DS431 Design of Instrumentation and Control Systems for Nuclear Power Plants – compilation of comments
BEST PRINTED ON A3

COMMENTS BY REVIEWER								RESOLUTION			
No.	Member State	MS No.	Para/Line No.	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
363	PAK	12	Annex I and II 7	I		Sections as defined in the table of annexure may be made consistent with the guide, i.e. section 6 "Life cycle activities" is not present in the guide. This topic is covered in section 2 of the draft guide. Same may be modified in the comparison table II.1 and table II.2 of this guide.	Annexure should be compatible with the contents of the guide.	x			
294	USA	3	Figure1 1	Figure 1		Computer Security Impact Analysis of the planned I&C system.	The "Interactions with Computer Security Program" should include a process that correctly identifies the computer security consequences of the new or replacement I&C system being installed. A vulnerability assessment of a critical digital asset does not completely address this.	x			
342	USA	51	Table I-1 9	Table I-1		Add IEC 62566 to the list of standards and update Table I-2 accordingly.	IEC 62566 provides guidance for FPGAs.	x			
343	USA	52	Table I-1 9	Table I-1		Add IEEE Std 1012-2012 to the list of standards and update Table I-2 accordingly.	IEEE Std 1012-2012 provides guidance for system, software and hardware V&V.	x			
344	USA	53	Table I-1 9	Table I-1		Add IEC 60880, IEC 15288, and IEC 12207 and update Table I-2 accordingly.		x	60880 was already there		
1	CAN	1	General (AM)	0		Comment	Generally the document is very thorough and of high standards. However, we would have expected a section dealing with Analog to Digital Upgrades. Since we are moving from analog to digital systems for most of our I&C modifications, some guidelines would be beneficial.			x	The guidance of this document applies to I&C modernization, but the application to a specific project will be highly plant specific. I&C modernization topics are already deeply covered in IAEA and other documents. For example: NS-G-2.3 provides guidance on plant modifications; NS-G-2.12 provides guidance on management of ageing and obsolesce; TECDOC 1398 & IAEA Nuclear Energy

											Series NP-T-1.4 provides information specifically on modernization of I&C; IEC 62096 gives guidance on making modernization decisions.
2	CAN	2	General (RJH)	0		Comment	Overall, this is a good, comprehensive document providing suitable guidance for the design and implementation of I&C systems for Nuclear Power Plants.	x			
3	CAN	3	General (RJH)	0		Comment	The same topic is often discussed in several sections of the document. For example, diversity is discussed in sections 6.58 to 6.67, and in sections 4.40 to 4.47, section 9.60, et.al. The document could be tightened up and made more concise by eliminating this redundant coverage of topic areas.			x	Some topics are discussed in different contexts. For example, para 4.40-4.47 discusses diversity in the context of I&C architecture, 6.58-6.67 discuss it in the context of system integrity strategies. Paragraph 9.60 has been deleted as a result of other comments. There is no perfect organization of a document such as this, but it is believed that the current structure reasonably limits the duplication.
113	FIN	1	General	0		The updating and integrating the previous safety guides enhance the guidance related to I&C for nuclear power plants.		x			
114	FIN	2	General	0		DS367 lays down the IAEA safety classification requirements. The classification requirements should be based on the new guide. This new draft DS431 is not based on the new guide. The level of requirements should vary according the safety class; why to have different safety classes if requirements are the same for all classes?				x	DS367 is not yet stabilized; therefore, it is not advisable to base this document on a draft. The recommendations in DS431 do vary according to safety class. Most recommendations apply to items important to safety. This is consistent with the requirements of SSR-2/1 where most requirements apply to items important to safety. Many recommendations of DS-431 apply only to safety items. These cases are clearly indicated in the text.
127	FRA	1		0		Limit the guide to high level, justified, consistent principles.	The draft covers in deep technical details topics corresponding to multiple detailed standards such as general requirements for systems, software, HDL programmed devices, smart sensors, requirements for coping with common cause failures, control room, environmental qualification, etc.		OPEN ITEM		
128	FRA	2		0		Keep the level of detail consistent across the guide.	the level and the range of technical details are excessive for a high-level guide (and not enough if the target is low-level design standardization).		OPEN ITEM		
129	FRA	3		0		Refocus the guide on recommendations an transfer informative text either in footnote or in annexes.	The guide is sometimes too pedagogic…		OPEN ITEM	x	During the development of this guide discussion was held with member states regarding the utility of explanatory

											material. Small and newcomer countries universally felt that the explanatory material was helpful. Deeply experienced countries felt that it was not necessary, but except for this comment did not object to its inclusion. Moving material to and annex or footnotes would diminish its usefulness and impair the ability to convert the document to other forms, such as tracking databases.
130	FRA	4		0		Delete design details which have already been published in IEC or IEEE standards.	For example, clause 7.77 about deterministic response times provides three detailed software design items about processor interrupts, static allocation of resources, bounds of iterations in loops. Such items are already in published standards such as IEC 61513, IEC 62340 or IEC 60880, so there is no need to repeat these details in the guide. In addition, such standards provide many other items about the considered matter. It is not clear why only those 3 have been selected in the draft. For example, as we consider deterministic response times, items about scheduling (and many other ones) are as important as those 3.		OPEN ITEM	x	IAEA cannot assume that all Member States will use IEC standards and it is beyond our authority to recommend that they do. An attempt has been made to capture top level recommendations with the hope that these will be the entry point for use of national and international standards.
131	FRA	5		0		Limit the contents to recommendations and guidance to comply with the safety requirements. Do not mention nor require specific means such as specific designs or specific verification tools/methods. Let the designers demonstrate that their designs fulfil such recommendations/ guidance and the safety requirements.	The draft frequently discusses not only objectives but also compliance means: specific architectures and designs, and specific verification and assessment methods. As these detailed specific means are not necessarily commonly accepted, the current contents of the draft would need a large number of discussions (much more detailed and technical than what has been done yet) to reach a consensus		OPEN ITEM		
132	FRA	6		0			For example, clause 7.100 establishes an objective: “Communications (…) should have no detrimental safety effect on any safety division”. This is fine and sufficient, but additional clauses introduce means which are said acceptable or not. Clause 7.102 describes a means, said acceptable, which is in fact a communication protocol. Anyway, a protocol does not know what the		OPEN ITEM		

							communicated items are, and what they are used to. So, using this means does not guarantee that the communication cannot have a detrimental effect on a safety division. Thus the means said acceptable by the standard does not ensure the fulfilment of the objective established by the same standard. This inconsistency shows that the standard must not address means.					
133	FRA	7		0		Delete all occurrences of the new items which are not commonly accepted practices	New means have been introduced in this draft (for information or even within requirements), such as “reliability growth”, “statistical testing”, etc. which: • are not the commonly accepted practice • are not technically discussed in the draft • have scientific grounds which make them unfitted to nuclear safety applications, or no scientific grounds at all • can dangerously mislead the reader if used for safety purposes		OPEN ITEM		
134	FRA	8		0		Delete all sections related to some or one member states. (e.g. 2.89, 4.33, 4.34…)	The guide is supposed to reflect the consensus (section 1-1) but often mentions the practice in “some” member states, where “some” may be equal to one. By definition, such practices do not reflect a consensus, so they must not be part of the guide. It happens that “some” member states have a specific practice which is explicitly detailed in the draft while the practice of the other states is not even mentioned.		OPEN ITEM		
218	IEC	1	General	0		IEC/SC45A experts recommend that the controversial added items, weakening the consensual status of this document, be suppressed from the document and the possibility of development of a Technical Report to capture the different national practices on those controversial topics be considered by the Agency. See also the proposals in the following detailed comments.	IEC/SC45A experts acknowledged the work done by the IEA expert team which produced this draft and recognized the high quality of the draft. IEC/SC45A experts recognized that the majority of comments formulated on the previous version of DS431 circulated summer 2011 and discussed during the IAEA meeting held in Lyon in December 2011 was taken into account and thanked		OPEN ITEM		

							the IAEA expert team for that. IEC/SC45A experts noted that new recommendations linked to techniques, methods or technical positions which are not commonly used and recognized were introduced in this new draft, see the detailed comments here beneath. Paragraph 1.1 of the Safety Guide, reminds the reader that this Safety Guide reflects international best practice and **a consensus** that the recommended characteristics (or equivalent) should be achieved in the development of I&C systems.				
366	PAK	15	Table ITable II.2 Para 6.17 Para 6.190 Para 6.155 Para 6.161 I	0		Various typo errors have been observed which need to be corrected.		x	Not found. Perhaps already corrected.		
345	USA	1	General	0		The terms “computer security” and “cyber security” appear to be used interchangeably throughout the document. Suggest using only computer security.” The term “cyber security” is not defined in “Computer Security at Nuclear Facilities,” Nuclear Security Series No. 17, IAEA, Vienna (2011).	Clarification.	x			
135	FRA	9	1.1	1	1	~~It reflects international best practice and a consensus that the recommended characteristics (or equivalent) should be achieved in the development of I&C systems.~~	Superfluous. Furthermore, IAEA standards usually reflects good practices, not best practices	x			
293	USA	2	1.13, bullet 3 1	1	1=	Change “Hardware Definition Languages” to “Hardware description Languages”	HDL is the acronym for Hardware Description Language”. This definition is provided in the draft guide and on the internet.	x			
72	DEU	1	1.4, 6th bullet	1	4	Exchange the existing text: Data transport between systems important to safety among others with special	At this highlighted place (“main topic areas”) the SG should state the **general topic** ‘data transport between systems important to safety’. The second part of	x	Corrected English		

						requirements for cases where the system receiving data is of a higher category than the system sending data.	the proposed sentence deals with a special case of data transport between systems of different safety categories and expresses that in this case special requirements are to cope with. The DS 431 guidance should directed towards avoiding such cases where ever possible as well as to justify unavoidable exclusions.				
136	FRA	10	1.10	1	10	This Guide is a consensus of the recommendations of representatives of design, operating, construction organizations, and regulatory authorities from Member States with long experience in nuclear plants and knowledge of recent developments in I&C and safety technology.	Superfluous	x			
4	CAN	4	1.14 (RJH)	1	14	Consider including support features of I&C systems that are an important aspect of system performance (e.g. cooling and detection of cooling failure, UPS, grounding and shielding design, etc.)	Cooling and detection of cooling failure (e.g. fan failure) can have a major impact on reliability and the lifetime of electronics. Energy supply decisions (such as use of uninterruptible power supplies) can determine whether the I&C system will meet its safety mission requirements. Similarly, the grounding and shielding design and other conducted and radiated electromagnetic interference mitigation approaches (e.g. use of filters and opto-couplers) will determine whether the I&C system can perform adequately in a specific Nuclear Power Plant (NPP) environment.			x	Power supply, grounding, and field cableing are addressed in DS430. Supporting systems are to be covered in a new safety guide. The essential requirement that I&C systems impose on support systems are already given in SSR 2/1 requirement 27.
5	CAN	5	1.17 (RJH)	1	17	The list of examples could be extended to include: • Effluent monitoring (liquid and gas) (especially since the Cover Page states "for protecting people and the environment") • Fuel Handling	Completeness	x	Simplified and made i&C specific		
73	DEU	2	1.18	1	18	Proposal: … and the measures needed for I&C functions realized with PLDs.	Why is there a focus on HDL? There are different kind of modules available and are to be expected in future.			x	This guide makes use of industry consensus that has been established for PLD that are programmed using HDL (see for example IEC 62566). Similar consensus has not yet been documented for the broader range of PLD.
74	DEU	3	1.26	1	26	Proposal: … and certain technologies such as digital systems and devices realized with PLDs	Focus on HDL is not reasonable.			x	This guide makes use of industry consensus that has been established for PLD that are programmed using HDL (see for example IEC 62566). Similar consensus has not yet been documented for the broader range of PLD.
115	FIN	3	Chapter 2, Configuration	2		The configuration management has been handled well, however there are some findings such as:				x	Configuration management terminology was discussed in considerable detail during development of the guide. In the end it

Formatiert: Hervorheben

Formatiert: Hervorheben

Formatiert: Hervorheben

			management			The definitions “configuration item” and “baseline” are quite essential in configuration management, but they are now presented only very weakly in some subordinate clauses. Configuration item should be handled as a hierarchical term. Not only a single equipment or software is a configuration item. One should also handle I&C architecture and different systems as configuration items so that it is possible to identify the versions of architecture or systems.					was decided not to go to more depth here because CM is not specific to I&C, and because the terminology that is suggested for inclusion is not used in other IAEA documents.
116	FIN	4	Chapter 2., Hazard analysis	2	,	The requirement for making I&C systems hazard analysis during the design processes is good, but it may also be a good idea to analyse hazards related to interaction between I&C-systems in different defence levels of defence in depth concept. This is also a common notice for entire guide. Defence in depth concept should be taken more deeply into account. For example requirement “2.126. *The implementation of requirements that are not important to safety should be shown not to interfere with functions important to safety*” is not adequate itself, because functions important to safety belonging to different defence levels should not interfere with each other.	”		x	Added to the hazard analysis discussion “For the overall I&C architecture should be performed to identify conditions that might compromise the defence-in-depth strategy of the plant design.			
117	FIN	5	Chapter 2., V&V	2	,	There should be also (independent) assessment in the chapter handling verification and validation. Now terms are somehow confusing because verification and validation and independence are mixed omitting assessment. All phases of design process should be verified and validated, but verification is normally done by organisation itself and validation by customer. Of course there should be some level of independence in these steps because people					x	Independence of V&V is already discussed in paragraph 2.72-2.74. If the comment relates to QA for the V&V, that topic is in the domain of GS-R-3 and the supporting safety guides.

						tend to come blind to their own doings. All phases should by safety standards also be independently assessed. It is also normal to allow doing only one assessment to several phases, but assessment should cover all phases.					
156	FRA	30		2			This commonly accepted practice has been formalized in the nuclear standards, has been in use since the beginning of the 80's, and has produced adequate safety software. It is used not only in the nuclear domain, but also in other safety-critical domains such as avionics, space, etc.	x	2.16. In response to this situation, the nuclear power community as well as other safety critical domains such as aerospace have applied development processes that are commonly represented as life cycle models, which describe the activities for the development of electronic systems and the relationships between these activities. These commonly accepted practice has been formalized in nuclear standards that provide extensive guidance regarding processes for developing I&C systems. Normally, activities related to a given development step are grouped into the same phase.		
295	USA	4	Fig. 2 1	Fig. 2		Include an explanation for the arrow linking the Operation Life Cycle phase to the System Requirements life cycle phase that System Retirement is another means by which a system modification may be performed. See suggested Fig. 2 attached to this Comment matrix.	While not obvious, the Retirement life cycle phase is very important from the security and overall system configuration viewpoint. Over years of operation, operators become accustomed to the controls and operating characteristics of a control system. When the system is retired, consideration of how the operators will be transitioned into the new system must be factored into the new system's requirements. Further, retiring a system requires consideration of how the documentation for the system will be retired, and how the functionality of the remaining system will be affected.	x	Added replacement. The security implications of retirement will be covered in detail in the forthcoming I&C computer security document. Issues related to modification are already discussed in paragraphs 2.169 – 2.183 and safety guide NS-G-2.3.		
77	DEU	6	2.14/13 2.29/17	2	14/13	HDL (VHDL) should be defined adequately in whole text: hardware description languages (code? or program?) please refer to the source of the definition e.g. IEEE /Verilog/Verilog-AMS/SystemVerilog	Standartization of the definitions			X	HDL is already defined in the glossary using the definition given in IEC 62566
229	IEC	12	2.23 Figure 1	2	2.23	Typo: interactions with Cyber security Program	Typo	x			
79	DEU	8	2.27, Fig. 2	2	2.27	Box title: Installation and Commissioning	For completeness	x			

