAC1 and CEAC2 will be inoperable in all channels; the CPC in each channel will use a predetermined PF. The result of applying that PF may or may not result in a plant trip….*

a. *Explain how the predetermined control element assembly (CEA) penalty factor (PF) value, during normal plant operation, provides requisite assurance that it will be a PF value that is an accurate representation of the actual core CEA PF.*

b. *Discuss why, after sensing that both reed switch position transmitter (RSPT)1 and RSPT2 signals have failed, the safety system would not automatically place the affected channel(s) in trip.*

c. *Discuss why, after sensing that both CEA calculator (CEAC)1 and CEAC2 are inoperable, the safety system would not automatically place the affected channel(s) in trip. How do you ensure not placing the affect channel in trip results in a safe state for the plant?*

Q17 Failed RSPT (2/2)

- **Response to NRC Question**
  - CEAC inoperable
    - When four or more sensors fail, the CEAC is inoperable.
    - The CPC issues the sensor failure alarm.
  - Both CEACs inoperable
    - Apply the penalty factors (PFs) based on a time delay logic.
      - ✓ During the time delay, larger value of the last good PFs between CEAC1 and CEAC2 is used.
      - ✓ If the CEACs are still inoperable after the time delay, the predetermined PF is used.
    - Predetermined PF is large enough to make DNBR and LPD trips.
    - The time delay is calculated through the safety analysis.
  - Both CEACs inoperable (CINOP) by planned
    - Operator sets CINOP as '3' (two CEACs Inoperable)
    - Two CEACs are under Tech. Spec. LCO 3.3.3, Item B
      - ✓ "Both CEACs inoperable in one or more CPCS channels."
      - ✓ B.1 Declare affected channel(s) inoperable (within 1 hour).
      - ✓ OR B2.1 and B2.2 and B2.3 and B2.4 and B2.5. (every 4 hours)

Q18 Uncertainty TeR (1/1)

- **NRC Question**

  What is the purpose of the Technical Report APR 1400-Z-NR-14004-P, "Uncertainty Methodology and Application for Instrumentation?" This TeR is not referenced in the APR 1400 FSAR Tier 2, Chapter 7 but it is incorporated by reference in the APR1400 application. What regulation does this technical report intend to meet?

- **Response to NRC Question**
  - **The Uncertainty TeR is intended to provide methodology for uncertainty calculations of safety-related instruments in accordance with ISA-RP 67.04, Part II and to meet the uncertainty requirements of RG 1.105 and ISA-S67.04, Part I, for the setpoint determination of safety-related instruments.**
  - **The Uncertainty TeR is described as a reference in Subsections 7.2.2.7 and 7.3.2.7 of DCD Tier 2, to provide the methodology for calculating uncertainty.**
  - **In Subsection 3.4.9 of the Safety I&C System TeR, the Uncertainty TeR is also described as a reference to substantiate claims that the setpoints of the safety I&C system comply with ISA-S67.04, Part I endorsed by RG 1.105.**

Q19 Inoperable Function or Component (1/1)

- **NRC Question**

  What does declaring a function or component "inoperable" in Tech Specs mean in terms of the output and processor state the affected components?

- **Response to NRC Question**
  - "Operable" in Section 1.1 of DCD Tier 2 Technical Specifications.
    - A system, subsystem, division, train, component or device shall be OPERABLE when it is capable of performing its specified safety function(s)...
  - "Inoperable"
    - It is not capable of performing its specified safety function(s).
  - Output state of the affected components declared as "Inoperable"
    - No trip ("On" state) of DO module
    - Closed state of relay
  - Processor is operating but can not generate trip signal.
    - Processor state of the affected components declared as inoperable

Q20 Invalid CEA Position (1/5)

- **NRC Question**

  If a CEAC receives an invalid CEA position, does that make the CEAC inoperable?

  For Tech Spec 3.3.3, does CEAC mean just the CEAC processor or does it refer to the CEAC rack ?

Q20 Invalid CEA Position (2/5)

- **Response to NRC Question**
  - CEAC operability when CEA positions are failed or invalid.

Type	RSPT1 or 2 Failure	AI failure in Primary	AI failure in Back-up	Processor or Communication section failure in Primary	Processor or Communication section unrecognized failure in Primary
Primary CEA	Failure	Failure	Good	Failure	Invalid
Back-up CEA	Failure	Good	Failure	Good	Good
CEAC Input Calculation	Use Previous Valid CEA Position	Use Back-up CEA Position	No Effect	Use Back-up CEA Position	Use Invalid CEA Position
Alarm	Sensor Failure	Trouble	Trouble	Trouble	Trouble by Comparison of CEA Positions and PF1,2
CEAC Operability	CEAC1 or 2 Failure Operable	Operable	Operable	Operable	Trip : Operable No trip : Inoperable

Q20 Invalid CEA Position (3/5)

- **Response to NRC Question**
  - **CPP2 Failure in Tier 2 Table 7.2-7(FMEA) (new item)**

