Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
	Introduction		
8.1.	8.1.1 Objectives & General Description	(e) To identify faults that are subject to detailed safety analysis in Chapter 16.	Where are these faults explicitly identified in this Chapter?
			Response: Failures of Instrumentation or instrumentation systems are not detailed in this chapter. They are considered fully in Chapter 16, 'Safety Analysis' both in terms of their initiation of spurious operation of Safety Systems and effect on accident sequence progression when the failure is unrevealed. The instrumentation systems, which have been confirmed for use in the RRRP, are sufficiently reliable (and based on triplicated redundancy) that no additional faults to the ones dealt with in Chapter 16 have been identified.
8.2.	8.1.2.1 Reactor Protection Systems	The First Reactor Protection System (FRPS) is implemented using computer technology, qualified for use in safety shutdown applications.	The wording suggests that this system has already been implemented. What stage of development is the system at?
			Response: At the time of issuance of the PSAR the contract between INVAP and Ivensys had not been signed although it was imminent. The FRPS is a Triconex system. Detailed engineering has not yet started.
8.3.	8.1.2.1 Reactor Protection Systems	Figure 8.1/2 shows a diagram of these systems and their links.	What is the Concentrator Field Unit? It appears that it is common to the FRPS, SRPS, and PAM (Figure 8.1/2)

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: The Concentrator Field Unit is an INVAP term and would be analogous in function to the Foxboro Fieldbus modules (such as FBM 204 and FBM 207 etc) with associated isolation. The drawing will be revised to reflect the Foxboro/Triconex systems and more clearly show the independence of the FRPS, SRPS and PAM. There is nothing in common between the FRPS and SRPS. The SRPS and PAM use separate Foxboro Spec 200 analogue equipment while the FRPS is a Triconex system. This is stated throughout Sections 8.1 and 8.2. Reactive Review Comment 1.38 sought more information on the relative reliability claims for the FRPS and the SRPS. The reliability of the FRPS is claimed to be 10E-3 failures per demand. This is a standard value that has been widely applied to digital safety systems and is based on the SIL 4 (Safety Integrity Level) as per IEC 61508. This is considered to be a conservative assumption since the Triconex system has a stated MTTF of greater than 200 years using the MIL-STD failure rates as defined in IEC 61508. In addition the system currently has over 100 million hours of error free service, including four applications at Kozloduy NPP units 1 to 4 in Bulgaria. Foxboro's SPEC 200 (used within the SRPS) is the most widely used control system in the nuclear industry. It was nuclear qualified in 1977 and has provided control to over 120 nuclear power plants around the world.

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.4.	8.1.2.5 Reactor Containment System	The Reactor Containment Systems are systems that isolate the containment when high activity is detected in the reactor building stack, and ensure the containment is unaffected by over or under pressure conditions.	Where will the detectors be located within the stack? Should containment be actuated when high activity is detected in the water?
			Response: The exact location of the sampling points has not yet been finalised. Maintenance, sensor time response, and iodine plateout will factor into the location. As long as the activity is contained in the cooling systems there is no reason to have an automatic containment isolation actuation. This could be left to the operating staff to determine if a release to the atmosphere is possible.
8.5.	8.1.3 Identification of Instrumented Safety Class 2 Systems	8.1.3.8 Emergency Make-up Water System	Should the Emergency Make-up Water System be classified as a Category 1 Safety System?
			Response: The classification of systems is not in the I&C scope. See Chapters 2, 6 and 16 of the PSAR.
	Reactor Protection Systems		
8.6.	8.2.2.1 General Requirements	To limit the uncontrolled release of radioactive materials by reliably initiating protective actions on gross failure of either the fuel cladding or on detection of the release of fission products from the PCS.	The word "either" should be before "gross failure" or removed entirely. Why wait until release is from the PCS, why not as soon as high activity is detected in the PCS?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: Noted, correction will be made. Gross failure of the fuel cladding will result in a release of fission products into the PCS that will be detected by the active liquids monitor (ALMO). If the activity reaches the top of the pool as fission products rise, protective action Trip 1 is initiated by the FRPS. Similarly if fission products are released from the PCS to the air then a different set of protection actions will be automatically initiated such as containment isolation. Ref: Sections 8.2.3.1.7.2 and 8.7.3.2.2.3
8.7.	8.2.2.1 General Requirements	Redundancy shall be provided, based on the potential for undetected failures that could degrade reliability.	Does this mean that a study has been completed that identifies the potential for undetected failures? Is the report available?
			Response: All SRPS and FRPS trip circuits and actuation circuits employ triple redundancy. All PAM circuits are duplicated. FMEAs will be completed on all safety circuits. Ref: Chapter 2, Section 2.5.1.1
8.8.	8.2.2.1 General Requirements	There shall be sufficient electrical and physical separation between redundant instrumentation and control equipment monitoring the same parameter…	Why state "the same parameter"? Should not all redundant systems have sufficient separation?
			Response: All safety trains are separated to IEEE 384 requirements. The "same parameter" is stated to imply that separation is from the sensor through to voting logic input, for each parameter such as temperature, pressure flow etc.