Formatiert: Hervorheben

78	DEU	7	2.23, Fig. 1, part Detailed design and implementation	2	2.23, Fig. 1, part Detailed design and implementation	a) Add at the right (under Interaction with Cyber Security program): Cyber Security Controls b) Change title of boxes: Software ~~lifecycle~~ design Hardware ~~lifecycle~~ design c) Complete the reference to chapters: Box Hardware design: (Sections 2, 6, 7)	To a) Cyber controls play a certain role in the detailed design To b) Wording To c) For completeness	x			
6	CAN	6	2.4 (RJH)	2	4	Include "qualification of staff"	A crucial aspect of the management system is for qualification of staff to be suitable for their assigned roles.			x	Paragraph 2.4 is a quote of SSR 2/1 and cannot be changed in this document.
75	DEU	4	After 2.4.	2	4.	Add a new par. under 2.4: The management systems should consider and utilize synergisms between safety and security measures and precautions.	Beside a possible negative impact as stated in 2.4 there are also synergisms between safety and security which should be considered and utilized. In this sense 2.4 (alone standing) is too negative concerning the relation of safety and security measures.			X	Paragraph 2.4 is a quote of SSR 2/1 and cannot be changed in this document. Therefore a additional paragraph (new under 2.4) is proposed which does not imply any change of SSR 2/1. Further reason for the comment: There are various ongoing activities addressing this aspect (IEC SC 45 A NWIP, branch specific guidelines (e.g. concerning Profinet), as well as national guidelines). Therefore this aspect should be addressed also in this IAEA safety guide on I&C.
7	CAN	7	2.6 (RJH)	2	6	Management systems should also include ongoing engineering programs (such as system performance monitoring, aging management, environmental qualification, etc.) as needed	This is needed so the I&C system will continue to meet its safety requirements.			x	See comment France 11
137	FRA	11	2.8	2	8	Each organization ~~Management systems should establish policies and objectives for all organizations involved~~ in I&C development activities should have a management system which is consistent with the expectations of the operating organization management system.	Clarification. Stress the importance of the licensee management system.	x			
364	PAK	13	2.10	2	10	Given reference for GS-G-3.1 is not correct. It may be [4] as mentioned in the references.		x			
8	CAN	8	2.11 (RJH)	2	11	Include reference to the tools and facilities (e.g. test rigs, HMI mock-ups, etc.) used in system integration and testing.	An important aspect of the development of I&C systems are the tools and facilities	x	Explicitly mentioned tools in the reference to products to be controlled. Since paragraph 2.11 is a list of topics of interest in GS-R-3, this discussion cannot		

Formatiert: Hervorheben

Formatiert: Unterstrichen

									go beyond what is in GS-R-3			
76	DEU	5	2.14, 1st bullet	2	14	… depends upon software ~~or~~ such as HDL code…	Code = SW	x				
9	CAN	9	2.15 (RJH)	2	15	An extensive testing regimen covering all system modes complemented by other formal analytical verification techniques are required. To make this practical, a graded approach must be applied.	A disciplined development process is a necessary condition for achieving correctness in a modern I&C system. However, it is not a sufficient condition.	x	Strengthened statement about the role of testing.			
138	FRA	12	2.16	2	16	~~In response to this situation, the nuclear power community has developed extensive guidance regarding processes for developing I&C systems.~~	Superfluous			x	Revised according to France 30	
139	FRA	13	2.19	2	19	Merge 2.19 with 2.18	Same topic	x				
140	FRA	14	2.21	2	21	Transform 2.21 as a footnote to the last bullet of 2.20	Explanatory note	x	Changed to note under the last bullet of 2.20. Footnotes are avoided in this document because it creates difficulty in exporting the text to other formats, e.g., requirements management tools or assessment databases such as the IAEA SARRP tool.			
296	USA	5	After After 2.24 (new 2.25) 2	2	24	Add: The computer security design requirements of I&C systems are one of many system requirements. Thus, security design must follow the same QA process as the other requirements of I&C systems.	Clarification.			x	Quality assurance is the domain of GS-R-3 and the supporting safety guides. Paragraphs 2.7 and 2.8 already make it clear that appropriate management systems (including QA) must be present for all activities related to design of I&C systems important to safety.	
80	DEU	9	2.27	2	27	Figure 2: Interaction between hardware and software design and between hardware and software implementation should be considered.		x				
230	IEC	13	2.27	2	27	V cycle shall include the phase of integration / commissioning before the operation, if not at least a non continuous line in place of the current line	IEC/SC45A experts noted that the V cycle representation shall include the phase of integration / commissioning with other I&C systems which is before the operation phase.			x	This figure was explicitly agreed by regulatory authorities from 10 member states. As not member state has requested a change it seems inappropriate to incorporate it at this point.	
10	CAN	10	2.29 (RJH)	2	29	Include other aspects of process planning such as: maintainability, obsolescence mitigation, and software maintenance/recovery.	Completeness	x				
141	FRA	15	2.29	2	29	Typically plans specific to I&C development will be prepared to deal with the topics* given below: ~~. Several topics may be combined into a single plan. The list below is not intended to represent a list of planning documents.~~ * Several topics may be combined into a single plan. The list below is not intended to represent a list of planning documents.	Simplification A footnote is enough to add explanatory note	x	Made a separate paragraph after the list. Footnotes are avoided in this document because it creates difficulty in exporting the text to other formats, e.g., requirements management tools or assessment databases such as the IAEA SARRP tool.			

297	USA	6	2.29 2	2	29	The sentence should be changed to state, "The list below is not intended to represent a complete list of planning documents.	The first paragraph of section 2.29 addresses plans for the development of I&C systems. The paragraph provides a list of topics that could be addressed in the plans. The last sentence of the first paragraph states, "The list below is not intended to represent a list of planning documents." This sentence appears to imply that the listed topics should not be included in the planning documents.	x	Deleted the phrase in question		
298	USA	7	2.32 / 5 2	2	32	…and computer security requirements, including a computer security impact assessment.	Clarification. This type of risk assessment is a key to understanding what computer security issues are posed by the introduction of the particular I&C system and as such should be included.			x	It is agreed that such an analysis should be performed, the statement is not meaningful without a description of such analysis. This should be included in the forthcoming IAEA document on computer security for I&C systems
11	CAN	11	2.34 (RJH)	2	34	Include other HFE-related aspects include context-based annunciation (to avoid flooding of messages during start-ups and transients) and I&C system fault reporting and maintainability.	Completeness	x			
12	CAN	12	2.35 (RJH)	2	35	Include response to annunciation messages, including time adequacy for credited operator actions.	Another HFE V&V aspect is response to annunciation messages, including time adequacy for credited operator actions.	x			
13	CAN	13	2.37 (RJH)	2	37	Further to just implementing cyber security measures, the I&C system architecture should proactively facilitate achievement of cyber security goals.	Completeness	x	Addressed by revision of paragraph 4.5. "4.5. The I&C architecture should satisfy the plant requirements, including system interfaces, performance requirements (e.g., timing and reliability), and facilitate achievement of cyber security goals."		
299	USA	8	2.39 / 2 2	2	39	…development environment with trustworthy personnel and/or vendors that meets the technical…	Personnel security is one of the critical elements of protecting the integrity of systems being developed. However, this section did not include this element.	x	Protection against insider threats is covered in IAEA NSS No. 8. A reference to this was added in paragraph 6.158. More is coming on development environments in the I&C computer security document.		
142	FRA	16	2.41	2	41	Transfer "IAEA TECDOC-1335, Ref. [25] provides more detailed discussion of configuration management." as a footnote	Tecdoc are not usually referenced	x	TECDOCS are referenced, but it is agreed that this particular one is weak.		
14	CAN	14	2.42 (RJH)	2	42	Other objectives should include: • Sustained conformance with the design basis • Consistency between the physical plant and the technical documentation • Facilitation in determining plant status conditions to enable implementation of work protection.	Completeness	x	Added the first two. The last bullet is unintellegible		
15	CAN	15	2.44	2	44	Included should be a software release discipline	To identify the specific software installed in	x	Added to 2.43		

			(RJH)				the plant.				
16	CAN	16	2.44 (RJH)	2	44	The software components should include a software maintenance/recovery plan.	Completeness			x	Addressed in paragraph 2.29. See Canada 10.
143	FRA	17	2.50	2	50	Merge 2.50 with 2.49	Same topic.			x	An effort has been made to clearly separate guidance from explanation. Combining the two paragraphs would violate this principle.
144	FRA	18	2.55	2	55	Merge 2.55 with 2.54	Same topic			x	An effort has been made to clearly separate guidance from explanation. Combining the two paragraphs would violate this principle.
145	FRA	19	2.57	2	57	Merge 2.57 with 2.56 : 2.56. The identity of software installed in I&C equipment and the values of configuration data should be retrievable from the I&C equipment <u>as</u> ~~. 2.57.~~ The ability to retrieve the identity of installed items and the values of configuration data support verification that the devices are properly configured. Automatic checking features or tools may assist this verification.	Same topic			x	An effort has been made to clearly separate guidance from explanation. Combining the two paragraphs would violate this principle.
146	FRA	20	2.58	2	58	Delete 2.58	Redundant with 2.56	x			
17	CAN	17	2.61 (RJH)	2	61	Common cause internal hazards should include excess humidity and temperature and electromagnetic interference (conducted and radiated).	Completeness			x	Internal and External hazards are described in other safety guides that are incorporated by reference. Rather than trying to make complete list of examples here all examples of such hazards were deleted.
353	PAK	2	2.63	2	63	Para 2.63 may be modified as “The hazard analysis should be updated during the design of the overall I&C architecture, and during the specification of requirements, design, implementation, installation, commissioning and modifications”.	It is expected that after hazard analysis design modifications may be expected, therefore it is proposed to rephrase the text accordingly.	x			
147	FRA	21	2.64	2	64	Merge 2.64 with 2.63	Same topic			x	An effort has been made to clearly separate guidance from explanation. Combining the two paragraphs would violate this principle.
148	FRA	22	2.66	2	66	Merge 2.66 with 2.65	Same topic			x	An effort has been made to clearly separate guidance from explanation. Combining the two paragraphs would violate this principle.
149	FRA	23	2.67	2	67	Merge 2.67 and 2.68: 2.67. <u>As</u> Each phase of an I&C development process uses information developed in earlier phases, and provides results to be used as the input for later phases, ~~. 2.68.~~ The results of	Same topic.			x	An effort has been made to clearly separate guidance from explanation. Combining the two paragraphs would violate this principle.

						each life cycle phase should be verified against the requirements set by the previous phases.					
18	CAN	18	2.70 (RJH)	2	70	Allowance should be made for crediting the qualification of proven items based on wide-usage in a similar application.	Wider applicability			x	This section does not deal with qualification. The recommendations for functional qualification are given in paragraphs 6.82 to 6.99 and include the possibility of considering operating experience.
150	FRA	24	2.71	2	71	Transform 2.71 in a footnote of 2.70 2.70. Each item* of I&C should be validated to confirm it implements all requirements (both functional and non-functional), and to investigate for the existence of behaviour that is not required (see paragraphs 2.134 to 2.149). ~~2.71.~~ *Note that the term 'item' used as above includes I&C components and software. This includes software modules, integrated software, firmware, integrated software and hardware, and HDL code and associated software etc.	Explanatory note			x	Footnotes are avoided in this document because it creates difficulty in exporting the text to other formats, e.g., requirements management tools or assessment databases such as the IAEA SARRP tool.
219	IEC	2	2.71	2	71	Reformulate the 2.70 and 2.71 using "component" of SCCs concept. IEC/SC45A experts propose to integrate in the glossary of this safety guide the following definition and to have it taken into account for the next revision of the IAEA safety glossary. Component: One of the parts that make up a system. A component may be hardware or software and may be subdivided into other components NOTE - The terms "equipment", "component", and "module" are often used interchangeably. The relationship of these terms is not yet standardised.	IEC/SC45A experts thought that the use of a limited number of terms well defined in the IAEA safety glossary will improve the quality of the document and facilitate its understanding and limit the interpretations. So definition of SCC, has to indicate explicitly that components are not only hardware but also software and "component" has to be used here.	x			
19	CAN	19	2.73 (RJH)	2	73	However, once established, the V&V budget and schedule should not be able to be compromised by pressure from the design organization.	The V&V teams cannot practically set their own budget or schedule or project chaos would likely ensue.	x			
151	FRA	25	2.73	2	73	Merge 2.73 and 2.72	Same topic			x	Footnotes are avoided in this document because it creates difficulty in exporting the text to other formats, e.g., requirements management tools or assessment databases

												such as the IAEA SARRP tool.
152	FRA	26	2.73	2	73	~~can set their own budget or schedule,~~		x	See Canada 19			
153	FRA	27	2.75	2	75	Delete 2.75	To be consistent with deletion proposed in 2.73	x				
20	CAN	20	2.77 (RJH)	2	77	The record of V&V activities should include results and the disposition of detected anomalies.	Completeness	x				
154	FRA	28	2.77	2	77	Locate 2.77 before 2.76	2.76 is a subset of 2.77	x				
155	FRA	29	2.83 to 2.91	2	83	Delete clauses 2.83 to 2.91 and all clauses which associate numerical values with software reliability or with CCFs due to software errors.	The new draft emphasises numerical reliability, for digital systems and components, including software. A whole section has been introduced on this topic (2.81 to 2.91), but it appears also in other places. Numerical reliability is not an accepted practice for software. Only the random failures of hardware (due to wear and tear) may be modelled by statistics. The logic (software or contents of HDL programmed devices) is a mathematical relationship between inputs, outputs and time. This relationship is either right or wrong and remains such: it does not “fail”. Software reliability is qualitative, not quantitative. The requirements for reliability figures at system level are translated at software level into design requirements (such as deterministic behaviour, proven independence regarding everything which is not a required input, etc.) and process requirements (such as independent verification). This commonly accepted practice has been formalized in the nuclear standards, has been in use since the beginning of the 80’s, and has produced adequate safety software. It is used not only in the nuclear domain, but also in other safety-critical domains such as avionics, space, etc.		OPEN ITEM			
81	DEU	10	2.84, 4th and 5th bullet	2	84	To both bullets add: Applicable on hardwired I&C only	Quantitative methods are not state of the art in safety assessment of SW-based I&C in the nuclear field.		OPEN ITEM			important
220	IEC	3	2.84	2	84	Delete the item “Reliability testing. Reliability testing usually involves statistical	IEC/SC45A experts noted that “reliability testing that involves statistical tests and		OPEN ITEM			

						tests and might be combined with the use of reliability growth techniques."	might be combined with the use of reliability growth techniques" are not widely recognised techniques. Such techniques have been used only in a small number of nuclear projects. In the IEC/SC45A frame, IEC/SC45A 61513 (6.2.4.2.2) requires a reliability assessment to be performed, whose rigor depends on the system's safety class. IEC 61513 requires that an appropriate mix of quantitative (hardware) and qualitative (software) methods be used to evaluate the system's reliability. However it does not prescribe a specific mean. IEC/SC45A experts think that this guide should not focus on means but on ends. Reliability testing is a mean which can be used for the reliability evaluation but it is not the only one and the guide should not be focused on it.				
221	IEC	4	2.87	2	87	Delete 2.87	IEC/SC45A experts noted that "Reliability model" is not defined in the document and paragraph 2.88 is sufficient and clearer.		OPEN ITEM		
82	DEU	11	2.89	2	89	Give reference or theoretical evidence for such figures or (better) rephrase the paragraph without such figures.	There is no reference to the provided reliability figures; IEC 61226 contains another (agreed) limit according to which the safety demonstration for a SW-based I&C function can be treated as acceptable.		OPEN ITEM		Important!
222	IEC	5	2.89	2	89	Delete 2.89	IEC/SC45A experts noted that the given examples emphasis the singular practices of only 2 member states. Typically such examples weaken the consensual character of the Safety guide.		OPEN ITEM		
157	FRA	31	2.92	2	92	Delete c)	I&C documents are not aimed at operators (or combine c) and d))	x	Changed to operating personnel in conformance with definition in IAEA safety glossary.		
223	IEC	6	2.92 e)	2	92	To be replaced by e) Be traceable throughout the I&C life cycle phases.	IEC/SC45A experts noted that a) states that I&C documentation should allow communication during the design process. While e) says that it should be traceable back to design documentation. As such this is confusing.	x			
158	FRA	32	2.94	2	94	The operating organization should establish	The licensee is responsible.	x			