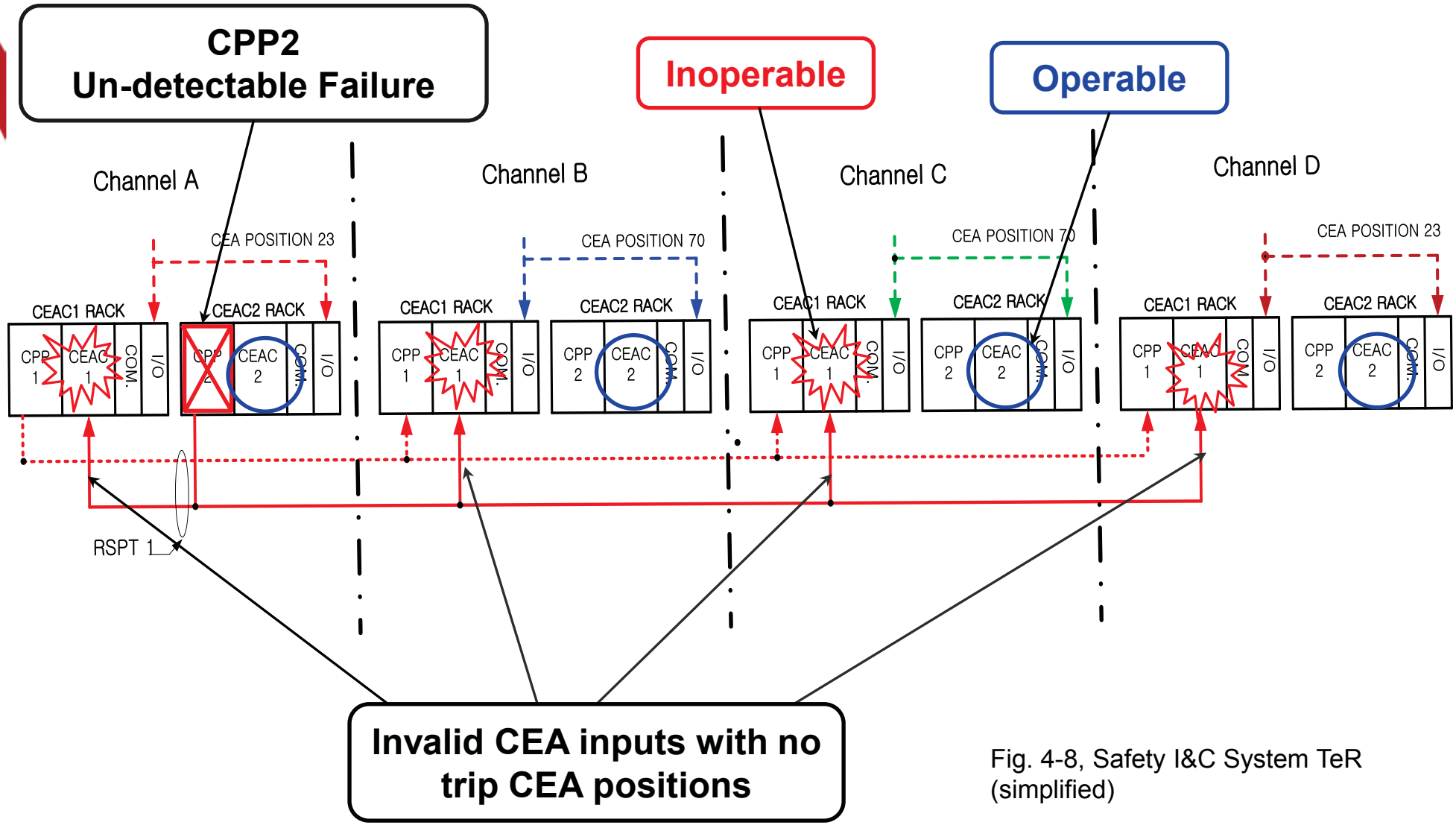


Fig. 4-8, Safety I&C System TeR (simplified)

Q20 Invalid CEA Position (4/5)

- **Response to NRC Question**
  - **Tier 2 Table 7.2-7 (FMEA) to be revised**
    - **This is the CEAC1 inoperable case by invalid CEA position.**
    - **Failure mode is erroneous CEA position transmitted by operating CPP2.**
    - **A new item will be added in the FMEA Table as follows.**

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
Later	CEA Position Processor 2 in Channels A or B. Processor and/ or communic -ation section.	b) ON; **Erroneous CEA position transmitted**	**Un-recognized** hardware or **software malfunction**	Failure to provide proper primary source of CEA position in CEAC 1 in all channels. Possible failure of alternative source of target CEA position transmission in channel of origin	Possible **erroneous non-target CEA position indication. Possible difference between PF of CEAC1 and CEAC2** If problem is occurred due to processor failure, this is detected by on line diagnostics and a CPP Trouble/CPP WDT time out.	CPP2 is primary source for CEAC 1 position indication, and is normally selected. If non-target CEA position may be improper in one CPC channel, CEAC2 is redundancy. CPP2 is alternative source of Target CEA position.	None. If **non-target CEA position is improper**, CEAC1s in all channel are inoperable, and CEAC2s are available in four channels. **RPS logic is in 2-out-of-3 coincidence logic**.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3. After on-line diagnostic function is performed and the problem within CEAC module is identified, CEAC fail condition is generated.

Q20 Invalid CEA Position (5/5)

- **Response to NRC Question**
  - For Tech Spec 3.3.3, CEAC means the CEAC rack.
  - CEAC rack includes
    - CEAC, CPP Processors
    - CI module for AF100
    - AI modules