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.9.	8.2.2.1 General Requirements	The following requirements reduce the probability of RPS operational reliability being degraded by operator error:	Requirements 18, 19, 20, 21, 22, 23, 24, 25, 27, 28 do not appear to relate to "operator error" induced events.
			Response: The discussion in these sections is about operator actions being based on clear and accurate information that would minimise operator error.
8.10.	8.2.3 Reactor Protection Systems Description	The only initiating protective function associated with this system is to shut down the reactor by the partial draining of the reflector vessel, SSS (Trip 2).	Why doesn't the SRPS initiate containment isolation?
			Response: All CIS functions are initiated by the FRPS only. Diversity is not a requirement. The valves can be manually closed if required. Ref: Section 8.4.1.3
8.11.	8.2.3.1.1 Shutdown Systems	The position of the SSS isolation valve is monitored by a limit switch located at the open position.	How many limit switches are there (two in series)? How many isolation valves are there?
			Response: Figure 8.4/1 shows three position switches on one isolation valve. There is an interlock preventing reactor start-up if this valve in not fully open. This valve is additional to the six trigger valves. These are normally closed and are opened by the SRPS on demand

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.12.	8.2.3.1.2.1 Primary Cooling Circuit	The inlet RTDs are located in the PCS inlet pipeline to the core and the outlet RTDs are located in the pipeline taking water from the chimney to the decay tank. These RTDs are also used to calculate the differential temperature across the core.	There is no diversity in sensing devices (all are RTDs) Will all the RTDs be from the one manufacturer?
			Response: There are no diversity requirements for these temperature measurements. RTDs are more accurate than other methods such as thermocouples, and for measuring core delta temperature this becomes a key factor. All FRPS RTDs will be from the same manufacturer. Note that where the SRPS and FRPS measure the same parameter then diversity is an issue however there are no temperature measurements that are monitored by both FRPS and SRPS
8.13.	8.2.3.1.2.1 Primary Cooling Circuit	Each train of the SRPS and FRPS share common high and low pressure taps. This arrangement ensures that a failure in one pressure tap would only result in the loss of one train from both the FRPS and SRPS and both systems would still be functional in a one out of two mode.	The FRPS and the SRPS are argued to be independent, however here appears to be an example of system interconnection. Please provide a list of all situations where the RPS share measuring devices.