						or be provided with documentation for I&C					
300	USA	9	2.94q / 3 2	2	94q	…and practices (including computer security), these are to be…	Clarification.	x			
159	FRA	33	2.97	2	97	Requirements specifications for the overall I&C and each individual I&C system should be derived from the I&C design basis ~~and the recommendations given in this guide~~.	Superfluous	x			
224	IEC	7	2.97	2	97	"Requirements specifications for the overall I&C and each individual I&C system should be derived from the I&C design basis and the recommendations given in this guide." To be replaced by: "Requirements specifications for the Overall I&C should be derived from the Plant design basis and the recommendations given in this guide. They constitute the I&C design basis. Requirements specifications for each individual I&C system should be derived from the I&C design basis and the Overall I&C architecture design documentation."	IEC/SC45A experts formulated a question about whether "I&C design basis" is the requirements specification, as according to section 3 it includes all the requirements on Overall I&C. Requirements on Overall I&C are not derived from the design of the Overall I&C. The Overall I&C requirements specification shall be an input for the design of the Overall I&C.			x	Requirements specifications are much more detailed that the design basis. Furthermore there are many levels of requirements specifications that fit below the design basis. They all should respond to design basis requirements.
21	CAN	21	2.99 (RJH)	2	99	The specifications should also include timing requirements: speed of the required action and duration.	Completeness			x	This is already given in paragraph 2.101.d.
225	IEC	8	2.99	2	99	Modify as follows "System Requirements Specification should define what each individual I&C system is to do." (deletion of "~~and the failure mode that are to be avoided~~")	The last part of the sentence implies that the system requirements specification shall define what the system shall not do. IEC/SC45A experts thought that such kind of specification should be avoided because completeness is impossible (it will be impossible to define all failure modes that should be avoided). Moreover, such requirements are very difficult (and most of the times impossible) to test. It is difficult to set up a test case to very that the failure modes are indeed avoided.	x	Changed to "failure modes that would be contradictory to safety analysis assumptions." For example, many safety analyses assume that the worst case for a rod withdrawal accident is uncontrolled withdrawal of one bank. In this case, failures of the rod control system must not result in withdrawal of multiple banks. If this is stated, design provisions can be made to prevent such a failure.		
160	FRA	34	2.100	2	100	Locate 2.100 after 2.96	More logical place as it is a governing principle when defining requirements	x	Located after 2.97		
22	CAN	22	2.101 (RJH)	2	101	Self-supervision features should include input rationality checking and important independent safe-state devices such as watchdog timers.	Wider applicability			x	Covered already in paragraphs 6.70, 785, 7.86.
161	FRA	35	2.101	2	101	Merge 2.101 with 2.99	Both paragraphs address system requirements			x	An effort has been made to limit each normative paragraph to one recommendation in order to facilitate traceability. Combining the two paragraphs would violate this principle.

301	USA	10	2.101f / 1 2	2	101f	Security features (such as validity checks, access privileges, specific computer security controls, and features that allow systems to inherit the security controls in their environments)	Clarification. Applicable computer security controls are integral to the security posture of a given I&C system with an associated critical digital asset. As such this feature should be highlighted.	x				
162	FRA	36	2.102	2	102	Merge 2.102 with 2.101 h)	Same topic			x	The text of paragraph 2.102 does not fit with the introduction to 2.101. Hence a separate paragraph is needed.	
163	FRA	37	2.103	2	103	~~Requirements Engineering~~ Specific processes should be used	Avoid too specific term	x	Rephrased for clarity			
226	IEC	9	2.103	2	103	« to ensure that all requirements are fulfilled, verified, implemented, and tested. » To be replaced by: « to ensure that all requirements are for instance verified, implemented, and fulfilled (tested if the validation mean is a test) »	IEC/SC45A experts noted that test is not the only means to ensure that a requirement is fulfilled. Analyses are performed too.	x				
164	FRA	38	2.104 to 2.106	2	104	Delete 2.104 to 2.106	Too vague or too much detailed			x	Paragraph 2.104 changed to an example. Reason for the comment is self contradictory.	
165	FRA	39	2.109	2	109	Merge 2.109 and 2.108	Same topic			x	An effort has been made to limit each normative paragraph to one recommendation in order to facilitate traceability. Combining the two paragraphs would violate this principle.	
166	FRA	40	2.111	2	111	Merge 2.111 with 2.107	Same topic			x	Paragraphs actually deal with different topics.	
227	IEC	10	2.111	2	111	To be replaced by “Safety requirements are requirements that have a potential impact on safety. They should be identified.”	IEC/SC45A experts noted that due to the rephrasing in revision G (different from D), what is considered a safety requirement, as opposed to non safety ones, should be clarified.	x	Rephrased for simplicity.			
167	FRA	41	2.112 2.113	2	112	Combine 2.112 and 2.113 as followed, with some modifications: 2.112 If Pre-developed items are ~~often~~ used in the implementation of I&C systems, they should be appropriately qualified. Pre-developed items might be hardware devices, pre-developed software (PDS), commercial off the shelf (COTS) devices, digital devices composed of both hardware and software, hardware devices configured with hardware definition language or pre-developed functional blocks usable in a HDL description. ~~2.113. Pre-developed items should be~~	Don’t encourage use of COTS, clarify the need for adequate qualification.	x				

						~~qualified in accordance with the guidance given in 6.82 through 6.138.~~					
168	FRA	42	2.114 2.115	2	114	Delete 2.114 and 2.115	Superfluous	x			
23	CAN	23	2.116 (RJH)	2	116	Where feasible, unused functions of a pre-developed item should be disabled .	To optimize system simplicity.	x	2.116a. Where feasible, pre-developed items should be configured such that unused functions are disabled		
169	FRA	43	2.117 2.118	2	117	Transform 2.117 and 2.118 as footnote related to 2.112 (where COTS are mentioned)	Information (not recommandations)			x	Footnotes are avoided in this document because it creates difficulty in exporting the text to other formats, e.g., requirements management tools or assessment databases such as the IAEA SARRP tool.
24	CAN	24	2.118 (RJH)	2	118	Consider partial credit towards qualification through demonstrated usage of a COTS device in a similar context.	Demonstrated usage of a COTS device in a similar context should merit at least partial credit towards qualification.			x	This concept is already addressed in the recommendations for functional qualification are given in paragraphs 6.82 to 6.99 and include the possibility of considering operating experience.
25	CAN	25	2.119 (RJH)	2	119	Consider purchase of lifetime spares of a specific version	This could be one strategy to maintain lifetime qualification of a COTS	x			
170	FRA	44	2.119	2	119	Split 2.119 in a recommendation and a footnote as follows: 2.119 In the process of deciding whether to use COTS devices or not, the licensee should pay attention to ~~An important consideration when using COTS devices is~~ the maintenance of their qualification during the plant lifetime*. *There might, for example, be frequent design changes of the product line such as, changes to subcomponents, new firmware versions, new manufacturing processes, or new software versions. This may cause challenges to the vendor as well as the plant configuration management in order to properly identify such modifications especially with regard to I&C maintenance and spare parts management.	Clarification	x	Footnotes are avoided in this document because it creates difficulty in exporting the text to other formats, e.g., requirements management tools or assessment databases such as the IAEA SARRP tool.		
171	FRA	45	2.121	2	121	Transform 2.121 into a footnote to 2.112	Not a recommendation	x	Moved. Footnotes are avoided in this document because it creates difficulty in exporting the text to other formats, e.g., requirements management tools or assessment databases such as the IAEA SARRP tool		
172	FRA	46	2.123	2	123	Transform 2.123 into a footnote to 2.122	Information			x	Footnotes are avoided in this document because it creates difficulty in exporting

											the text to other formats, e.g., requirements management tools or assessment databases such as the IAEA SARRP tool
173	FRA	47	2.124 2.125	2	124	Delete 2.124 and 2.125	Superfluous	x	Deleted 2.124. Combined 2.125 with 2.123. The information seems useful.		
174	FRA	48	2.129 2.130	2	129	Merge 2.129 and 2.130 with 2.130 modified as follows: ~~It is advisable to use~~ software tools may be used to control the issue of modules for assembly into system components and to control the build used for system validation and for on-site use in operation to facilitate configuration control and traceability ~~can be established~~ between installed components and validated components.	Same topic Offer flexibility on the use of software tools.	x	The flexibility was already there, nevertheless, the paragraph was further weakened. The paragraphs were not combined. An effort has been made to clearly separate guidance from explanation. Combining the two paragraphs would violate this principle		
175	FRA	49	2.131	2	131	Locate 2.131 before 2.129	2.131 defines system integration, which is discussed in 2.129+2.130	x			
176	FRA	50	2.132	2	132	Delete 2.132	Information only	x			
177	FRA	51	2.135	2	135	Delete 2.135	Implicit considering 2.134	x			
26	CAN	26	2.136 (RJH)	2	136	Final validation may require waiting for the plant to start-up and progress to full-power operation.	It may not be feasible to complete system validation as soon as the system is installed in the plant.			x	Some aspects of I&C cannot be fully tested until hot functional tests, initial startup, or even during initial full power operation. This is part of commissioning and the plant operation must be carefully specified to ensure the unknowns going into the activities do not pose a risk to continued fulfillment of critical safety functions. Consequently, these tests are not the domain of I&C engineers – although I&C does need to be involved. The end of validation should be specified at some point. In working sessions of the writing group and in working sessions of the MDEP Digital I&C Working Group the decision was to consider validation complete before commissioning otherwise it leaves the implication the plant is being started up when the I&C has not been sufficiently validated
178	FRA	62	2.136	2	136	Some additional elements of system validation ~~will~~ may be performed after the system is installed in the plant.		x	Changed as requested although I don't understand how the performance of the neutron instrumentation system can be validated before there are neutrons		
179	FRA	53	2.138	2	138	Merge 2.138 with 2.137	Same topic			x	An effort has been made to limit each normative paragraph to one recommendation in order to facilitate traceability. Combining the two

											paragraphs would violate this principle.
180	FRA	54	2.143	2	143	Merge 2.143 with 2.141	Same topic			x	An effort has been made to limit each normative paragraph to one recommendation in order to facilitate traceability. Combining the two paragraphs would violate this principle.
83	DEU	12	2.144	2	144	Rephrased text: Statistical testing may provide additional confidence …	Quantitative methods are not state of the art in safety assessment of SW-based I&C in the nuclear field.		OPEN ITEM		important
228	IEC	11	2.144	2	144	Delete 2.144	IEC/SC45A experts noted that "statistical testing" is not a widely recognised technique. Such technique has been used only in a small number of nuclear projects.		OPEN ITEM		
181	FRA	55	2.146	2	146	Merge 2.146 with 2.142	Same topic			x	An effort has been made to limit each normative paragraph to one recommendation in order to facilitate traceability. Combining the two paragraphs would violate this principle.
182	FRA	56	2.147	2	147	Delete 2.147	Superfluous	x			
354	PAK	3	2.151	2	151	It may be modified as "Equipment receipt inspection, installation, pre-commissioning or commissioning tests should verify that the system has not suffered damage during transportation".	The term pre-commissioning may be replaced with installation, as it is more common and in line with the terminology used by IAEA such as SSG-12.	x	Used term construction. The intent was to refer to tests that occur prior to turnover for commissioning (e.g., calibration, grooming, and alignment).		
183	FRA	57	2.152	2	152	Delete `2	Also true, superfluous 2.153 is enough	x			
184	FRA	58	2.155	2	155	Merge 2.155 with 2.157	Same topic			x	An effort has been made to clearly separate guidance from explanation. Combining the two paragraphs would violate this principle.
27	CAN	27	2.156 (RJH)	2	156	Supplementary analysis should be applied to address the gap, where testing some aspect of an I&C system/plant integration is not feasible,	Testing some aspect of an I&C system/plant integration may not be feasible,			x	Some aspects of I&C cannot be fully tested until hot functional tests, initial startup, or even during initial full power operation. This is part of commissioning and the plant operation must be carefully specified to ensure the unknowns going into the activities do not pose a risk to continued fulfillment of critical safety functions. Consequently, these tests are not the domain of I&C engineers – although I&C does need to be involved. The end of validation should be specified at some point. In working sessions of the writing group and in working sessions of the MDEP Digital I&C Working Group the

											decision was to consider validation complete before commissioning otherwise it leaves the implication the plant is being started up when the I&C has not been sufficiently validated
185	FRA	59	2.161 2.162	2	161	Delete 2.161 and 2.162	Also true, superfluous 2.163 is enough	x			
186	FRA	60	2.164	2	164	Changes to I&C system parameters should be undertaken using appropriate means and facilities ~~that have been shown to be fit for the purpose~~.	Clarification	x			
187	FRA	61	2.165	2	165		???	x			Clarified, but there is no way to judge if the comment is resolved
188	FRA	62	2.167 2.168	2	167	Delete 2.167 and 2.168	Also true, superfluous 2.169 is enough	x	.		
302	USA	11	2.167 – 2.183 2	2	167	In Modifications section, address control of design information for discarded systems design information.	In discussing modifications, there should be guidance for what is done with the replaced system to limit access to the discarded system's design features. The discarded system may be installed in other facilities. If the design details are not protected, a cyber attacker may be able to reverse-engineer the system to identify vulnerabilities that could be exploited in facilities that continue to use the system.			x	The security implications of retirement will be covered in detail in the forthcoming I&C computer security document.
189	FRA	63	2.170	2	170	Delete 2.170	Not specific to I&C	x			
190	FRA	64	2.171 c)	2	171	Practical considerations with respect to the equipment or technology commercially available ~~when required by the project programme~~, and the prospects for securing support of such equipment and technology by manufactures or third parties for the installed life of the equipment, and	Superfluous	x			
191	FRA	65	2.173	2	173	Merge 2.173 with 2.172	Same topic			x	An effort has been made to limit each normative paragraph to one recommendation in order to facilitate traceability. Combining the two paragraphs would violate this principle.
192	FRA	66	2.176	2	176	Merge 2.176 with 2.175	Same topic			x	An effort has been made to clearly separate guidance from explanation. Combining the two paragraphs would violate this principle.
193	FRA	67	2.177	2	177	Delete 2.177	Superfluous	x			
28	CAN	28	2.178 (RJH)	2	178	Include the fact that enhancements to the operator interface should precipitate incremental training.	Completeness	x			

						were necessary.					
194	FRA	68	2.178	2	178	Transform 2.178 as a footnote to 2.179 (HFE analysis)		x	Merged the two paragraphs. Footnotes are avoided in this document because it creates difficulty in exporting the text to other formats, e.g., requirements management tools or assessment databases such as the IAEA SARRP tool		
195	FRA	69	2.180	2	180	in the adequacy of the new system ~~should~~ may be considered as a part of the validation process.	To allow flexibility, considering 2.181	x			
196	FRA	70	2.181	2	181	Merge 2.181 with 2.180	Same topic			x	An effort has been made to clearly separate guidance from explanation. Combining the two paragraphs would violate this principle.
197	FRA	71	2.182	2	182	Transform 2.182 as a footnote to 2.180	Information only	x	Merged with 1.180. Footnotes are avoided in this document because it creates difficulty in exporting the text to other formats, e.g., requirements management tools or assessment databases such as the IAEA SARRP tool		
118	FIN	6	Chapter 3., Content of I&C design bases	3	,	There is now requirements in the chapter ”content of I&C design bases” for the definition of failure modes of I&C. However it is impossible to design and analyse the plant without defined failure modes and behaviour.				x	Section 3 does not deal with failure modes but does deal with failure characteristic.
352	PAK	1	Figure 1 and Figure 2	Figure 1 and Figure 2		Configuration control may be made part of I&C life cycle process as referred in figures.	Since verification and validation starts from the design and ends at the installation phase and system may be modified after V&V; therefore, it is proposed that configuration Control may be made part of flow diagrams as mentioned in Figures.			x	Configuration control is already discussed as one of several activities that are common to all life cycle phases. Adding CM (and the other common activities) to the figures would make them very complicated and detract from the main purpose which is to illustrate the relationship of the life cycle phases.
198	FRA	72	3.4	3	4	Delete 3.4	Superfluous	x			
199	FRA	73	3.6	3	6	Merge 3.6 with 3.5	Same topic			x	An effort has been made to clearly separate guidance from explanation. Combining the two paragraphs would violate this principle.
200	FRA	74	3.7 bullet list	3	7	Inverse last two bullets	Mitigation is also applicable to DEC	x			

