System Requirements Specification

Attributes	Definition
Safety Classification	The system safety classification (e.g., safety, important to safety)
Failure Avoidance	
Functional Qualification	The testing and analyses required to demonstrate the system performs the required functions
Control of Access	The provisions for preventing unauthorized access to equipment or controls.
Restrictions on sharing between units	The limitations of using system functions or equipment to perform functions in more than one unit.
Human Factors	The requirements imposed upon the human machine interface. Typically a reference to NUREG-0700.
Reliability Goals	The qualitative or quantitative goals for probability of the system performing protective actions on demand.
Reliability Analysis Requirements	The testing and analyses required to demonstrate reliability goals are met.
Failure Tolerance	
Redundancy	Requirements for providing multiple components, channels, trains, or systems
Diversity	Requirements for the provision of diverse functions to compensate for failure, particularly common mode failure
Failure Mode	The state to which functions should preferentially fail
Failure Isolation	
Electrical Independence	The provisions made to prevent propagation of failures between redundant functions along electrical connections
Physical Independence	The provisions made to prevent failure of redundant functions because of common equipment locations
Control Protection Isolation	The provisions made to prevent failures from both causing accidents and disabling the protective system response
Behaviors	
Protective Actions ( )	The initiation of a signal for the purpose of accomplishing a safety function.
Function Name	The identification of the function under review.
Inputs	
Parameter	The parameters or set of parameters to be measured
Measurement Location	The location at which each parameter is to be measured
Span	The difference between the maximum and minimum values to be measured.
Rate of Change	The magnitude of change per unit time that the system must accommodate for a specified signal
Frequency Content	The signal bandwidth that must be maintained in the measurement
Spatial Dependency	Number & locations of measurements needed (most often used for core flux or temperature measurements)
Manual Controls	Manual inputs to the functions
Process	
Actuation Algorithm	The relationship between input and the trip/no-trip conditions. Typically a constant with hysterisis. Sometimes a function of other parameters.
Initialization / Reset Mode	The condition that the function assumes upon startup or energization - both initially and after reset.
Outputs	
Outputs	The output signals or commands to be provided by the system
Completion of Protective Action	The point at which the function is considered to be complete and may be reset.
Displays	The information about the function to be displayed to operators
Performance	
Uncertainty	The allowable about by which the channel output is in doubt. Typically includes accuracy, environment effects, drift, etc.
Response Time	The time required after an abrupt change input until the output comes to rest a its new value
Update Rate	The time required to obtain a collection of data
Operational Bypass Functions ( )	Inhibition of the capability to accomplish a safety function that could otherwise occur in response to a particular set of generating conditions.
Function Name	The identification of the function under review.
Inputs	
Permissive Parameter	The parameters or set of parameters to be measured
Measurement Location	The location at which each parameter is to be measured
Span	The difference between the maximum and minimum values to be measured.
Rate of Change	The magnitude of change per unit time that the system must accommodate for a specified signal
Frequency Content	The signal bandwidth that must be maintained in the measurement

Spatial Dependency	Number & locations of measurements needed (most often used for core flux or temperature measurements)
Manual Controls	Manual inputs to the functions. Typically the controls to manually trip or actuate safety functions.
Process	
Bypass Algorithm	The relationship between input and the trip/no-trip conditions. Typically a constant with hysterisis. Sometimes a function of other parameters.
Initialization / Reset Mode	The condition that the function assumes upon startup or energization - both initially and after reset.
Outputs	
Bypass Outputs	The output signals or commands to be provided by the system
Completion of Protective Action	The point at which the function is considered to be complete and may be reset.
Displays	The information about the function to be displayed to operators
Performance	
Uncertainty	The allowable about by which the channel output is in doubt. Typically includes accuracy, environment effects, drift, etc.
Response Time	The time required after an abrupt change input until the output comes to rest a its new value
Update Rate	The time required to obtain a collection of data
Functional Test ( ) -- For each function the following constraints should be considered	
Function Name	The identification of the function under review.
Inputs	
Manual Controls	Manual inputs to the functions. Typically the controls to initiate bypass.
Process	
Test Process	The description of the tests to be performed including pass / fail criteria.
Initialization / Reset Mode	The condition that the function assumes upon startup or energization - both initially and after reset.
Outputs	
Action on Test Failure	The automatic actions, e.g. trip or bypass (if any) taken upon test failure.
Displays	The displays of test results or test status.
Maintenance Bypass Functions -- For each by	Functions to allow removal of the capability of a channel to perform a protective action due to a requirement for replacement, repair, test, or calibration.
Function Name	The identification of the function under review.
Inputs	
Manual Controls	Manual inputs to the functions. Typically the controls to initiate and remove bypass.
Process	
Bypass algorithms	The relationship between input and the bypass/unbypass conditions. Typically a function of the manual bypass control and the status of redundant channels.
Outputs	
Displays	The display of bypass status at the bypass actuation location.
Bypass and Inoperable Status Indication Functions -- For each function the following constraints should be considered	
Inputs	
Bypass Inputs	The bypass status inputs to the bypass and inoperable status indication (BISI) display.
Inoperable Status Inputs	The inoperable status inputs to the bypass and inoperable status indication (BISI) display.
Manual Controls	Manual inputs to the BISI system. Typically switches to manually input status information.
Process	
Bypass indication algorithms	The function that describes the relationship between input conditions and the display. Typically a simple function such as "if bypass then display bypass."
Outputs	
Displays	The system level display of bypass and inoperable status in the control room operating area.