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: In the sentence before what is listed it states " There are two sets of three differential pressure transmitters one set for the FRPS and one set for the SRPS". There is no sharing of measuring devices. Furthermore these transmitters will be of different types such as capacitance, resonant wire or piezoelectric to name a few. The FRPS and SRPS are functionally independent. They share no sensors, measuring devices or cables in common. However they share common cable routes, equipment rooms, and power supplies on a train basis. For core delta Pressure, they share common pressure taps, again on a train basis due to the space restrictions imposed by the core design. Any single failure would not inhibit either the FRPS or SRPS from fulfilling its safety function. Presently there are no other areas where pressure taps are shared. Ref: Section 8.2.4.3.1
8.14.	8.2.3.1.2.3 Emergency make-up Water System	The tank isolation valves are monitored by three limit switches located at the open position.	Three limit switches per tank or per valve?
			Response: Per valve; there are no limit switches associated with tanks.
8.15.	8.2.3.1.3 Nucleonics Channels	Additionally the SRPS and FRPS trains, in which these channels are located, are diverse and share no instrumentation in common.	Does it mean that instrumentation performing the same function (in different trains) are from different manufacturers?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: No, it means that the SRPS and FRPS share no equipment in common. Diverse techniques are employed in the measurement of the parameters for the FRPS and SRPS. The FRPS trains and the SRPS trains each comprise three triplicated, identical channels for each parameter. This is stated throughout Sections 8.1 and 8.2
8.16.	8.2.3.1.3.1 Start-up Channels	They (Pulse fission chambers) are housed in containers that provide electrical isolation and prevent ingress of moisture around the detectors in order to keep them in a suitable environment.	Will the containers be water-tight? Should "Campbell" processing be used in Start-up channels?
			Response: Yes they will be water tight No Campbell processing is a worthwhile technique in certain applications (for wide range). For narrow range startup channels the low sensitivity to high gamma fields in addition to the wide range afforded by Campbelling is not an issue.
8.17.	8.2.3.1.3.2 Wide Range Logarithmic Channels	The detector signal is sent with minimal interference, to the preamplifier module, which is located beyond the radiation field of the core, (as near as possible to the detector in a dry position, outside of the reactor pool).	Where are the detectors located? Are they separated by an appropriate distance? How will "minimal interference" be achieved? What is the testing criteria?
			Response: See Section 8.2/4 through 8.2/6. Separation is adequate. Minimising interference is accomplished by reducing the cable length, proper shielding and distance from noise sources such as large motors and power cables.

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.18.	8.2.3.1.3.3 Power Channels	Detector output current lies in the range of 10-11 to 10-4A.	Is "output current lies in the range of 10-11 to 10-4A" a typing error? Where are the detectors located? Are they separated by an appropriate distance?
			Response: This is not a typing error however it is meant to be read as 10^{-11} to 10^{-4} Amperes. This is a typical current range for nucleonics. See Figures 8.2/4 through 8.2/6. Separation is adequate
8.19.	8.2.3.1.4 Seismic System	Two sets of three seismic monitoring systems are provided, one for the FRPS and the other for the SRPS.	Where are the detectors located?
			Response: Exact location of the sensors has not yet been determined this will be done during the detail engineering phase
8.20.	8.2.3.2.3 Voting Generation	The voting criterion is two out of three channels in the tripped state.	Are these signals then put through an additional 2oo3 logic system (FFAL)? (see Figure 8.2/7)
			Response: The Triconex system is based on a triplicated 2oo3 system for each single input. This ensures that even a failure internal to the Triconex will not affect the output of a single channel. The output of each of the triplicated channels is again voted on 2oo3 to produce the safety signal. There is a 2oo3 voting scheme in FFAL
8.21.	8.2.3.2.4 Protection Logic Generation	The resulting Protection Action Initiation Signals (PAIS) and Protection Interlock Initiation Signals (PIIS) are the output of the First Reactor Protection System.	Are the PAIS and PIIS signals duplicated and sent via different paths?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: Each redundancy has one output. Last voting is done in FFAL and SFAL. The resulting three PAIS and three PIIS signals are the output of the FRPS. These are voted on 2 out of 3 logic to actuate the FSS. Ref: Section 8.2.3.2.4
8.22.	8.2.3.3.3 trip Comparator Unit	The trip set points are fixed using digital to analogue converters combined with hard-wired components.	The SRPS meant to be a hardwired system. It appears to be a mixture of hardwired and solid-state devices, is this correct? (see 8.2.4.3.1)
			Response: The Foxboro Spec 200 comparator module is analogue. There are no digital signals involved in this system. Solid state devices can be either digital or analogue
8.23.	8.2.3.3.5.2 Protective Logic	The protective logic within the VPLU implements the required logic equations and conditions between the voted signals to generate the final PAIS. It also has a self-verification system that is based on the channels' dynamic characteristics.	The SRPS meant to be a hardwired system. It appears to be a mixture of hardwired and solid-state devices, is this correct?
			Response: See Above
8.24.	8.2.3.3.6 Voting and Protective Logic Interface Unit	The function of the VPLIU is to provide electrical isolation between the destination units.	Will these units comply with IEEE 384 and Class 1E requirements?
			Response: As stated in Section 8.2.3.3.2 the opto isolators will comply with IEEE 384 and are Class1E qualified isolation devices