201	FRA	75	3.11	3	11	Transform 3.11,as modified, into a footnote to 3.10: The overall I&C architecture is the organizational structure of the plant I&C systems. The overall I&C architecture of a nuclear power plant includes multiple I&C systems, each playing specific roles. ~~Each I&C system within the overall I&C architecture will be designed to meet its design basis, which consists of a defined set of requirements.~~	Informative		x	Modified text but did ot transform to footnote. Footnotes are avoided in this document because it creates difficulty in exporting the text to other formats, e.g., requirements management tools or assessment databases such as the IAEA SARRP tool		
231	IEC	14	3.12	3	12	Add a reference to paragraphs 5.8 to 5.12.	Classification scheme need to be explained to avoid misunderstandings.		x	Revised to say " This information will then be used to allocate functions to each I&C system and to identify the safety classification of I&C systems." Reference to the classification scheme in this guide was inappropriate as it is recognized that users will classify according to their own scheme.		
202	FRA	76	3.13	3	13	Transform 3.13 in a footnote to 3.12	Information only				x	Footnotes are avoided in this document because it creates difficulty in exporting the text to other formats, e.g., requirements management tools or assessment databases such as the IAEA SARRP tool
203	FRA	77	3.14 bullet list	3	14	Merge j, l and m	All relate to operation				x	An effort has been made to limit each normative paragraph to one recommendation in order to facilitate traceability. Combining the two paragraphs would violate this principle.
303	USA	12	3.14h / 1 3	3	14h	Computer security vulnerability assessments and impact analyses	The vulnerability assessment only addresses part of the overall computer security issue. The impact analysis addresses potential gains in security posture as well as possible changes to current security controls, technologies, and efforts. "Cyber security" was changed to "computer security" for consistency and message broadening.		x			
84	DEU	13	3.15 b.3, lines 2 to 4	3	15	Change the text to: System and component reliability and availability limits should be specified ~~using probabilistic criteria,~~ using qualitative deterministic criteria (e.g., compliance with single failure criterion or specific procedures and verification methods for	Quantitative methods are not state of the art in safety assessment of SW-based I&C in the nuclear field.		x	Rephrased for clarity and to more accurately convey the understood intent of the comment.		To which text the par. is rephrased?

						software~~), or both.~~ Some member states use quantitative system and component reliability and availability criteria.					
204	FRA	78	3.15 c 2.	3	15	~~Nuclear power plants will have physical protection, including access control to I&C systems, and computer security plans which impose constraints on design and operation of the I&C system~~	Superfluous	x			
232	IEC	15	3.15, 7.76, 7.77, 7.81, 7.82, 7.83, 7.95, 7.142, 7.143, 9.33	3	15	Add a definition for determinism to the glossary of this SG and funnel it to the IAEA Safety Glossary revision. IEC/SC45A expert propose the following definition to considered : **Determinism:** Principle by which the order of facts perfectly defines the conditions for existence of a phenomenon such that the phenomenon must occur if these conditions are satisfied. NOTE 1 : A deterministic behaviour fulfils this principle. The level at which the principle is applied is very important , because for example a system which has a deterministic behaviour at function and timing level can be not at all a system having a deterministic behaviour strictly speaking (for example a computer based system using a general purpose operating system sufficiently complex for the user is not capable to sufficiently characterized the execution context to be sure to know it exactly). **Predictability:** Principle according to which the behaviour of software or a programmed system with regard to its environment can be determined using a model. NOTE 1: A predictable behaviour fulfils this principle. NOTE 2: See also “Determinism”.	IEC/SC45A experts noted that the term “deterministic” is used 10 times in this Safety Guide and is also used in SSR 2/1 5.34, a definition is a need for “deterministic” The IAEA safety glossary contains two definitions for deterministic analysis and deterministic effect which are not directly related to the concepts used in this safety guide. For those terms deterministic is opposed to probabilistic. If we are more precise about what is determinism a definition for predictable can be useful.	x			
305	USA	14	3.15.d	3	15.d	Insert “3.15.d 8. The equipment protective	Limitations of equipment preventing	x			

			(Design Basis) 3			provisions that could prevent the safety systems from accomplishing their safety functions."	safety functions to be performed are a realistic constraint. "Limitations on materials to be used" is identified, 3.15.d.5, but this should not be the same.				
304	USA	13	3.15.b.3 3	3	15.b.3	"Subject to Member State policy, system and component reliability and availability limits may be specified using probabilistic criteria, deterministic criteria (e.g., compliance with single failure criterion or specific procedures and verification methods for software), or both."	The guidance states, "System and component reliability and availability limits may be specified using probabilistic criteria, deterministic criteria (e.g., compliance with single failure criterion or specific procedures and verification methods for software), or both." Some member states may not accept the use of probabilistic criteria for accepting safety systems.	x			
233	IEC	16	3.16	3	16	Modify "In any case it is essential that the design bases for the overall I&C **and for the individual** systems be consistent with each other (...). "	IEC/SC45A experts noted that a clarification is needed.	x			
29	CAN	29	3.17 (RJH)	3	17	Also included should be the conditions which must be satisfied before an actuated protective system can be reset.	Completeness	x			
205	FRA	79	3.17 d	3	17	~~Reactors that have short operating cycles (e.g., less than 90 days) may not need Maintenance bypasses.~~ ~~Both maintenance and operational bypasses need to be taken into account (see paragraphs .13, 6.180, and 7.37 – 7.41).~~	Superfluous	x			
346	CHW	1	2.42, first point	Figure 1 and Figure 2	42	To identify all items under configuration management, i.e. **documents**, products and associated records .	The term documents was missing. Should be the same as in Para 2.41.	x			
119	FIN	7	Chapter 4., Common cause failure	4	,	It is not taken into account in chapter "consideration of common cause failure" that software based system can generate also spurious actions. Other defence lines should be capable to bring the plant to the controlled state in this kind of incidents.		x	Added errors in development tools to the examples of CCF causes given in paragraph 4.27		

30	CAN	30	4.1 (RJH)	4	1	A defined design strategy should be used for partitioning, such as “separation of concerns” or “information hiding” to minimize system complexity and to restrict unnecessary interactions between individual I&C system elements. Strong consideration of timing constraints must factor in to the system partitioning decisions.	The overall I&C architecture should result from a systematic, step-wise decomposition of required functionality plus other requirements.	x	Systematic approach wording added as paragraph 2.120a. Paragraph 4.5 discusses timing. Information hiding seems to be more a software architecture concern and is addressed in section 9.		
85	DEU	14	4.1, last bullet, 3rd line	4	1	… signal connections such as the status …	Wording			x	See France 80
206	FRA	80	4.1	4	1	~~Communications include, for example: analogue signal connections such as a 4 to 20 mA signal, single bit signal connections such status of a switch contact, and digital data communications such as a serial data link or data communications over a digital data network.~~	Superfluous	x			OK
234	IEC	17	4.1.	4	1.	Could be replaced by: “the interfaces between these systems”	IEC/SC45A experts noted that the meaning of « the hierarchical structure of these systems » is unclear	x	Changed to tiered structure. It is more than just interfaces, but overall organization.		
31	CAN	31	4.4 (RJH)	4	4	Software modules performing similar functions should have a consistent structure.	To increase the coherency and understandability of the I&C system architecture,	x	Added as paragraph 9.29a. Section 4 deals with system architecture not software.		
207	FRA	81	4.5	4	5	Locate 4.5 after 4.2	More logical place.	x	The paragraph is meant to apply to both overall architecture and individual system architecture. This has been clarified.		
208	FRA	82	4.7	4	7	Delete 4.7 or transform it as a footnote				x	The cross reference is useful. Footnotes are avoided in this document because it creates difficulty in exporting the text to other formats, e.g., requirements management tools or assessment databases such as the IAEA SARRP tool
209	FRA	83	4.8 4.9 4.10	4	8	Merge 4.8 and 4.9 and locate {4.8+4.9} and 4.10 paragraph before 4.2.	Same topic More logical location			x	An effort has been made to limit each normative paragraph to one recommendation in order to facilitate traceability. Combining the two paragraphs would violate this principle. The three referenced paragraphs respond to SSR-2/1 requirement 7 which is explained in paragraph 4.6. Therefore, they logically should come after the statement of the requirement.
86	DEU	15	4.10	4	10	Defence-in-depth within the overall I&C architecture is achieved through a combination of redundancy (both within systems and across systems), physical	Not only one attribute is sufficient but at least several. Diversity should be considered in general and not only certain types of it.	x	Also changed functional diversity to functional independence and did inot include statement about achievement of safety goals. Paragraphs 4.30 – 4.39		OK

						segregation, independence, ~~functional diversity and design~~ diversity. The required achievement of safety goals by implementation of diversity measures hast to be analyzed adequately.			already cover the need to demonstrate that design bases are achieved.		
32	CAN	32	4.11 .b (RJH)	4	11	Determination and implementation of safe states and a mechanism (such as “heartbeats”) should be considered for confirming that I&C system elements remain active and functional.	For consistency of application and for confirming that I&C system elements remain active and functional			x	This section deals with architecture, not fail safe design. Paragraphs 6.69 to 6.80 already cover fail safe design
235	IEC	18	4.11 a.	4	11	“Include” could be replaced by “allocate”	IEC/SC45A experts noted that the wording is not clear here: “The overall I&C architecture should: a. Include all I&C functions needed to fulfil the plant design basis »			x	Architecture cannot allocate as it is not capable of decision making.
236	IEC	19	4.11b, g,h,i	4	11b	To be deleted	IEC/SC45A experts noted that it is too detailed			x	No technical justification is provided
210	FRA	84	4.12	4	12	~~Economics will generally encourage minimizing the number of different platforms used~~.	Not a safety consideration	x			
211	FRA	85	4.13 b	4	13	Systems of lower safety class ~~typically do~~ may not need to have redundant elements for reasons of nuclear safety,	Not so true…	x			
33	CAN	33	4.14 (RJH)	4	14	It is not clear what is intended here, and whether a graded approach should be applied.	There are many possible types and degrees of independence (e.g. physical independence, logical independence, electrical isolation, etc.).			x	Graded approach is not mentioned here. The paragraph means what it say. It introduces the rationale for the section. No change was proposed.
34	CAN	34	4.17 (GR)	4	17	Safety systems should be independent from systems of lower safety classification including all their components from sensors to the final actuation	“Safety systems should be independent from systems of lower safety classification” Comment: This statement does not explicitly mention the components in the train.			x	Since the components of a system are part of a system the concept follows directly from the existing statement.
237	IEC	20	4.18	4	18	Delete or define what “elements” means. Some interpretations of “elements” would for example, lead to forbid signal exchange for voting	IEC/SC45A experts noted that the perceived intent seems to be already covered by the general independence requirement	x			
238	IEC	21	4.19	4	19	Delete, or define the safety function of a system device and explain what “own” in “its own division” refers to (the safety function? The system device ?)	IEC/SC45A experts noted that the perceived intent seems to be already covered by the general independence requirement. Furthermore, IEC/SC45A experts pointed out that this clause is not easily understood. An operator interface is not mandatorily assigned to a single division. For instance, there could be manual actions like operational bypasses (see clause 7.37) where a single button is	x	Reformulated. Note that operational bypasses that comply with the recommendations of paragraph 7.41 DO NOT suppress a safety function.		

							provided to the operator to activate the bypass of a protection function in all divisions at the same time (the button being of course subject to a validation button). Suggestion is to remove the clause or to reformulate it.				
355	PAK	4	4.27	4	27	Common cause failure might happen, for example, because of human errors, errors in the development or manufacturing process, failure propagation between systems or components, or inadequate specification, qualification for, or protection against, internal or external hazards, or failure of common support systems.	Failure of common support systems is also be considered as common cause failures.			x	There should not be common support systems for safety systems. There may, however, be common cause failure of support systems because of the reasons already given.
347	CHW	2	4.32	4	32	An analysis should be done .... from performing the needed safety functions. **For typical analysis techiques (eg FMEA, Defence-in-Depth and Diversity Analysis, ...) see paragraph 2.84.**	The relation between para 4.32 and para 2.84 should be indicated more clearly and more explicitly.	x	Added as an example method. D-in-D&D analysis is often taken to mean analysis in accordance with NUREG/CR 6303. There may be other ways to accomplish the same goal.		
239	IEC	22	4.32, 4.33, 4.34 and 4.37	4	32	Replace by 4.32 The combination of PIE with credible CCF should be analyzed. Methods to be used and concerned PIE vary among member states. Delete 4.33, 4.34 and 4.37	IEC/SC45A experts noted that the given practices emphasis the singular practices of a small number of member states. IAEA guidance should reflect the best practices that are accepted by a large number of member states.		OPEN ITEM		
306	USA	15	4.32 4	4	32	An analysis should be done of the consequences of each PIE in combination with CCF's that will prevent the I&C safety systems from performing the needed safety functions.	Identification of Common Cause Failure - Clause 4.32 uses the term "credible CCF" to identify those CCF's that need to be analyzed for consequences. This is interpreted by many to mean that only those CCF's that are within design basis need to be considered. Consequently, because software CCF's are considered to be beyond design basis, they would not need to be considered. This conflicts with the US NRC's standing policy that requires software CCF's to be included in analysis regardless of whether the failure is within design basis.	x			

212	FRA	86	4.33 to 4.36	4	33	Delete 4.33 to 4.36	See general comment		OPEN ITEM		
240	IEC	23	4.38	4	38	Delete	IEC/SC45A experts noted that this example appeared as not necessary.	x			
365	PAK	14	4.40	4	40	Given reference for IAEA safety glossary may be corrected as [7] as mentioned in the references of this guide.		x			
35	CAN	35	4.42 (RJH)	4	42	Change "that the diverse features actually achieve the diversity that is claimed." to "that the diverse features actually achieve the common cause mitigation that is claimed."	Clarification and correctness	x			
348	CHW	3	4.43(?)	4	43	When diverse I&C systems are provided to meet requirements for defence-in-depth **or diversity,** the diverse systems should be ...	Diversity as another reason was not mentioned.	x			
307	USA	16	4.44 4	4	44	Delete this item, or clarify the acceptance criteria for "negligible."	This line states that diversity may not be needed where the possibility of CCF is negligible, but it does not provide any criteria for what is negligible. Although the NRC considers a software CCF to be beyond design basis, the NRC always requires a D3 analysis to determine the susceptibility to software CCF.	x	Deleted. Paragraph 4.31 provides the needed guidance on this topic		
120	FIN	8	4.45	4	45	The sentence ….*I&C items important to safety as fully independent unless they are diverse* should be clarified. Separation of the systems is as important.		x	And deleted 4.47 which contained the same concept.		
213	FRA	87	Section 5	5			What consistency with DS367 ?			x	DS367 is not yet stabilized; therefore, it is not advisable to base this document on a draft. The recommendations in DS431 do vary according to safety class. Most recommendations apply to items important to safety. This is consistent with the requirements of SSR-2/1 where most requirements apply to items important to safety. Many recommendations of DS-431 apply only to safety items. These cases are clearly indicated in the text.
69	KOR	2	5.	5		General Comment: IAEA Safety Standard, DS 367, provides the safety classification process. It is necessary to refer to DS 367 in Section 5 of DS 431				x	DS367 is not yet stabilized; therefore, it is not advisable to base this document on a draft. The recommendations in DS431 do vary according to safety class. Most recommendations apply to items important

											to safety. This is consistent with the requirements of SSR-2/1 where most requirements apply to items important to safety. Many recommendations of DS-431 apply only to safety items. These cases are clearly indicated in the text.
121	FIN	9	Chapter 5. Fig.3	5	0	The picture is illustrative. However, there is need to comment the picture due to the fact that the operation of the safety systems has been classified into safety related category. The whole safety function should be in the same safety class.	Deleted I&C associated with operations of safety system. It is not clear what was meant by this.	x			
87	DEU	16	5.2 c)	5	2	Complete sentence: … to perform a safety function	Wording	x			
88	DEU	17	5.2 d)	5	2	Complete the text.	Incomplete sentence (?).	x			What is the completed text?
241	IEC	24	5.2	5	2	Modify "c) the frequency with which the item will be called upon to perform a safety **function** d) The time following a PIE at which, or the period for **which the system must perform"**	IEC/SC45A experts noted that the end of c) and d) are missing.	x			
68	KOR	1	5.2 (c),(d)	5	2	Refer to section 5.34 (c) & (d) of SSR 2/1.	(c) and (d) are incomplete sentences.	x			
308	USA	17	5.2.d 5	5	2.d	(d) The system requirements for the period during and/or following a postulated initiating event.	The bullet states, "The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, with due account taken of factors such as: . . . .(d) The time following a postulated initiating event at which, or the period for". The meaning is unclear such that the suggested replacement may not be correct.			x	The comment is on text quoted from SSR 2/1. Text of the safety requirements cannot be modified in this guide.
214	FRA	88	5.4 to 5.13	5	4	Delete 5.4 to 5.13	Figure 3 is enough			x	The proposed change would eliminate the explanation of the safety classification scheme, as well as the relationship between the safety classification used in the guide and a classification scheme used in a Member State. This would leave only an example that could be misleading. The commenting member state has already expressed the desire that DS367 be