System Requirements Specification

Attributes	Typical Source of Constraints	Typical Location of Constraints	Comments
Safety Classification	10 CFR 50, IEEE 603 Sec 5.12	SAR Ch. 7.1	Protection systems and auxiliary features must be safety
Failure Avoidance			
Functional Qualification	10 CFR 50 Appendix B, Sec III	SAR Ch. 7.1, 7.2, 7.3	

Control of Access	IEEE 603 Sec. 5.9	SAR Ch. 7.1, 7.2, 7.3	
Restrictions on sharing between units	IEEE 603 Sec. 5.13	SAR Ch. 7.1, 7.2, 7.3	
Human Factors	IEEE 603 Sec 5.14	SAR Ch. 18	
Reliability Goals	GDC 21, GDC 29, IEEE 603 Sec. 5.5	SAR Ch. 7.1, 7.2, 7.3, 19	May be quantitative or qualitative
Reliability Analysis Requirements	IEEE 603, Sec. 5.15	SAR Ch. 7.2, 7.3	
Failure Tolerance			
Redundancy	IEEE 603 Sections 5.1	SAR Ch. 7.1, 7.2, 7.3	
Diversity	DiD&D Analysis, IEEE 603 Sec. 5.16	SAR Ch. 7.1, 7.2, 7.3, 7.8	DiD&D analysis should conform with SECY 93-087
Failure Mode	GDC 23	SAR Ch. 7.1, 7.2, 7.3	
Failure Isolation			
Electrical Independence	IEEE 603, Sections 5.6	SAR Ch. 7.1, 7.2, 7.3	
Physical Independence	IEEE 603, Sections 5.6	SAR Ch. 7.1, 7.2, 7.3	
Control Protection Isolation	GDC 24, IEEE 603, Sections 6.3	SAR Ch. 7.1, 7.2, 7.3	
Behaviors			
Protective Actions ( ) -- Each function described in the SAR should be specified. Typically the function may be supported by a process control and measurement diagram or a logic diagram.			
Function Name	Accident analysis assumptions	SAR Ch. 7.2, 7.3, 15	
Inputs - For manual functions only the manual controls item is germane			
Parameter	Accident analysis assumptions, IEEE 603 Sec 6.4	SAR Ch. 15	Parameters shall be direct measures where feasible and practical
Measurement Location	Accident analysis assumptions	SAR Ch. 7.2, 7.3, 15	Unnecessary if parameter measurement is insensitive to location
Span	Accident analysis results (bounds of accident and normal values)	SAR Ch. 15	
Rate of Change	Accident analysis results (measured from transient curves)	SAR Ch. 15	
Frequency Content	Accident analysis results (calculated from transient curves)	SAR Ch. 15	
Spatial Dependency	Accident analysis assumptions	SAR Ch. 7.2, 7.3, 15	Typically important only for neutron monitoring.
Manual Controls	IEEE 603 Section 6.2	SAR Ch. 7.1, 7.2, 7.3	
Process			
Trip Algorithm	Accident analysis assumptions	SAR Chapter 15	Typically bistable decision
Initialization / Reset Mode	SRP	SAR Ch. 7.1, 7.2, 7.3	
Outputs			
Outputs	Accident analysis assumptions	SAR Ch. 7.1, 7.2, 7.3, 15	
Completion of Protective Action	IEEE 603, Section 5.2	SAR Ch. 7.1, 7.2, 7.3	
Displays		SAR Ch. 7.1, 7.2, 7.3, 18	
Performance			
Uncertainty	Accident analysis assumptions	SAR Chapter 15	
Response Time	Accident analysis assumptions	SAR Chapter 15	
Update Rate	Accident analysis results (calculated from transient curves)	SAR Ch. 15	Update rate must be fast enough to be consistent with these.
Operational Bypass Functions ( ) -- For each function the following constraints should be considered			
Function Name	Identifier Only	SAR Ch. 7.1, 7.2, 7.3	
Inputs			
Permissive Parameter	Accident analysis assumptions	SAR Ch. 15	Bypasses will typically be implemented using a sensor channel