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.25.	8.2.3.4.1.1 First Shutdown System Logic Compressed Air Storage Tank Pressure	Once the reactor is in operation, this interlock shall be inhibited.	Why is this interlocked inhibited during operation?
			Response: During Start up Operation, this interlock inhibits rod withdrawal. Reactor Operation is enabled by tank pressure. Once reached, this condition is locked, thus enabling rod withdrawal. If after this moment a low pressure is measured in the tank, it will be announced to operators using visual and acoustic alarms
8.26.	8.2.3.4.1.3 Primary Cooling System Logic	The Trip 1 action initiated by Primary Coolant Flow and Core Pressure Difference parameters is disabled when the reactor operates in low power mode.	How is Low Power Mode selected?
			Response: Via the operational mode, keyed switch on the main control panel this will be further developed during the detailed engineering phase Ref: Section 8.2.3.4.1.7
8.27.	8.2.3.4.1.6 Reactor and Service Pools Cooling System Logic	These analogue parameters are acquired in the RSPCS piping between the heat exchanger, and the reactor pool, and measures the cooling water circulation flow. It triggers Trip 1 by a low flow when the RSPCS flap valve is closed and the reactor is not in a low power mode	Logic Diagram appears to be wrong (Figure 8.2/15) – a Trip 1 occurs when the reactor is in Low Power Operation. Is this correct?
			Response: The logic is correct the wording is wrong. It should have stated that the reactor is in a low power operation

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.28.	8.2.3.4.1.7 Nucleonic Instrumentation System Logic	The pre-set values are disabled when the Power Range condition is enabled and neutron flux reaches 10% of the high-trip value.	Is this a generally accepted practice in reactor operations around the world?
			Response: Yes this is a common practice. For example Westinghouse power reactors require a manual disable of the startup trip when the intermediate channels have a set minimum value reading, and similarly the intermediate channels are manually disabled when the power range instrumentation is at an acceptable level. On HIFAR's low power instrumentation, used after a lengthy shutdown, the high flux trips are disabled when the log period channels read on scale.
8.29.	8.2.3.4.2.2 Primary Cooling Circuit Figure 8.2/23 Second Reactor Protection System Trip Logic	Power Operation signal	How is the "Power Operation" signal generated? Does it come from the RCMS? Is it from the key switch (see 8.2.3.4.1.7 Nucleonics - Operational States)
			Response: The Power Operation signal is from the operational mode, keyed switch on the main control panel this will be further developed during the detailed engineering phase. Ref: Section 8.2.3.4.1.7
8.30.	8.2.3.4.4 Data Communication to Reactor Control and Monitoring System	Safety parameters, trip settings and the results of the self-checking process of the RPS are provided to the RCMS, through one way read only, electrically isolated interfaces.	Will these units comply with IEEE 384 and Class 1E requirements?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: As stated in Section 8.2.3.3.2 the opto isolators will comply with IEEE 384 and are Class1E qualified isolation devices
8.31.	8.2.3.5 Reactor Protection Systems Software Development Verification and Validation Process	Independent verification and validation tasks are performed as a required stage in software design…	Is there a Flow Chart available to demonstrate the process?
			Response: The verification and validation (V&V) Plan will follow IEEE-1012 recommendations. The Flow chart is outlined in this Standard. At present the V&V Plan is under discussion with INVENSYS
8.32.	8.2.3.5.1 Verification and Validation Processes	Task Reports	The titles of the Task Reports do not match clearly with the Outputs identified in Table 8.2/2.
			Response: Report names will be changed to line up with names in the table. These names could change as the programs get developed although the intent will remain
8.33.	8.2.3.5.1 Verification and Validation Processes	Verification and Validation Final Report: This report will be issued at the end of the Installation and Commissioning Activity	The Validation process is not clearly established. When does validation of the software occur?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: Validation of the software will be completed during factory acceptance tests and by INVAP doing an integrated test of all systems at Bariloche. This also extends to the plant installation and commissioning stage
8.34.	8.2.3.6 Reactor Protection Systems Testibility	Testing of individual trains while the reactor is operating is accomplished by tripping the output of the channel being tested, if required, or bypassing the equipment, if safety requirements and operating limits allow.	Please provide a listing of equipment that will be bypassed for testing purposes.
			Response: All analogue input signals will be tripped during testing. There are 20 analogue input signals in each redundancy at the present moment. No equipment bypassing is considered during testing.
8.35.	8.2.4.1.1	The selection of the trip settings has been developed through analytical modelling, and experience gained in the development of the initial safety system settings.	Where are the settings stated?
			Response: Settings have not been finalised and are part of the detail engineering. "has been" shall be changed to "will be". See also Chapter 17.
8.36.	8.2.4.1.2	In addition, the FSS action initiated by the reactor pool area radiation monitors satisfactorily limits the radiological consequences of failure of the fuel plates and irradiation facilities by initiating a Trip 1 action.	If there is gross failure of Fuel Cladding, will the Control Rods be able to drop?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: Fuel failure effects on control rod functions are described in Chapter 16 Additionally: The Control Rods will be able to drop because they move inside the Control Rod Drive Box. Non-credible, gross, core-wide distortion of fuel plates would need to be postulated to produce sufficient distortion of the Guide Box to overcome the pressure exerted by the pneumatic system on the Control Rods. This event is sufficiently unlikely as to render it beyond design basis.
8.37.	8.2.4.1.21	Requirement 23: Local instrumentation shall be provided to monitor the performance of equipment, which requires regular maintenance. A regular surveillance and maintenance program for all equipment requiring periodic support is provided.	Where is the surveillance and maintenance program detailed?
			Response: Safety related equipment will have their surveillance and maintenance requirements outlined in the OLCs. All others will be part of the calibration program that is part of the ILS requirements. Maintenance requirements are based largely on vendor recommendations and will be developed during the detailed engineering phase. Ref: Chapter 13, Section 13.6 and Chapter 17.