												referenced. The comment would make sense in this context, but as already discussed DS367 is not yet stable enough to reference.
309	USA	18	5.4 5	5	4	5.4. The possibility that the failure of an item important to safety may directly cause or exacerbate a PIE should be considered when determining safety classification.	Failures of a safety system may not always cause a PIE, but their failure may make the consequences of the PIE worse.	x				
89	DEU	18	5.11, 1st line	5	11	One word modification: … components <u>include</u> ~~are~~ those provided …	Otherwise the listed items must be complete.			x		Paragraph 5.11 is consistent with the IAEA definition of the term important to safety. The proposed change would make it inconsistent with the IAEA safety glossary.
310	USA	19	5.12 and Figure 4 5	5	12	Incorporate into Figure 4 the DS 431 term used for Safety related items.	Section 5.12 states, "Safety related items are items important to safety that are not part of a safety system. This guide avoids using the term 'safety related' because it is used with a very different meaning in some Member States." However, Figure 4 then uses that term as one of the classifications of items important to safety.			x		The paragraph says that the use of the term is avoided, not that it is eliminated. The IAEA term for Safety Related items is "Safety Related." Its use cannot be eliminated but it is avoided to the extent possible to reduce the potential confusion caused by the USA's particular use of the term.
36	CAN	36	5.17 (GR)	5	17	In nuclear power plants the following systems are typically classified as safety systems: • Reactor protection system; • Some elements of the accident monitoring systems; • The minimum I&C systems needed to achieve safe shutdown from operational states or design basis accident conditions including the systems providing cooling, confinement and monitoring functions;	"In nuclear power plants the following systems are typically classified as safety systems: • Reactor protection system; • Some elements of the accident monitoring systems; • The minimum I&C systems needed to achieve safe shutdown from operational states or design basis accident conditions" Comment: This statements does not explicitly mention the Emergency core cooling and containment systems			x		Deleted paragraph per comment France 89
215	FRA	89	5.17	5	17	Delete 5.17	Superfluous	x				
349	CHW	4	5.18 new after44.27 .	5	18	**Diverse safety equipment shall normally be classified to the same class and qualified according to equal qualification requirements as the safety equipment for which the diversity is foreseen..**	This is an important point that was already discussed in some projects/areas. .	x	This is not a universal practice. Added a some member state clause as paragraph 4.42a.			
125	FIN	13	Chapter 6. Marking	6		Marking of cables is missing from chapter "Marking and identification of items				x		Marking of cables is covered in NS-G-1.8 and DS430/

			and identification of items important to safety			important to safety”					
126	FIN	14	definitions failure	6		All of the failure mode should be included. failure can be also spurious action		x	Failure modes is used in the context of components and systems. Spurious operation is more of a system affect. The document was reviewed and the term “failure or spurious operation” was inserted as seemed necessary.		
311	USA	20	6.5 and §6.8 6	6	5	Change §6.8 to remove the option for incorporating complexity that is not necessary for safety. 6.8 Design techniques such as testability, fail-safe characteristics, functional diversity, and diversity in component design and in concepts of operation shall be used to the extent practicable to prevent loss of a safety function.	§6.5 (avoiding complexity) recommends avoiding complexity to keep the I&C system as simple as possible but still fully implement its safety requirements. §6.8 (reliability) recommends, among other things, “Design techniques such as…, including a self-checking capability where necessary…,” to improve reliability. The caveat “where necessary” opens the door for increasing complexity in a system to improve plant availability.			x	Paragraph 6.8 is text quoted from SSR 2/1. Text of the safety requirements cannot be modified in this guide. Both paragraphs 6.5 and 6.8 deal with systems important to safety. To some extent complexity should be allowed in non-safety systems. Paragraph 6.4 places additional restrictions on complexity in safety systems.
216	UKR	1	Page 47, line 19, after para 6.6 add a new one	6	6	The interface between safety and security in I&C systems should be addressed. Characteristics of I&C systems should be beneficial to security measures. At the same time security measures should not be performed by I&C systems and would be implemented in dedicated equipment.	The specific requirements on interaction with physical protection and computer security are given in Chapter 7. But safety and security interface is more general requirement.			x	Paragraph 6.6 is a quote from SSR-2/1 and cannot be modified in this document.
242	IEC	25	6.13	6	13	Modify as follows "Each safety group should perform all actions required to respond to a PIE in the presence of the following: a. Any single detectable failure within the safety system in combination with: b. Any undetectable failures, that is to say, any failure that cannot be detected by periodic testing, alarm or anomalous indication (see 6.78) c. All failures caused by the single failure, …	IEC/SC45A experts noted that the word "detectable" could be clarified by adding a reference to clause 6.78 that explains that undetectable failures should be considered in the Single Failure criteria.	x			
243	IEC	26	6.13	6	13	Modify as follows : d. The removal from service or bypassing	In point "d.", IEC/SC45A experts noted that it is not mandatory to remove from service or bypass the whole division	x			

						of part of safety system for testing or maintenance that is allowed by plant operating limits and conditions.	when testing or maintenance is performed. As formulated it may be understood that the whole division shall be considered as "removed from service" or "bypassed" when testing or maintenance is performed. Suggestion is to replace "division of safety system" by "part of safety system"				
70	KOR	3	6.13. a		13.	Any single detectable failure within the safety system in combination with all identifiable, but nondetectable failures;		x	See comment IEC 25		
312	USA	21	6.13 6	6	13	Include non-detectable failures as 6.13.e	Non-detectable failures (i.e., those failures that cannot be detected by indication or testing) should be included in the single failure analysis.	x			
313	USA	22	6.15 & 6.16 6	6	15	Delete 6.15 and 6.16.	Single Failure Criterion – Clause 6.10 clearly characterizes compliance with single failure criterion as a system requirement; however, clauses 6.15 and 6.16 allow for exceptions to the SFC, as long as the exceptions are justified. The justification criteria in clause 6.16 include low probability of occurrence of the PIE and of the failure. It also allows exceptions when components of the I&C system are taken out of service for maintenance repair and testing. This does not align with US NRC regulations which state that the SFC must be met even during system testing. This regulation is defined in 10CFR 50 Appendix A, General Design Criteria 21 “Protection System Reliability and Testability”. IEEE 279 Clause 4.11 also states that “The system shall be designed to permit any one channel to be maintained and when required, tested or calibrated during power operation without initiating a protective action at the system level. During such operation, the active parts of the system shall of themselves continue to meet the single failure criterion.			x	Paragraphs 6.176 and 6.204 cover the situation considered by GDC 21 and IEEE 279 clause 4.11. See NUREG 1431 Vol 1 ,Rev 3., Table 3.3.3-1 item 1 Condition B, item 4 Conditions F and G, item 17 Condition O, and item 19 Condition P for example situations in which NRC accepts continued operation when the single failure criterion is not met.
37	CAN	37	6.16 (GR))	6	16	Non-compliance with the single failure criterion may be justified for:	Non-compliance with the single failure criterion may be justified for:			x	The proposed change is confusing and is inconsistent with other existing consensus

						• Very rare PIEs, that are found to be less frequent by alternate methods (e.g., site specific data);	• Very rare PIEs; Comment: Very rare PIEs are not well defined. Instead, justification method could be defined.				standards.
122	FIN	10	6.16	6	16	Single failure criteria is a deterministic requirement. It should not be possible to override single failure criteria by statistical justifications.				x	The proposed change is confusing and is inconsistent with other existing consensus standards.
123	FIN	11	6.25	6	25	This requirement is connected to the definition of the failure. see below. What is meant by the ability to perform?				x	The paragraph is a statement of the definition in the IAEA Safety Glossary and cannot be changed in this document.
38	CAN	38	6.28 (RJH)	6	28	Consider changing the guidance to align with the first sentence of 6.29	For consistency; The guidance provided here contradicts the guidance in the first sentence of 6.29.			x	There is no conflict. Paragraph 6.29 states that there may be multiple devices and according to 6.28 they should all be part of the higher class system.
314	USA	23	6.48 6	6	48	Add item "Member countries may have additional requirements and restrictions on connections of non-safety maintenance systems to safety systems."	Different member countries have different requirements on connection of lower safety class maintenance systems to safety equipment. This should be pointed out in this guide. For example, the US only allows temporary connections of non-safety maintenance systems to safety systems, while the affected division is off line. This is enforced through physical disconnects.	x	Revised paragraph according to the stated practice		
90	DEU	19	6.51, 1st line	6	51	The ~~communication~~ transfer of data …	The term communication associates too much the protocol driven data exchange, which - from the cyber security point of view - is not the recommended option in comparison with stateless data transfer.	x			
91	DEU	20	6.54 + 6.55	6	54	Rephrase and combine the both par.: In justified cases signals may be send from systems of lower to systems of higher safety classification via individual analogue or binary signal lines, provided that a. Completion of safety actions cannot be interrupted by commands from the system of lower safety classification, and b. The potential for failures in the system of lower safety classification that cause spurious actuation is assessed and shown to be acceptable.	See IAEA Security series No. 17.	x			
315	USA	24	6.58	6	58	Difficulties might arise in demonstrating the	Diversity – Clause 6.58 states that diverse	x	Changed to "… then diverse I&C		

			6			reliability of computer-based systems or systems that use complex hardware functions, complex hardware logic or complex electronic components. If it is not possible to justify the adequate reliability of a function being performed by I&C then diverse I&C equipment may be used to provide additional reliability. Insert: “Diverse equipment designs can also be used to address requirements that are not associated with reliability. Providing alternate means of maintaining core protection for specific beyond design basis events such as software CCF may also be addressed by including diverse equipment.”	I&C equipment may be used to provide additional reliability in cases where it is not possible to justify adequate reliability of a function by the I&C system. This statement implies that providing justification for adequate reliability of a required safety function is the only reason for including diverse I&C equipment in a plants. Diverse equipment designs can also be used to address requirements that are not associated with reliability. Providing alternate means of maintaining core protection for specific beyond design basis events such as software CCF may also be addressed by including diverse equipment.		equipment may be used to increase confidence that the fundamental safety functions will be achieved.”		
92	DEU	21	6.59	6	59	Sentence should be deleted	Diversity does not worse the cause of CCF but even more avoids or controls effects of it.	x			
93	DEU	22	6.62	6	62	Examples of different types of diversity include: ☐☐ Design diversity: achieved by using different design approaches to solve the same or a similar problem; ☐☐ Signal diversity: achieved by systems in which a safety action may be initiated based upon the value of different plant parameters; ☐☐ Equipment diversity: achieved by hardware that employs different technology (e.g., analogue vs. digital, solid-state vs. electromagnetic, computer-based vs. FPGA-based); ☐☐ Functional diversity: achieved by systems that take different actions to achieve the same safety intent; ☐☐ Human diversity: achieved by using different design personnel; ☐☐ ~~Logic diversity (including software diversity): achieved by using different programs using, for~~	Order of enumeration should be changed beginning with the most important and most efficient types of diversity. Logic diversity repeats different types of diversity already listed before and thus should be deleted.	x	Changed, but it is not agreed that the justification given is correct. Both before and after the orders are arbitrary.		

						~~example, different programmers, languages, methods, or tools.~~					
244	IEC	27	6.62	6	62	Integrate those definitions of different type of diversity in the main definition of diversity as a note.	IEC/SC45A experts noted that it could be useful to enhance the definition of diversity including this information.			x	The different types of diversity are mainly used here. Thus they don't seem to warrant inclusion in the definitions.
316	USA	25	6.62 6	6	62	6.62. Examples of different types of diversity include: . . . • Human diversity: achieved by using different design personnel; management diversity, tester and installer diversity, and development team diversity.	The examples of human diversity should include management diversity, tester and installer diversity, and development team diversity.	x	Also changed term to Life cycle diversity.		
94	DEU	23	6.63.	6	63.	6.63. Where diversity is provided the choice of the types of diversity used should be justified under consideration of DiD and diversity.	It has to be added concerning what diversity has to justified.	x	See Canada 45		
245	IEC	28	6.64 and 6.65	6	64	Delete or propose a consensual formulation.	IEC/SC45A experts noted that there is no consensus on that topic and the practice presented as widely accepted is singular to a few member states. Note that during the discussion held in the frame of the OECD/NEA/MDEP/DICWG (in particular for the common position 1) there was no consensus on the problem of the type of architecture to be used and the type of diversity to be used for backup systems.	x			
95	DEU	24	6.65	6	65	~~6.65. Functional and signal diversity are considered to be particularly effective methods to protect against common cause failure due to design errors. These methods might not be sufficient by themselves to protect against common cause failure.~~	If functional diversity is really effective is highly discussed among experts. Further already a form of technical solution is proposed. This should be avoided. Thus the whole sentence should be deleted.	x			
96	DEU	25	6.66	6	66	6.66. Diversity need not always be implemented in separate systems. For example, functional diversity and signal diversity may be implemented within a single system to protect against errors in requirements. Some Member States require application of functional and signal diversity within protection systems for such reasons.	Allowance. Text should give requirements, thus deletion of the whole paragraph.			x	The text of a safety guide NEVER gives requirements, but it may give either recommendations or explanations. This seems to be a useful point. See comment IEC 29.

