ISG Rev C Content	Industry Comments	Resolution
Task Working Group #4: Highly Integrated Control Rooms – Communications Issues (HICRc) Interim Staff Guidance	Start with a scope clarification, since this is applicable to inter-division safety communications and non-safety to safety communication only.	
BACKGROUND This section presents guidance concerning operator workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division. This guidance also applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation.	Some of these requirements also apply to any workstation controlling only multiple non-safety functions.	
3.1 Independence and Isolation Multidivisional control and display stations must permit control/modification of equipment in only one safety division at a time.	"At a time" is not clear. The intent of multi-division operator stations is to allow concurrent control of all safety divisions. What if two divisions of a safety I&C system actuate two separate solenoid pilots on a single isolation valve. Such a configuration is used to prevent spurious actuation due to single failure of the safety system (e.g., MSIV); however, it also means that to actuate the single valve, a command must be sent to two safety divisions to operate their solenoid pilots. Also, for the containment isolation function, generally two safety divisions will separately send close an inner or outer isolation valve. A single manual command for containment isolation will	

ISG Rev C Content	Industry Comments	Resolution
	need to go to the two divisions that can control the inner (or outer valve).	
3.1.2 Safety related stations receiving information from other divisions (safety or nonsafety): All communications with equipment outside the station's own safety division, including communications with equipment that is not safety related, must be as described in the guidelines for interdivisional communications.	Reword underlined to: is not safety related or safety related,	
3.1.3 Nonsafety stations influencing the operation of safety related equipment:		
• The nonsafety station must access the safety equipment only by way of the safety related controls or priority module associated with that equipment. Communications with those safety related controls must be as described in the guidelines for interdivisional communications or for command prioritization, as applicable.	Reword underlined to: safety related controls or priority module must	
• The safety related controls for the subject equipment must include provisions for command prioritization as described in this guidance.	Reword underlined to: safety-related controls or separate priority logic function for	
• The safety related controls must be designed so as to preclude the nonsafety station from influencing the operation of the safety related controls when the safety related controls are performing their safety function.	Reword to: The safety related controls must be designed so as to preclude the nonsafety station from adversely affecting the operation of the safety related controls prior to completion of the safety function.	

ISG Rev C Content	Industry Comments	Resolution
	Comment: For consistency with previous section. After the safety function is completed, it is acceptable to use non-safety workstations to reposition components.	
This includes: ☐ The nonsafety station must not be able to bypass any safety function unless that function's own safety system has itself determined that such action would be acceptable.	It is acceptable to allow non-safety control station to be able to bypass a safety function in a division under the specific condition when that division has itself determined that such action would be acceptable. Reword from: "must not be able to bypass any safety function unless that function's own safety system has " to: 'must be able to bypass any safety function only when the affected division has'	
☐ The nonsafety station must not be able to suppress any safety function.	Reword to: The nonsafety station must be able to reset any safety function only when the affected division has itself determined that such action would be acceptable.	
☐ The nonsafety station must be able to bring a safety function out of bypass condition only when that function's own safety system has itself determined	This cannot be applied to maintenance bypasses. These restrictions should allow these operations, if the affected division determines it is safe. For operating bypasses, the nonsafety control station must be able to bring a safety channel out of bypass condition only when that affected division has itself determined that such action would be	

ISG Rev C Content	Industry Comments	Resolution
	acceptable. Reword to: The nonsafety station must be able to bring a safety function out of bypass condition only when the affected division has itself determined that such action would be acceptable.	
3.4. Safety related stations influencing the operation of equipment in other divisions: Safety related stations influencing the operation of equipment in other divisions are subject to constraints similar to those described above for nonsafety stations that influence the operation of safety related equipment. • The control station must address equipment outside its own division only by way of the safety related controls or priority module associated with that equipment. Communications with <u>those safety related controls must</u> be as described in the guidelines for interdivisional communications or for command prioritization, as applicable.	Reword underlined text to: '<u>those safety-related controls or priority module must</u>'	
• <u>The controls in the s</u>afety division of the subject equipment must include provisions for command prioritization as described in this guidance. • The controls in the safety division of the subject equipment must be designed so as to preclude any station outside the equipment's division from influencing the operation of the controls that are within the equipment's own division when the safety related controls are performing their safety	Reword the underlined text to: '<u>The controls or priority module in the</u>'	