Measurement Location	Accident analysis assumptions	SAR Ch. 7.2, 7.3, 15	that is also used for a trip function. In these cases, the input
Span	Accident analysis results (bounds of accident and normal values)	SAR Ch. 15	characteristics will be the same as for the trip function.
Rate of Change	Accident analysis results (measured from transient curves)	SAR Ch. 15	
Frequency Content	Accident analysis results (calculated from transient curves)	SAR Ch. 15	
Spatial Dependency	Accident analysis assumptions	SAR Ch. 7.2, 7.3, 15	Typically important only for neutron monitoring.
Manual Controls	IEEE 603 Section	SAR Ch. 7.1, 7.2, 7.3	
Process			
Bypass Algorithm	Accident analysis assumptions, IEEE 603 Sec. 6.6, 7.4	SAR Chapter 15, 7.1, 7.2, 7.3	
Initialization / Reset Mode	SRP	SAR Ch. 7.1, 7.2, 7.3	
Outputs			
Bypass Outputs	IEEE 603 Sec	SAR Ch. 7.1, 7.2, 7.3	
Displays	IEEE 603 Sec. 5.8	SAR Ch. 7.1, 7.2, 7.3	
Performance			
Uncertainty	Accident analysis assumptions	SAR Chapter 15	Bypasses will typically be implemented using a sensor channel
Resolution	Accident analysis assumptions	SAR Chapter 15	that is also used for a trip function. In these cases, the trip
Response Time	Accident analysis assumptions	SAR Chapter 15	will normally establish the performance characteristics.
Update Rate	Accident analysis results (calculated from transient curves)	SAR Ch. 15	
Functional Test ( ) -- For each function the following constraints should be considered			
Function Name	Identifier Only	SAR Ch. 7.1, 7.2, 7.3	
Inputs			
Manual Controls	Design Decision	SAR Ch. 7.1, 7.2, 7.3	
Process			
Test Process	GDC 21, IEEE 503 Sec 5.7, 6.5	SAR Ch. 7.1, 7.2, 7.3	
Initialization / Reset Mode	SRP 7.1-C, Section 10	SAR Ch. 7.1, 7.2, 7.3	
Outputs			
Action on Test Failure	SRP 7.1-C, Section 10	SAR Ch. 7.1, 7.2, 7.3	
Displays	IEEE 603 Sec 5.10	SAR Ch. 7.1, 7.2, 7.3	
Maintenance Bypass Functions -- For each bypass function the following constraints should be considered			
Function Name	Identifier Only	SAR Ch. 7.1, 7.2, 7.3	
Inputs			
Manual Controls	Design Decision	SAR Ch. 7.1, 7.2, 7.3	
Process			
Bypass algorithms	GDC 21, IEEE 603 Sec 6.7	SAR Ch. 7.1, 7.2, 7.3	
Outputs			
Displays	IEEE 603 Sec. 5.8	SAR Ch. 7.1, 7.2, 7.3	
Bypass and Inoperable Status Indication Functions -- For each function the following constraints should be considered			
Inputs			
Bypass Inputs	IEEE 603 Sec. 5.8.3 (b)	SAR Ch. 7.1, 7.2, 7.3	

Inoperable Status Inputs	IEEE 603 Sec. 5.8.3 (b)	SAR Ch. 7.1, 7.2, 7.3	
Manual Controls	IEEE 603 Section 5.8.3 (c)	SAR Ch. 7.1, 7.2, 7.3	
Process			
Bypass indication algorithms	IEEE 603 Sec. 5.8	SAR Ch. 7.1, 7.2, 7.3	
Outputs			
Displays	IEEE 603 Sec. 5.8	SAR Ch. 7.1, 7.2, 7.3	

System Requirements Specification

Attributes	Safety Constraint	Source	Actual Requirement	Source	Constraints Met?	Comments
Safety Classification						
Failure Avoidance						
Functional Qualification						
Control of Access						
Restrictions on sharing between units						
Human Factors						
Reliability Goals						
Reliability Analysis Requirements						
Failure Tolerance						
Redundancy						
Diversity						
Failure Mode						
Failure Isolation						
Electrical Independence						
Physical Independence						
Control Protection Isolation						
Behaviors						
Protective Actions ( ) -- For each function the following constraints should be considered						
Function Name						
Inputs						
Parameter						
Measurement Location						
Span						
Rate of Change						
Frequency Content						
Spatial Dependency						
Manual Controls						
Process						
Actuation Algorithm						
Initialization / Reset Mode						
Outputs						
Outputs						
Completion of Protective Action						
Displays						
Performance						
Uncertainty						
Response Time						
Update Rate						
Operational Bypass Functions ( ) -- For each function the following constraints should be considered						
Function Name						
Inputs						
Permissive Parameter						

Measurement Location						
Span						
Rate of Change						
Frequency Content						
Spatial Dependency						
Manual Controls						
Process						
Bypass Algorithm						
Initialization / Reset Mode						
Outputs						
Bypass Outputs						
Displays						
Performance						
Uncertainty						
Resolution						
Response Time						
Update Rate						
Functional Test ( ) -- For each function the following constraints should be considered						
Function Name						
Inputs						
Manual Controls						
Process						
Test Process						
Initialization / Reset Mode						
Outputs						
Action on Test Failure						
Displays						
Maintenance Bypass Functions -- For each bypass function the following constraints should be considered						
Function Name						
Inputs						
Manual Controls						
Process						
Bypass algorithms						
Outputs						
Displays						
Bypass and Inoperable Status Indication Functions -- For each function the following constraints should be considered						
Inputs						
Bypass Inputs						
Inoperable Status Inputs						
Manual Controls						
Process						
Bypass indication algorithms						
Outputs						
Displays						