246	IEC	29	6.66	6	66	Modify as follow: “Functional diversity and signal diversity should be implemented to protect against errors in requirements. They can be implemented within a single system and in separate systems. “	IEC/SC45A experts noted that functional and signal diversity are widely accepted measures that are the only ones to protect against errors in requirements. IEC/SC45A experts noted that functional diversity and signal diversity are of prime importance in IEC standards.	x			
40	CAN	40	6.67 (GR)	6	67	The provision of diversity also involves avoiding areas of potential commonality in the application of diversity, such as materials, components, similar manufacturing processes, similar logic, subtle similarities in operating principles, or common support features. For example, different manufacturers might use the same processor or license the same operating system, thereby potentially incorporating common failure modes. Claims for diversity based only on a difference in manufacturers’ names or model numbers are insufficient without consideration of this possibility. To minimize common failure modes, the design should consider the options of same processor with different operating system or different processors with same operating system or different processors with different operating system. However, this should be described in paragraph 9.60.	The provision of diversity also involves avoiding areas of potential commonality in the application of diversity, such as materials, components, similar manufacturing processes, similar logic, subtle similarities in operating principles, or common support features. For example, different manufacturers might use the same processor or license the same operating system, thereby potentially incorporating common failure modes. Claims for diversity based only on a difference in manufacturers’ names or model numbers are insufficient without consideration of this possibility. Comments: Guidance on achieving this may require clarification.			x	These possibilities are already within the types of diversity given already in paragraph 6.62.
39	CAN	39	6.72 (RJH)	6	72	Consider revision.	This guidance seems internally contradictory; (i.e. if something is random, how can it be “known”) and inconsistent with the first sentence of 6.75.	x	Changed to non-systematic. Still random is not incorrect. The random end states of a six sided die are very well known.		
247	IEC	30	6.72	6	72	The ~~**random**~~ failure modes of I&C components and systems should be known and documented.	IEC/SC45A experts reminded that a single failure mode may encompass several possible random failures. However the purpose of this requirement is precisely that possible failure modes are known in advance, they are therefore not random.	x	Changed to non-systematic.		See CAN 39
41	CAN	41	6.74 (GR)	6	74	The failures that result from software errors are difficult to predict. Nevertheless, it is not necessary to know how the software fails to determine the possible failure states as seen at device terminals. The failure modes can be classified into a manageable set of possibilities, e.g., output fails high, output fails low, output fails in place, ~~short, open,~~ produces incorrect message, produces	The failures that result from software errors are difficult to predict. Nevertheless, it is not necessary to know how the software fails to determine the possible failure states as seen at device terminals. The failure modes can be classified into a manageable set of possibilities, e.g., output fails high, output fails low, output fails in place, short,	x			

						incorrect checksum, produces incorrect data, produces incorrect address	open, produces incorrect message, produces incorrect checksum, produces incorrect data, produces incorrect address. Comment: Short and open are physical phenomena, not related to software errors. It is suggested to remove these words here.				
248	IEC	31	6.74	6	74	Delete	IEC/SC45A experts noted that there is an apparent contradiction between this paragraph 6.74 that states that software error can be can be classified into a manageable set of possibilities and the next paragraph 6.75 that states that the failure modes that might result from systematic errors in the design or operation of hardware or software are essentially unpredictable.	x	Clarified. The set of failure modes as observed at the device terminals can be predicted, but the specific failure mode that is most likely to occur cannot. This is different from, for example, a relay where the failure modes may be "failure in the de-energized state" or "failure in the energized state (welded contacts)" of these two the former is generally considered the most likely. This is important for the application of the fail-safe concept as it is not possible to design for fail-safe in both modes.		
97	DEU	26	6.75, 1st and 2nd line	6	75	Modified text: The failure modes that might result from systematic errors in the design ~~or operation~~ of hardware or software are essentially unpredictable.	Design CCF is the most unpredictable mode.	x			
124	FIN	12	6.75	6	75	The systematic failures are mastered by Defense-in-Depth design. However, this is not considered at all in requirements 6.75. Also the maximal failure behavior of each Defense-in-Depth line should be defined.				x	Comment is unclear.
42	CAN	42	6.79 (GR)	6	79	6.79. As far as practicable, the failure of a component or a subsystem should not cause spurious actuation of safety systems.	As far as practicable, the failure of a component should not cause spurious actuation of safety systems. Comments: For clarity, additional text added (may be considered) e.g., software, air			x	Generally a subsystem will fail as a result of a component failure.
249	IEC	32	6.80	6	80	To be deleted	IEC/SC45A experts are dubious about the feasibility.	x	Clearified.		
317	USA	26	6.81 6	6	81		EQUIPMENT QUALIFICATON. This section should address detection of counterfeit components.			x	Paragraph 6.93 encompasses the idea of counterfeit parts, but generally protection against counterfeiting is a procurement, not a qualification function. Procurement is discussed in the GS-R-3 series of documents. The implications of

											counterfeiting on I&C functionality will be discussed in the forthcoming I&C computer security document.
43	CAN	43	6.104 (RJH)	6	104	The ability to preclude adverse environmental conditions should be demonstrated.	This section appears to suggest that that exposure to only mild environment is predicated on situating the equipment in an environmentally protected room or cabinet.			x	Normally the possible environmental conditions are established for each region of the plant by subcompartment analysis that considers all hazards present. This analysis is beyond the scope of the I&C document.
250	IEC	33	6.105	6	105	Modify as follow: “Environmental qualification of components that are required to function in environmental service conditions that are at any time significantly more severe than the conditions during normal operations (harsh environments including seism) should show that the component is, at the end of its qualified life, capable of performing its safety functions under the full range of specified service conditions.”	IEC/SC45A experts noted that it is necessary to clarify that seismic qualification is included in “harsh environments”.			x	Paragraph 6.100 makes it clear that the discussion of environmental qualification (including paragraph 6.105) does not include seismic. IAEA recommendations for seismic qualification are given in NS-G-1.6 which is incorporated by reference in paragraph 6.115. NS-G-6 uses different criteria for establishing qualification recommendations for seismic. Using the mild/harsh paradigm would create a conflict between the two IAEA guides.
44	CAN	55	6.109 (RJH)	6	109	Change “may be applied...” to “may be necessary to apply..”.	Clarification and correctness	x			
356	PAK	5	6.121 and para 6.126	6	121	Statement “electrical components” may be corrected as I&C components.	The term electrical components creates confusion as this guide deals with the design of I&C systems and this para specifically states the electromagnetic qualification of I&C systems not for the electrical components.	x			
45	CAN	45	6.122 (RJH)	6	122	Consider producing a grounding design for the entire I&C architecture.	To ensure proper grounding of I&C equipment, there should be a grounding design produced for the entire I&C architecture and it should be compatible with the grounding design for the entire Nuclear Power Plant.			x	The topic of grounding is discussed in DS 430
357	PAK	6	6.123	6	123	It may be modified as “Appropriate installation, maintenance and test practices are essential for the proper implementation and continued effectiveness of these provisions”.	Electromagnetic qualification of I&C system should be verified during periodic testing and maintained by appropriate installation and maintenance, therefore it may be included in the text.			x	EMI testing is very difficult to conduct at any time and especially during operation. The main goal here is to check that EMI provisions, e.g., wire routing in termination areas, decoupling devices, ground, door bonding) have not been degraded.
46	CAN	46	6.137 (RJH)	6	137	Consider including an alternative: fibre-optic cables	Alternatively, fibre-optic cables can provide EMI immunity.	x	Clarified that the paragraph applies only to electrical cable.		
318	USA	27	62/128 62/128 6.137 6	6	137	6.137. Instrumentation cables should be twisted and shielded pairs to minimize interference from electromagnetic and electrostatic interference.	The cables should be twisted and shielded pairs.	x			

47	CAN	47	6.142 (RJH)	6	142	Consider establishing strategies to achieve qualified life (such as life-time spares purchase)	The qualified life of electronic I&C systems will likely be considerably longer than the duration of support available from the equipment suppliers.			x	Addressed already in paragraph 2.119. See Canada 25.
48	CAN	48	6.153 (GR)	6	153	6.155. ~~6,153~~. At the present time it is expected that the service life of some I&C systems will be on the order of 10 to 20 years. Therefore, it might be appropriate to provide features that will facilitate the installation of and switchover to replacement systems. Such facilities might include space reserved for installation of new equipment and associated cable.	6.155. 6,153. At the present time it is expected that the service life of some I&C systems will be on the order of 10 to 20 years. Therefore, it might be appropriate to provide features that will facilitate the installation of and switchover to replacement systems. Such facilities might include space reserved for installation of new equipment and associated cable. Comment: Appears to be editorial	x			
251	IEC	34	6.154	6	154	The service time of the components and sub-components should provide the operating organization with the information they need to make long term agreements with suppliers, to plan acquisition of extra spares, and to plan for timely replacement of obsolete items. Typo: "…and to plan for **timey** replacement of obsolete items"	IEC/SC45A experts noted that the original sentence is not easily understandable as such.	x			
252	IEC	35	6.155	6	155	Replace "After evaluation, some I&C systems may be found to have a service life significantly shorter than the plant life. Therefore, it might be appropriate to provide features that will facilitate the installation of and switchover to replacement systems. Such facilities might include space reserved for installation of new equipment and associated cable."	IEC/SC45A experts noted that those numbers have no undisputable source. Moreover IEC/SC45A experts remind that an expected service life mentioned without a use environment is not very meaningful. The same equipment might last 10 years when exposed to radiation on a day to day basis, but up to 40 years when protected from it. IEC/SC45A experts' proposed reformulation preserve the essence of the original requirement.	x	Also clarified that the cause may be obsolesce as well as ageing.		
71	KOR	4	6.155	6	155	Typo "6,153"		x			
319	USA	28	6.155 6	6	155	Remove "6,153" from this section.	Typo error that could cause confusion when the safety guide is translated.	x			
49	CAN	49	6.168 (GR)	6	168	Periodic tests during plant operation will normally be needed to achieve the reliability required of safety systems; however it is	Periodic tests during plant operation will normally be needed to achieve the reliability required of safety systems;			x	The proposed text is redundant to the already existing text. Paragraph 1.168 discusses the need to avoid risk to normal

						sometimes desirable to avoid testing during operation if it puts at risk normal or safe plant operation. The capability for testing and calibration during power operation is not necessary if doing so would adversely affect the safety or operability of the plant. To achieve the required reliability for safety systems, the design should incorporate test provisions without causing undue risk to the normal plant operation. If this provision can not be accommodated in the design, a justification should be provided.	however it is sometimes desirable to avoid testing during operation if it puts at risk normal or safe plant operation. The capability for testing and calibration during power operation is not necessary if doing so would adversely affect the safety or operability of the plant. Comment: To achieve the reliability required of safety systems, the design should incorporate test provisions during operation without causing risk for normal or safe plant operation. If this provision can not be accommodated in the design, should be justified.					operation. Paragraph 1.169 discusses the need to justify the need to defer testing to outages..
358	PAK	7	6.173	6	173	Para 6.173 may be modified as “Alarms should be provided for loss of redundancy and un-safe failure in safety systems”.	Alarms for the unsafe failure should also be provided and annunciated so that operator may take necessary actions.				x	Alarms may be annunciations or other alerts for operators. Loss of redundancy would include unsafe failures
359	PAK	8	6.178	6	178	The proposed text is: Arrangements for testing include, procedures, test interfaces, installed test equipment, measurement and test equipments and built in test facilities.	Measurement and Test Equipments are also used for conducting tests of I&C components and systems and may be included.				x	Measurement and test equipment is not (and should not be) part of the I&C system. It is instrumentation that is controlled by the instrument shop and hense is not part of the scope of this guide. The interfaces for connecting MT&E are in the scope and are already addressed in paragraph 6.178.
360	PAK	9	6.182	6	182	It may be modified as “I&C systems should include provisions to automatically alert operators that channels or components are in test mode or in maintenance”.	These provisions are also considered for maintenance.		x	The concept is covered by paragraph 6.206, hence paragraph 6.182 was deleted.		
361	PAK	10	6.183 6	6	183	It may be modified as “Operator notification that channels or components are in test mode or in maintenance is often accomplished by alarm or bypass indications when a channel is bypassed for testing or maintenance”.	These provisions should also be considered for the channel or component under maintenance.		x	The concept is covered by paragraph 6.206, hence paragraph 6.183 was deleted.		
253	IEC	36	6.184	6	184	Include expected test results to the list.	IEC/SC45A experts noted that a test program will normally include the expected test results.				x	The need to identify expected test results is already discussed in paragraph 6.192.e.
254	IEC	37	6.192	6	192	Delete “… or configuration parameters of plant components.”	IEC/SC45A experts noted that modification of some parameters can be necessary for periodic tests. There is no reason to forbid them if they are performed under appropriate				x	If configuration parameters are changed for testing, what is testing is different from what is operated, thus making the tests not a valid indication of operability in normal operation.

							administrative controls.					
50	CAN	50	6.196 (RJH)	6	196	Incomplete	This should include software maintenance/recovery plans.				x	Already addressed in paragraph 2.29. See Canada 10.
350	CHW	5	6.202 new after	6	202	**The maintainability shall be analysed in combination with the Single Failure Criterion.**	This is an important point that was already discussed in some projects/areas.				x	The comment is not consistent with the general application of the single failure criterion and it is not clear how maintainability would be fit into the concept, beyond the existing consideration that known failures must be repaired before another failure occurs. Normally, this is controlled best by the allowed outage times specified in Operational Limits and Conditions (Tech Specs) in which AOTs are usually set short enough that a second failure is not anticipated.
51	CAN	51	6.211 (RJH)	6	211	Consider including adjustment of set-points.	Over time set-points will need to be adjusted to reflect plant aging.	x	Addressed in paragraph 6.215.			
100	DEU	29	7.138/86	7	138/ 86	HDL configured devices are programmable electronic modules ~~integrated circuits~~ providing logic structures (e.g. arrays of gates and switches) which are customized by the I&C developer to provide specific functions.	HDL configured devices may comprise different parts: e.g. ICs, flash memories, microprocessors, network features	x				
101	DEU	30	7.139/86	7	139/ 86	This customization involves special tools to formally describe the required functions, to ~~build an electronic scheme which~~ implement~~s~~ these functions on programmable devices ~~and to map this electronic scheme on the available logic structures of the integrated circuit~~. ~~The mapping information transferred to the electronics is referred to as 'bitstream'.~~	Presents one specific solution of the FPGA technology only and should be generalized.	x				
102	DEU	31	7.142/86	7	142/ 86	The HDL design should guarantee ~~synchronous and~~ deterministic behaviour of the component.	Why synchronous only? Is synchronous behavior of the hardware best way to fulfill safety criteria? Or it is possible cause for CCF?				x	Synchronous design consists in enforcing the change in state of the internal registers and of the outputs simultaneously only at the times defined by a clock. It favors modular and understandable design. It minimizes the potential for wrong behaviours due to gliches, and it favours the best use of synthesis and verification tools. See IEC 62566.
103	DEU	32	7.142/86	7	142/ 86	~~Synchronous and~~ deterministic behaviour favours correctness and testability and allows for the best use of the design and verification tools.	What does mean "synchronous behavior"? Why synchronous? Is synchronous behavior of the hardware best way to fulfill safety criteria? Or it is				x	See Germany 32

							possible cause for CCF?					
52	CAN	52	7.3 (RJH)	7	3	Consider including validation of the basis for the calculation and pre-determination of the path forward.	When a plant variable is determined based on a calculation, the basis for the calculation must be validated and the path forward in the absence of an available measurement (e.g. use of a default, conservative value) must be pre-determined.			x	The issue is already covered by the recommendation to address failure modes and the guidance of V&V
255	IEC	38	7.6	7	6	To be replaced by “The consequences of sensor CCF combined with a PIE should be no greater than those accepted in clause 4.32.”	IEC/SC45A experts noted that as seen in 4.32 the acceptable criteria vary from one member state to the other. This new formulation of 7.6 ensures consensus.	x			
256	IEC	39	7.11	7	11	Modify as follow: “The automatic control so that the main process variables are maintained within the limits assumed in the safety analysis is part of the defense in depth of the plant, and therefore the concerned control systems will normally be important to safety.”	IEC/SC45A experts noted that the scope of the concerned automatic control should be defined. The proposal is consistent with IEC/SC45A standards.	x	Modified for clarity and to recognize that control systems are responsible for enforcing operational limits, not safety limits. See for example NS-G-2.2 Fig A1		
257	IEC	40	7.12	7	12	Delete	IEC/SC45A experts noted that the term “stable state” is confusing as it has another meaning in the IAEA safety glossary definition of “accident management”. We propose to define the scope in paragraph 7.11 (see comment SC45A 35 above).	x			
258	IEC	41	7.13	7	13	Delete	IEC/SC45A experts noted that requiring redundancies in the control system is well beyond the actual best practices.	x	The paragraph was intended to apply to HMI displays that affect many functions. In this context it is well within accepted practice, but belongs in section 8. No in paragraph 8.58.		
259	IEC	42	7.15	7	15	To be replaced by “Loss of power should result in bump less transfer to stand by equipment (…), or bump less source transfer so that the same automatic controls are used but powered by another source.”	IEC/SC45A experts noted that no standards forbid the use of the same automatic controls powered by different source. This is a widely used solution.	x	Simplified to bumpless transfer to standby equipment. The standby equipment could be a different controller or a different source.		
320	USA	29	7.19 7	7	19	7.19. The protection system as a whole may include several systems, and is required for protection for against design basis accidents and abnormal operating occurrences.	The guidance states safety systems are only for design basis events. Abnormal operating occurrences (events that are expected to occur at least once in the life of the plant) should also be addressed by safety systems. For example, turbine trips without runback are an abnormal occurrence that would require a safety system response. This guidance would then be consistent with §7.20.	x	Deleted the last phrase as AOO’s may not be included in all member states.		
260	IEC	43	7.24	7	24	Modify as follow:	IEC/SC45A experts noted that this	x			