ISG Rev C Content	Industry Comments	Resolution
function		
• The controls in the safety division of the subject equipment must be designed so as to preclude any station outside the equipment's division from influencing the operation of the controls that are within the equipment's own division when the safety related controls are performing their safety function. This includes: ☐ The extra divisional (that is, "outside the division") control station must not be able to bypass any safety function unless that function's own safety system has itself determined that such action would be acceptable.	Reword "influencing" to 'adversely affecting'. It is acceptable to allow an extra-divisional control station to be able to bypass a safety function under the specific condition when the division has itself determined that such action would be acceptable. Reword the bullet to: 'The extra-divisional (that is, "outside the division") control station must be able to bypass any safety function only when the affected division has itself determined that such action would be acceptable.'	
☐ The extra divisional station must not be able to suppress any safety function.	Reword to: The extra divisional station must be able to suppress any safety function only when the affected division has itself determined that such action would be acceptable.	
☐ The extra divisional station must be able to bring a safety function out of bypass condition only when that function's own safety system has itself determined that such action would be acceptable.	Safety control stations are prohibited from initiating safety system bypasses or resetting safety functions in other divisions. We propose rewording these restrictions to allow these operations, if the safety division determines it is safe. Reword to: The extra-divisional control station must be able to bring a channel in the equipment's own division out of bypass condition only when the affected division has itself determined that such action would be acceptable.	

ISG Rev C Content	Industry Comments	Resolution
3.4.1 Malfunctions and Spurious Actuations: • No single unit of software shall generate commands to multiple control processors that are assumed to malfunction independently by the safety analysis.	Scope is unclear. Does this apply to non-safety control systems? Or does it also apply to the safety systems? What is a unit of software? Can we point to a definition? The industry suggests: "A single unit of software is defined to be a section of code that once it begins to execute will execute to completion without further user intervention." Reword underlined text to: software function block or single line of executable code should generate Comment: It should be noted in the text that the point of this bullet is to prevent a single event (failure) that causes a piece of code to execute from causing the malfunction of multiple control processors that are assumed to malfunction independently by the safety analysis.	
• No single control action (e.g., mouse click or screen touch) shall generate commands to multiple control processors that are assumed to malfunction independently by the safety analysis. Additional confirmatory command should be added (e.g. do you want to proceed followed by a "Yes" and a "No" choice for critical functions.	Change shall to should. Comment: This is an HFE issue that should not be discussed in this document. This is not needed for communications reliability; the first sentence is sufficient for that purpose. Comment:	

ISG Rev C Content	Industry Comments	Resolution
	It should be noted in the text that the point of this bullet is not to address operator error, but to prevent a single event (failure) from causing the malfunction of multiple control processors that are assumed to malfunction independently by the safety analysis.	
• Each control processor or its associated communication processor shall detect and block commands from the shared resources that do not pass the communication error checks.	Change shall to should.	
• Multidivisional control and display stations must withstand the effects of adverse environments, seismic conditions, EMI/RFI, and all other design basis conditions applicable to safety related equipment at the same plant location.	Does this mean qualification testing? We need to clarify this. At the end, add. . . "without generating multiple spurious control commands." We need to be clear that these workstations do not have to function during and after these adverse conditions. Qualification requirements do not have to ensure functionality. Instead, they simply need to ensure no adverse effects. Comment: The level of required qualification is unclear. If the stations are not required for an automatic safety function or for a credited manual action, then they do not have to function during or after the event. They merely have to "not interfere" with any safety function or place the plant in an unanalyzed situation.	
• Loss of power to any operator workstation or	Comment:	

ISG Rev C Content	Industry Comments	Resolution
controller must not result in spurious actuation of any plant device or system.	Loss of power is one event but there are others such as momentary loss and return of power, etc. This should be more generic.	
• The design should consider the need for an "operator workstation shutdown" switch to be activated upon abandonment of the control room, to preclude spurious actuations that might otherwise occur as a result of the condition causing the abandonment (such as control room fire or flooding).	Reword to: The control and safety system designs required for safety shutdown should include logic that is activated upon abandonment of the Control Room, to preclude spurious workstation actuations that might otherwise occur as a result of the condition causing the abandonment (such as Control Room fire or flooding). Comment: Shutting down the work station may not preclude spurious re-powering due to hot shorts in the MCR. You must block spurious signals at the receiving end.	
• Control processors must be configured and functionally distributed so as to preclude spurious actuation of more than one plant device or system as a result of processor malfunction or software error.	Additional clarification needed here, especially with respect to the first two bullets. It appears that it calls for one computer connecting to one end device. Reword to: Control processors must be configured and functionally distributed so as to preclude spurious actuations that are not enveloped in the plant design bases, accident analyses, and anticipated transients without scram (ATWS) provisions, or in other unanticipated abnormal plant conditions. Spurious actuations that are analyzed are ok. Comment:	