						“The operator is allowed sufficient time to evaluate the status of the plant and to complete the required actions. For new designs, it is advisable to design such that during the first 30 minutes of a design basis event, operator actions are not needed to maintain plant parameters within the established limits.”	practice is widely accepted and should consequently be recommended by this guide.				
261	IEC	44	7.31	7	31	Modify as follows "The sensors that provide signals to the protection system ~~should be classified as part of the projection system and their signals~~ should only feed other systems through appropriate buffering and isolation devices"	IEC/SC45A experts noted that the part of the requirement that suggests to classify the sensors with the Protection System may not be suited to all designs. Indeed, as specified by IEC62340 éd. 2007 §6.2.3 and more specifically by the footnote 7 second bullet, there are design strategies where a same sensor can be used by the Protection System and one (or several) other I&C systems. Classifying the sensor with the Protection System maybe confusing, because one could think that in case of CCF on the Protection System, we also loose the sensors, and thus both lines of defense. That is not true. For such design strategies, in order to avoid misunderstanding, it may be preferable to classify the sensors, independently from the I&C system they are connected to. It shall be left to the designers with which system the sensors are classified.	x			
262	IEC	45	7.38	7	38	Modify as follow: “As far as practicable, the protection system should prevent the activation of an operational bypass when the applicable permissive conditions are not met.”	IEC/SC45A experts noted that there are some specific cases where it is not possible to automatically determinate if the applicable permissive conditions are met or not.	x	Revised paragraph 7.41 so that paragraph 7.38 is unnecessary		
98	DEU	27	New par. after 7.47	7	47	The provision to manually reset a protection system function should be specified and implemented according to the requirements on safety systems.		x			
321	USA	30	7.52 7	7	52	7.52 Interference between protection systems and control systems at the nuclear power plant shall be prevented by means of separation, by avoiding interconnections and by suitable functional independence.”	§7.52 states, “Interference between protection systems and control systems at the nuclear power plant shall be prevented by means of separation, by avoiding interconnections or by suitable			x	Paragraph 7.52 is a quote of SSR 2/1 and cannot be changed in this document.

							functional independence." The or implies that suitable functional independence allows a design to have interconnections between safety systems and control systems. Rephrase or to and to remove the ambiguity.				
322	USA	31	7.54 (Interaction; protection and other systems) 7	7	54	"should satisfy all reliability, redundancy, and independence safety requirements in the presence of a failure of any component …"	There is no justification to limit or identify just these few requirements; all safety requirements should be maintained by the safety system in the presence of any non-safety system failure.			x	Paragraph 7.54 paraphrases NRC requirements given in 10 CFR 50, Appendix A, GDC 24.
263	IEC	46	7.57	7	57	To be replace by "The possibility of failure in the protection system may be itself a PIE that triggers a control system action **for** which the protection system is necessary cannot be disregarded. "	Typo	x			
323	USA	32	80/128 §80/128 §7.68 7	7	68	7.68. Digital systems include, for example, computer based systems and systems programmed with Hardware Description Languages."	§7.68 states, "Digital systems include, for example, computer based systems and systems programmed with Hardware Definition Languages." The appropriate term is hardware description languages.	x			
264	IEC	47	7.72	7	72	To be modified as follows "Unidentified errors ~~will~~ **might** exist and they ~~will~~ **might** exist in all redundant component uses (…). "	IEC/SC45A experts noted that for the same reason one cannot be sure that all digital system errors have been identified (excessive complexity), one cannot be sure that errors are present. The limitations imposed by complexity go both ways.	x	Nevertheless, the comment is extraordinarily optimistic.		
53	CAN	53	7.73 (RJH)	7	73	The implementation of digital I&C systems should be deterministic.	The implementation of digital I&C systems should be deterministic such that small differences in timing do not result in differences in system behaviour.			x	See paragraph 7.76
55	CAN	55	7.76 (RJH)	7	76	Data in messages processed by a receiving safety system should not have limited ranges. Also, data received by the receiving safety system should be verified or validated before it is acted upon.	It is also advisable that data in messages processed by a receiving safety system should have limited ranges. Data outside of the pre-determined range would be ignored. Also, data received by the receiving safety system should not be acted upon until it has been returned to the source and a confirmatory hand-shake message returned to the receiving safety system that the correct data was received.			x	Already covered by paragraphs 7.84 to 7.88
265	IEC	48	7.76	7	76	To be replaced by "I&C systems should be	IEC/SC45A experts noted that the	x			

						designed to have a predictable response time, i.e., the time delay between stimulus and response has a guaranteed maximum and minimum. “	described behavior refers to predictability not determinism (in which case you would know an exact response time). IEC/SC45A suggested rephrasing is what was agreed during the previous review of the draft (rev D). General note: The two terms predictable/deterministic are close in meaning and very often confused and misused. Using such terms without a clear definition will lead to misunderstanding.				
54	CAN	54	7.77 (RJH)	7	77	Suggest including the use of interrupts	Avoiding use of interrupts may be inadvisable in that this could result in delays in responding to plant conditions which demand prompt action of reactor shutdown mechanisms.			x	There is no recommendation here to avoid the use of interrupts. It is given as on of several examples of methods that may be used to ensure deterministic response. It is agreed that there may be some cases where it is inadvisable. That is why it is NOT a recommendation.
266	IEC	49	7.81	7	81	To be replace by “Data communication systems should be designed to have predictable transmission times, i.e. the time delay between the posting of a message by the sender and its receipt by the addressee has a guaranteed maximum and minimum.”	IEC/SC45A experts noted that as above, the described behavior is a predictable one (known max and min), not a deterministic one (known response time).	x	Also deleted 7.83 as no longer necessary.		
267	IEC	50	7.102	7	102	Delete	IEC/SC45A experts noted that communication between safety divisions concerned essentially the votes. Each division typically send its partial trip to the others and receive partial trip from the others to do the votes. In such a case, it is unclear how one-directional communication is possible between safety divisions.	x	Nevertheless, it is possible to have two one-directional links. One in each direction. Many existing systems use this approach.		
324	USA	33	7.106 7	7	106	Add the following lines before 7.106: “A team that consists of facilities’ Computer Security Teams, which should include I&C engineers, should be formed to perform computer security impact analysis to determine computer security requirements for any design changes including acquiring/developing new systems.”	Added clarification to IAEA Nuclear Security Series No. 17, Ref. [32]. It is difficult for a person to have broad working knowledge of plant operation, computer security, physical security, engineering, maintenance, and other subjects. The team will ensure that the computer security of I&C systems properly address system and programmatic threat vectors.			x	This topic will be covered in detail in the forthcoming I&C computer security document.
325	USA	34	7.106:	7	106	Add the following lines before 7.106: The team should perform a computer security	Addressing computer security at system and program levels ensures new systems			x	This topic will be covered in detail in the forthcoming I&C computer security

			7			impact analysis to identify potential vulnerabilities, weaknesses, and risks introduced by design changes, and determine how these identified computer security threats are addressed. The computer security impact analysis includes the following: Perform a comprehensive analysis as described in Section 5.3 “Asset Analysis and Management,” of IAEA Nuclear Security Series No. 1. Perform a comprehensive analysis to determine how the baseline computer security measures will be applied to a system under design. Perform a comprehensive analysis to determine any adverse impact to the facilities’ computer security strategies for the existing environment by the new design. Additionally, determine any adverse conditions that have been introduced to any related systems in the existing environment by the new design. Based on these analyses, the team should determine computer security design requirements for the systems being modified. If applicable, the computer security design requirements should include a system’s design requirements to inherit the program or already existing security measures to minimize the modification of security features added into the system. To minimize the complexity and adverse impact to the reliable operation of the system under design, computer security requirements added directly to the design components should be kept to a minimum.	will properly inherit the existing security measures (this may minimize the number of security features added to the systems) and new systems do not adversely impact computer security of other systems and/or computer security strategies of the facilities.				document.
326	USA	35	7.110 add after 7	7	110	If security features added to the system adversely impact proper operation of the I&C systems and/or HMI so that operators’ abilities to perform their functions are degraded, then such security features should be removed and alternative computer security measures implemented to address vulnerabilities	Clarification. Additionally, with the removal of any security features, the systems are now vulnerable to threats that the removed security features mitigated. Thus alternative computer security measures need to be implemented to address the threat that the removed security feature addressed.			x	The concept of adverse impact is already covered in paragraph 7.107. Previous sections already deal with the need to implement sufficient controls. Further detail will be in the forthcoming I&C computer security document.

268	IEC	51	7.112	7	112	To be deleted	IEC/SC45A experts noted that is it really necessary for equipment not involved in the real time process			x	Comment is self-contradictory. Furthermore, a computer security feature that is included in an I&C system IS involved in a real time process.
327	USA	36	7.112 7	7	112	The security requirements are part of the overall system requirements. Therefore, the developers should follow the development process provided in Section 2 of this guide to ensure the completeness, accuracy, testability, and consistency of the security measures incorporated into the I&C systems.	Clarification.			x	Further detail will be in the forthcoming I&C computer security document.
56	CAN	56	7.113 (RJH)	7	113	The design of the overall I&C architecture should include a strategic approach	to minimize cyber security risks and to facilitate hardening of important cyber assets.	x	Paragraph 3.15 already recommends identifying security requirements, Paragraph 2.120a has been added to recommend a systematic approach to implementing requirements.		
328	USA	37	7.113 7	7	113	Replace the last phrase “computer security” with “computer security of the facility where the systems are developed.”	To protect the integrity of the I&C system during development, the facilities where I&C systems are developed need to address the following: developing facilities’ computer security quality of the developing process trustworthiness of vendors	x			
329	USA	38	7.113 7	7	113	Add the following before 7.113: The computer security program should be planned and implemented at the facilities where I&C systems are being developed and manufactured to ensure that the integrity of the systems being developed are protected from adversaries’ malicious acts. This includes the following: securing developing facilities’ equipment and systems that are used to develop I&C systems ensuring trustworthiness and reliability of employees implementing measures to protect against supply chain threats: establishment of trusted distribution paths validation of vendors requiring tamper proof products or tamper evident seals on acquired products	To protect the integrity of the I&C system during development, the facilities where I&C systems are developed need to address the following: developing facilities’ computer security quality of the developing process trustworthiness of vendors			x	Further detail will be in the forthcoming I&C computer security document.
330	USA	39	7.116 7	7	116	For I&C systems acquired from a vendor, the acquiring facility should develop,	Vendors and developers of I&C systems need to implement computer security to			x	Further detail will be in the forthcoming I&C computer security document.

						disseminate, and periodically review and update formal, documented acquisition/procurement procedures that address issues of personnel trustworthiness, information security, and supply chain integrity.	protect the integrity of I&C systems being developed at their facilities. The computer security that the vendors or the developers need to apply to protect the I&C systems while they are being developed should be provided by the facility owners who are procure I&C systems.				
331	USA	40	7.116 7	7	116	Add the following after 7.116: Performing and documenting computer security tests and evaluations to ensure that the acquired or developed I&C systems meet all specified security requirements and are free from known, testable vulnerabilities and malicious codes.	To protect the integrity of the I&C system during development, the facilities where I&C systems are developed need to address the following: developing facilities' computer security quality of the developing process trustworthiness of vendors			x	Further detail will be in the forthcoming I&C computer security document.
332	USA	41	7.116 7	7	116	Suggest moving 7.116 to a requirements section, such as 2.101(i).	7.113-7.115 refer to the development process, while 7.116 refers to requirements for the developed system.	x	Inserted as 2.102a		
57	CAN	57	7.117 (RJH)	7	117	Consider applying a graded approach for access control/enclosure of non-consequential data connections.	A graded approach should be applied for access control/enclosure of non-consequential data connections.			x	Access to data points clear path to changing functionality of equipment. Modifications to lower class systems also present a risk to the plant
333	USA	42	7.117 7	7	117	Add the following before 7.117: Redraft the section after drafting team decides what areas (life cycle phase) of access control that this document needs to address before this section is further developed. Currently, this section covers various areas (phases of the lifecycle) of access controls.	This section is not clear about what access control is covered by this section. Does this section cover access controls of developing facilities, access control capabilities of system being developed, access configuration of developed system during implementation phase of life cycle, or access control to the developed system during operational phase of the life cycle? The section appears to address access controls for various areas discussed above. Drafter of the document should decide this.	x	Clarified that this applies to plant equipment by changing section heading. Further detail on development environment ument.control will be in the forthcoming computer security doc		
334	USA	43	7.117 7	7	117	Add the following after 7.117: Remove unnecessary services and programs in the systems and connection to the systems. Additionally, facility owners need to document all required applications, utilities, system services, scripts, configuration files, databases, and other software and the	This provides some elements of computer security associated with installation of the developed I&C systems on the facilities' I&C networks.			x	Further detail will be in the forthcoming I&C computer security document.

						appropriate configurations, including revisions or patch levels, and connection to other devices for each of the systems being developed. They need to maintain a list of services and connections required for the systems being developed. The listing includes all necessary ports and services required for normal and emergency operations. The listing also includes an explanation or cross reference to justify why each service is necessary for operation. Only those services and programs that are necessary for operation are allowed.					
335	USA	44	7.118/2. 7	7	118	Add at end of 7.118: "Data connections should be limited to those that are protected at the same level as the system being connected. This may include the facilities to establish processes for establishing trust levels for each of these devices and people who are using these devices before granting devices connection to the systems."	Clarification.			x	Further detail will be in the forthcoming I&C computer security document.
58	CAN	58	7.123 (RJH)	7	123	Reconsider the use of two different means of authentication in addition to access control.	Two different means of authentication in addition to access control appears excessive.			x	More people have access to cabinets who should not be able to make functional changes. Two factor authentication is now used frequently simply for access to corporate data. The consequences of improper access to modify NPP functions may be much higher.
269	IEC	52	7.123	7	123	Modify as follow: "Access to functions that allow changes to software or configuration data of digital safety systems should require that the user be authenticated by one mean beyond those that allow entry into equipment rooms or equipment enclosures"	IEC/SC45A experts recommended that such mechanisms are recommended for safety systems only. Furthermore, this need is recognized by the current state of the art requires one means.			x	More people have access to cabinets who should not be able to make functional changes. Two factor authentication is now used frequently simply for access to corporate data. The consequences of improper access to modify NPP functions may be much higher.
336	USA	45	7.128 add after 7	7	128	The developed system should have capabilities to either perform the following areas of access control or inherit the capability of facilities to perform the following areas of access control: Account Management Access Enforcement Information Flow Enforcement Separation of Duties	The developed systems should either have the capabilities or should have the capabilities to inherit the security measures in their environment to control and monitor the access.			x	Further detail will be in the forthcoming I&C computer security document.