ISG Rev C Content	Industry Comments	Resolution
	"One plant device" is too restrictive. Even "one plant system" is too restrictive. Clearly we want separate control processors for the major NSSS systems, but we do not want to require separate control processors for minor system.	
• Failure or malfunction of any operator workstation must not result in a plant condition (including simultaneous conditions) that is not enveloped in the plant design bases, accident analyses, and anticipated transients without scram (ATWS) provisions, or in other unanticipated abnormal plant conditions	Reword to: Credible Failure or malfunction of the hardware in any operator workstation must not result in a plant condition (including simultaneous conditions) that is not enveloped in the plant design bases, accident analyses, and anticipated transients without scram (ATWS) provisions, or in other unanticipated abnormal plant conditions. Comment: Software failures are addressed in the previous bullets.	
• Multiple spurious actuations due to failure or malfunction of one or more operator workstations must not be possible, or the impact of such multiple spurious actuations must be analyzed and shown to be acceptable under all plant conditions	Suggest deleting or rewording since: 1. The bullets above are intended to define criteria, which if met, precludes the need to consider multiple spurious actuations. 2. Adding this bullet opens the door for additional requirements imposed by each individual reviewer. 2. Some reviewers will claim one can't prove a negative and therefore one cannot satisfy these criteria. Comment: The last two bullets are the "key" guidance. They	

ISG Rev C Content	Industry Comments	Resolution
	should be listed first and the other bullets should be "examples/techniques", not criteria.	
3.3.2 Human Factors Considerations Safety related plant equipment will need safety related controls and displays. If the "normal" controls and displays for such equipment are on multidivisional control and display stations, then additional "backup" control and display stations will be needed. Backup controls and displays may be provided via operator workstations, or they may be provides via hardwired devices such as switches, relays, indicators, and analog signal processing circuits. In either case, the "backup" provisions must consist of safety related devices with safety related software and must be dedicated to specific safety divisions.	Add to the end of the 1st sentence: "…, if manual control of that equipment is credited in the safety analysis or credited to achieve safe shutdown." Replace underlined text with "provided via diverse digital computers and operator workstations". Replace "provides" with 'provided'.	
The need for a plant operator to use backup provisions under upset or accident conditions could pose Human Factors concerns, since the need to use less familiar provisions would coincide with the need for maximum effectiveness and timeliness in operator actions. Such an approach could also result in confusion if the nonsafety displays, as a result of lack of qualification and of lesser quality standards, present obsolete or erroneous information to the plant operator but fail to advise the operator of these potential inaccuracies.	Delete "result in confusion" or provide specific examples of what causes confusion. There needs to be clear guidance on when the Operator may use nonsafety displays. For example, if there is harsh environment, the Operator should not be using non qualified displays originating from non EQ transmitters. The environment at the transmitter has nothing to do with the use of HSI in the MCR. Operators should always suspect erroneous data from unqualified instrumentation, regardless of how that information is displayed in the MCR. This is why	

ISG Rev C Content	Industry Comments	Resolution
	there are specific markings on PAM instruments.	
An applicant would need to demonstrate that such Human Factors considerations, including operator response time, have been adequately addressed in the system design, operating procedures, and accident analyses. This aspect of the application must be reviewed and found acceptable by appropriate Human Factors, Operations, and plant system experts within the NRC.	This should specify the areas to be reviewed such as Human Factors, Operations, and Plant Systems. It also should not require multiple experts to provide reviews.	
3.3.3 Diversity and Defense in Depth (D3) Considerations D3 considerations may influence the number and disposition of operator workstations and possibly of backup controls and indications that may or may not be safety related. The guidance provided herein is not dependent upon such details.	Comment: BTP 7-19 and SRP 7.8 specifically allow non-safety systems to provide diverse actuation capability.	
Footnote omission	This footnote did not appear in the latest ISG draft: "(3) The communication function and the safety logic function can be implemented in separate logic within a single FPGA or ASIC. The interface between the two functions must meet these requirements for interdivisional communications"	