						Least Privilege Unsuccessful Login Attempts System Use Notification Previous Login Notification Concurrent Session Control Session Lock Session Termination Supervision and Review/Access Control Permitted Actions Without Identification or Authentication					
337	USA	46	7.129 7	7	129	Add the following to before 7.129: Implement technical and operational measures to provide high assurance that the direct or indirect data link between activities off site or at the Emergency Control Centre does not provide a pathway that adversaries can exploit to attack I&C systems and/or equipment or systems located off site or at the Emergency Control Center.	Unlike the analog systems, the boundaries of a digital system end with communicating systems. Thus, all the links to the I&C systems need to be protected.			x	Further detail will be in the forthcoming I&C computer security document.
338	USA	47	7.130 7	7	130	Add the following to before 7.130: Implement automatic features or other features to monitor network activities between I&C systems or equipment or systems located off site or in Emergency Control Centers to detect and notify appropriate people when abnormal or suspicious activities are detected.	Because of the amount of volume of collected data and the pace of the attack that could occur, manual collection of data and analysis of collected data may be very difficult. However, this can be accomplished through automatic means.			x	Further detail will be in the forthcoming I&C computer security document.
99	DEU	28	7.131	7	131	Data communication	Wording	x	Either is correct.		
270	IEC	53	7.142	7	142	To be modified as follows “The HDL design should guarantee synchronous and predictable behavior of the component.”	IEC/SC45A experts noted that if what is meant by ‘determinist’ is the existence of a maximum and a minimum response time, the word predictable should be used. See 7.76. See also the proposal to introduce definition for determinism and the proposal for predictability.			x	See IEC 62566, clause 6.3 “The requirement specification shall specify that the function of the HPD is deterministic by design.”
104	DEU	33	7.159	7	159	Add: Particularly the potential of systematic	Consider tools as a potential source for CCF	x			

						failures should be considered.					
105	DEU	34	7.160, 1st bullet	7	160	Delete bullet ~~Tools that have the ability to introduce faults need to be verified to a greater degree than tools that do not have that capability;~~	Each tool can be considered in general as a source to introduce faults.			x	Tools that only record outputs during testing, for example do not have the capability to introduce faults. Than modify the text to: **"… than tools for which is demonstrated that they do not have that capability. "** Reason: There might be e.g. unused tool interfaces or non-disclosed software options for bi-directional data transfer. Therefore a justification/ demonstration is recommended to relax verification activities.
339	USA	48	7.166 7	7	166	Add sections that address the potential for counterfeit devices being introduced by the acquisition process.	QUALIFICATION OF INDUSTRIAL DIGITAL DEVICES OF LIMITED FUNCTIONALITY FOR SAFETY APPLICATIONS – This section does not address detection of counterfeit devices.			x	Paragraph 6.93 encompasses the idea of counterfeit parts, but generally protection against counterfeiting is a procurement, not a qualification function. Procurement is discussed in the GS-R-3 series of documents. The implications of counterfeiting on I&C functionality will be discussed in the forthcoming I&C computer security document.
271	IEC	54	7.168	7	168	Modify as follow: "The only interface between a device of limited functionality and the other parts of I&C systems is the transmission or receipt of a value representing a physical quantity or command (e.g. pressure, open/close order) according to a standardized format (e.g. 4-20 mA, 0 – 5V or dedicated simple communications interfaces)."	IEC/SC45A experts consider that the definition is too restrictive compared to the coming IEC/SC45A standard on this topic.	x	Partly accepted. Dedicated simple communications interfaces is too vague and is not an example of a standardized format.		
362	PAK	11	7.168 7	7	168	Following statement may be included: Industrial digital devices of limited functionality should be compatible with the respective I&C system of concern.	Compatibility of industrial digital devices of limited functionality with respective I&C system should also be considered in the design as these devices are made part of the overall I&C system.	x	This should be part of component requirements. Consequently, paragraphs 2.96 to 2.111 were revised to clarify that they apply also to I&C components		
106	DEU	35	7.174, last bullet	7	174	Add: . Statistical testing applied to hardwired I&C	Quantitative methods are not state of the art in safety assessment of SW-based I&C in the nuclear field; statistical testing is not commonly accepted as compensatory evidence in the nuclear safety domain.		OPEN ITEM		
272	IEC	55	7.174	7	174	Delete "Statistical testing"	IEC/SC45A experts noted that "statistical testing" is not a widely recognised technique.		OPEN ITEM		

Formatiert: Schriftart: Fett

							Such technique has been used only in a small number of nuclear projects.					
351	CHW	6	8.4 new after	8	4	**The design of the HMI-architecture shall not jeopardize the overall design of the overall I&C architecture. Especially, no safety function shall be actuated by means of a non-safety HMI-equipment.** **.**	This is an important point that was already discussed in some projects/areas.			x	This comment is already addressed in paragraphs 6.45 to 6.57. It is not so much a HMI issue as an issue of independence of the systems behind the HMI.
273	IEC	56	8.12	8	12	To be modified as follows " (…) to the extent that ~~maintenance~~ execution of the fundamental safety functions cannot be ensured."	IEC/SC45A experts noted that the term "maintenance" has been given a specific meaning in the other parts of the guide. Using it here as a verb might lead to confusion.	x			
217	UKR	2	Page 92, line 27, after para 8.12 add a new one	8	12	The design of the control rooms should take into account the security recommendations (IAEA NSS No 13/INFCIRC/225/Rev.5, pares 5.8, 18, 19, 36)	Security recommendations on protection of control equipment and rooms are stated for physical protection alarm stations but also advantageous and applicable for nuclear facility control systems.			x	These topics are in the domain of IAEA's nuclear security organization. A document specifically on I&C security is forthcoming.
59	CAN	59	8.15 (GR)	8	15	The supplementary control room that is physically and electrically separate from the main control room should contain information displays for monitoring plant conditions as needed to support the response to events which may result from situations that necessitate evacuation of the main control room.	The supplementary control room should contain information displays for monitoring plant conditions as needed to support the response to events which may result from situations that necessitate evacuation of the main control room. Comment: To emphasis the requirement of SCR, additional text included			x	The requirement for physical and electrical separation is already in SSR 2/1 requirement 66. It does not need to repeated as guidance.
107	DEU	36	8.17	8	17	Add: Accessibility in accident situations should be considered.				x	This is already addressed in paragraphs 8.90 through 8.93 OK
60	CAN	60	8.31 (RJH)	8	31	Consider pre-validating computer guidance.	Any computer guidance provided must be fully pre-validated for all situations.			x	Procedure development including computer-based procedures is in the domain of the Operational safety standards
61	CAN	61	8.53 (RJH)	8	53	Consider revising text.	This appears to be in partial conflict with 8.4.			x	There is not conflict. Paragraph 8.4 does not exclude the possibility that functions that operators can be precluded from executing functions that are not necessary (e.g,, deleterious to) safe operation of the plant.
274	IEC	57	8.56 and 8.57	8	56	Delete	IEC/SC45A experts noted that such recommendation would significantly complicate the displays, especially digital displays and could be detrimental to the			x	Since a given bit of data can come from many different sources the operators should be aware of the dependability of the source. This is an established principle

							ergonomic of the HMI. Furthermore, what really matter is that the information presented to the operators on the displays have a qualification level consistent with the use of these information. This has to be verified carefully with the operating procedures of the plant.				even for hardware control boards where the source of the data for a given value is displays. The comment would also seem to imply that the operator does not need to know the instrument number associated with the display.
108	DEU	37	New par. After 8.58	8	58	Add: <u>The HMI design should support the development of a common situational awareness of the control room crew, e.g. via large wall mounted plant status displays.</u>		x			
275	IEC	58	8.74	8	74	-Delete the following sentence “The I&C should alert the operator to failure of an automatic control or protection function”	IEC/SC45A experts suggested to remove this clause. There are two reasons to delete this clause. Protection functions are required in accidental situations. In such situations, the operator usually follows a "state approach", that is to say that he will base his actions on the current status on the plant derived from the analysis of the main plant parameters. This means that the alarm that is suggested to be created by this clause will be non relevant to the operator. Moreover, such alarm may be very difficult to elaborate considering that the success criteria may depend on the accident.	x			
67	CAN	67	(RJH)	9	(RJH)	Please correct the spelling of names and affiliations of earlier contributors	If not already corrected, “Hohendor” should be “Hohendorf” and “B. Fichman” should be “E. Fichman”. Also, Hohendorf, Fichman and Babcock are associated with Ontario Power Generation.	x			
62	CAN	62	9.2 (RJH)	9	2	Limit the complexity of software used in safety systems.	An explicit objective of software implementation should be to limit the complexity of software used in safety systems.			x	See paragraphs 9.22 and 9.23.
63	CAN	63	9.9 (RJH, GR))	9	9	Replace: “hav” with “have”.	Editorial	x			
109	DEU	38	9.9	9	9	Word: … should <u>hav**e …**</u>		x			
277	IEC	60	9.9	9	9	To be modified as follows “The developers of	Typo	x			

						software requirements should have an appropriate (…).”					
110	DEU	39	9.11 g, h	9	11	Combine the both par. as following: Identify and meet the supporting software requirements needed to ensure that the required level of reliability and availability are achieved. The level of reliability might be defined qualitatively. Some member states use quantitative requirements.	Quantitative methods are not state of the art in safety assessment of SW-based I&C in the nuclear field.		OPEN ITEM		important
276	IEC	59	9.12	9	12	Delete	IEC/SC45A experts noted that the “Reliability model” is not defined in the document and paragraph 2.88 is sufficient and clearer.		OPEN ITEM		
111	DEU	40	9.17, 1st line	9	17	Delete: ~~correct~~ or add a note to declare that correct does not mean freedom from faults	If ever achievable in practice, to prove SW correctness might be the objective of validation (after HW and SW integration).	x			
278	IEC	61	9.33	9	33	Modify as follow: “The software design of safety systems should ensure deterministic operation (including in terms of the functional and timing response to particular inputs) and predictable behavior for other systems important to safety, see paragraph 7.76.”	IEC/SC45A experts noted that the determinism and predictability are not the same thing in some member states. Consistently with IEC/SC45A standards, it is proposed to recommend a design ensuring deterministic behavior only for safety systems.	x			
64	CAN	64	9.36 (RJH)	9	36	Add to the end: “and the cause of the fault can be ascertained.”	Clarification and completeness			x	Logs are already recommended. It is difficult to ensure that fault causes can be ascertained.
112	DEU	41	9.42 a, 1st line	9	42	Delete: ~~and design~~	If ever achievable in practice, to prove SW correctness might be the objective of validation (after HW and SW integration); Design verification is a different step which has to be finished before the implementation step can start.			x	The statement asks for completeness with respect to design, not completeness OF the design. Therefore, the existing statement is appropriate. The statement also asks for **correctness** of the **design** which is difficult to demonstrate. There are following proposals to rephrase the text accordingly: - delete either **design** or **correctness** or - add a note such as proposed in DEU 40 German comment on 9.42 d, 1st line is missing: Not clear what is meant with “maximized”;

Formatiert: Schriftart: Fett

Formatiert: Schriftart: Fett

Formatiert: Schriftart: Fett

Formatiert: Unterstrichen

Formatiert: Schriftart: Fett, Unterstrichen

Formatiert: Hochgestellt

											associated criteria are missing?
65	CAN	65	9.49 (RJH)	9	49	Add to the end: "These characteristics must be balanced with the need for simplicity in implementing safety systems."	Clarification and completeness			x	The referenced paragraph does not deal with implementation of safety systems, but with selection of programming language. Therefore, the requested change is not appropriate. Simplicity is already dealt with in paragraph 9.22
279	IEC	62	9.60	9	60	Delete	IEC/SC45A experts noted that there is no consensus on that topic and the practice presented as widely accepted is singular to a few member states.	x			
340	USA	49	9.62 9	9	62	Revise section to be consistent with the body of knowledge on V&V (e.g., see IEEE Std 1012-2012).	SOFTWARE VERIFICATION AND ANALYSIS – This section should address both verification and validation. Not only should software be verified that it has been built correctly, but it should be validated that the software will perform the job for which it is intended. Activities such as dynamic testing (see , §9.66c on page 107) and §9.73 - §9.78 are validation activities.			x	Paragraphs 9.66, and 9.73-9.78 are already included in the section on validation.
280	IEC	63	9.66	9	66	Modify by "b. Static analysis of the source code belonging to safety systems, and"	IEC/SC45A expert reminded that the general use of static analysis as defined by IEC 61508-7 B.6.4 does not correspond to the current state of the art. According to state of the art practice, it may be used on safety systems.		OPEN ITEM		
282	IEC	65	9.66, 9.67 and 9.68	9	66	IEC/SC45A experts propose that if static analysis are maintained in the document, first there is a definition given (see the one of IEC 61508) and that their use be limited to some parts of safety systems.	IEC/SC45A experts noted that the general use of static analysis as defined by IEC 61508-7 B.6.4 does not correspond to the current state of the art. It is sometime used for part of some safety systems. Static analysis/ Aim: To avoid systematic faults that can lead to breakdowns in the system under test, either early or after many years of operation. Description: This systematic and possibly computer-aided approach inspects specific static characteristics of the prototype system to ensure completeness, consistency, lack of ambiguity regarding the requirement in question (for example construction guidelines, system		OPEN ITEM		

							specifications, and an appliance data sheet). A static analysis is reproducible. It is applied to a prototype which has reached a well-defined stage of completion. Some examples of static analysis, for hardware and software, are: consistency analysis of the data flow (such as testing if a data object is interpreted everywhere as the same value); control flow analysis (such as path determination, determination of non-accessible code); interface analysis (such as investigation of variable transfer between various software modules); dataflow analysis to detect suspicious sequences of creating, referencing and deleting variables; testing adherence to specific guidelines (for example creepage distances and clearances, assembly distance, physical unit arrangement, mechanically sensitive physical units, exclusive use of the physical units which were introduced). Usually in standards static simulation model are recommended. During a static analysis the code is not executed (not tested). Static simulation model is representative of a system at a certain point of time. Dynamic simulation model is a representation of a system as it evolves over time.					
281	IEC	64	9.67	9	67	Modify by "**When it is applied,** static analysis should be performed on the final version of the software."	IEC/SC45A experts noted that according to IAEA's answer to IEC/SC45A comment on revision D this 9.67 requirement (former 10.73) aims at highlighting that analysis performed should be done on the final version of the software, the one that will be installed. It does not mean to make the use of static analysis mandatory in all situations. The proposed reformulation makes the requirement's purpose clearer.		OPEN ITEM		

283	IEC	66	9.68	9	68	Modify as follows: “Static analysis includes a wide range of techniques such as verification of compliance with design, coding, and standards constraints; control, data and information flow analysis; symbolic execution; and formal code verification.”	IEC/SC45A experts noted that there is no consensus on the type of static analysis to be performed.		OPEN ITEM		
66	CAN	66	9.73 (RJH)	9	73	Consider revising text.	The best test strategy may combine both bottom-up and top-down aspects.			x	The statement does not exclude the possibility of doing both.
284	IEC	67	9.79	9	79	Modify as follows: "Verification personnel should be independent as required by clause 2.72."	IEC/SC45A experts noted that depending on the importance of the software with regard to the safety, the verification could be performed by someone independent from the designer but belonging to the same team (for items not important for safety). The original formulation of the clause may be too strong. The formulation of clause 2.72 is less restrictive.	x	Used wording from 2.72.		
285	IEC	68	9.95	9	95	Delete	IEC/SC45A experts noted that the “alternative approach” mentioned in this paragraph is not clear at all. Paragraph 9.92 to 9.94 defines the approach for Pre-developed software not necessarily developed to nuclear standards.	x			
341	USA	50	9.97 9	9	97	9.97 s Third party assessments should be performed concurrently with the software development process.	§9.97 states, “A third party should assess safety system software.” The number of assessments and the timing of the assessments are critical. If the assessment is performed only once, then the assessment must be performed at the end of the development effort, when changes to the system resulting from assessment findings may be too expensive or delay delivery too much, thereby resulting in the developer arguing why the changes cannot be performed, instead of making the needed corrections. Assessments should be performed regularly through the development life cycle so that changes can be made as issues arise.	x			
286	IEC	69	REFERENCES	10	REFERENCE	Modify reference [1] to point to the version published in January 2012	IEC/SC45A experts noted that extract from the draft version of reference [1] given in the text of this guide has to	x			

					S		checked to be sure they are aligned with the published version of reference [1].				
287	IEC	70	REFERENCES	10	REFERENCES	Add reference [23]	IEC/SC45A experts noted that reference to [23] is made in 6.156.	x			
288	IEC	71	REFERENCES	10	REFERENCES	Add reference [34]	IEC/SC45A experts noted that reference to [34] is made in 7.67.	x			
289	IEC	72	Annex	11	Annex	IEC/SC45A propose to add the following relationship between IEC or IEEE standards and the topic area of this guide: HFE of MCR : IEEE 1082 HDL devices : IEC 62566 Qualification of industrial devices : IEC 62671 Supplementary control rooms: IEC 6095	IEC/SC45A experts appreciated the fact that IAEA integrated this annex in this Safety Guide to help the reader to identify relevant IEC and IEEE standards.	x			
292	IEC	73	Glossary	12	Glossary	IEC/SC45A experts are aware that some discussions currently held in the OECD/NEA/MDEP/DICWG have to be considered to finalize a definition but they propose to consider the following proposal as a basis in order to develop a finalized definition to integrate in the glossary of this safety guide and then to have it taken into account for the next revision of the IAEA safety glossary. System validation: Confirmation by examination and provision of other evidence that a system fulfils in its entirety the requirement specification as intended (functionality, response time, fault tolerance, robustness).	IEC/SC45A experts noted that the IAEA safety glossary contains the following definition : Validation: The process of determining whether a product or service is adequate to perform its intended function satisfactorily. Validation is broader in scope, and may involve a greater element of judgment, than verification. Computer system validation: The process of testing and evaluating the integrated computer system (hardware and software) to ensure compliance with the functional, performance and interface requirements. The IAEA definitions completely lack the concept of a phase model. This is why the definition of validation by IAEA introduces the vague statement that “validation is broader than verification”.	x			

							In fact, such a statement should not be part of a definition. Than the definition proposed by IEC/SC45A experts specifies the reference of validation, namely the requirement specification, whereas the IAEA definition only refers to the “intended function”.				