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.38.	8.2.4.1.30	Some software verification and validation techniques used during software design tasks include algorithm analysis, database analysis, sizing and timing analysis, and simulation. Some software techniques used during code verification and validation tasks are control flow analysis, database analysis, regression analysis, and sizing and timing analysis.	The Verification and Validation processes appear to be intermixed. IAEA Technical Report Series No. 384 indicates that Validation occurs at the final system testing stage. There is no reference to IEEE 1012-1986 Standard for Software Verification and Validation Plans, will this Standard be used?
			Response: The verification and validation processes are not intermixed. The Verification and Validation Plan will be produced early in the detail engineering phase. The Software Verification and Validation Plan will follow IEEE-1012. The list of reference in Section 8.1.4.2 will be amended.
8.39.	8.2.4.1.36 Conformance to General Requirement 41	The RPS are based on an "as-simple-as-possible" criterion relying on a structured development process that includes; requirement specifications, prototypes and simulations when needed, as well as reviews and testing for all custom design components.	Please provide a list of custom designed components.
			Response: The FRPS was originally based on a custom INVAP designed platform. With the signing of a contract with INVENSYS for the supply of the Triconex qualified platforms for the FRPS this is no longer applicable. INVAP will be supplying the following custom designed components: Start-Up Channel, Power Channel and Pool Open End Gamma activity channel.

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.40.	8.2.4.3.1 Conformance to Additional Requirements 1 and 2	Passive components such as cables trays and some instrument piping (that measuring core pressure difference) are shared between the FRPS and SRPS while maintaining separation of the three redundant trains.	To what extent are cable routes and same piping shared between the FRPS and SRPS? How is the sharing of cable trays and piping kept to a minimum? Please clarify compliance with IEEE class I system requirements.
			Response: Compliance with the IEEE Class 1E requirements is maintained by the three train concept. It is not a requirement of IEEE 384 to separate safety systems. Failure of a complete train, which could fail one train of both FRPS and SRPS, does not affect either safety systems capability to safely protect the plant. The only instance of sharing of tubing is in the core delta pressure measurement and this again is a sharing by train basis. All cable raceways and power supplies are shared on a train basis by the SRPS and FRPS and PAM (for two trains only).
8.41.	8.2.4.3.5 Conformance to Additional Requirement 6	Requirement 6: The RPS shall have sufficient recording instruments to monitor reactor parameters during and following operational occurrences and accident conditions. The RPS communicate the status information on all their parameters to the RCMS, where the information is displayed and stored for future retrieval	Does this mean that the RPS themselves have no recording instruments?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: The FRPS has integrated SOE (sequence of events) capability (TRICON module). The control program manages the events collection. I addition, all safety process variables (inputs to the FRPS) and outputs of voting logic are sent to the RCMS through a digital communication channel for processing, display and data archive. For the SRPS all safety process variables and outputs of voting logic are sent to the RCMS through isolation devices (analogue and digital) for processing, display and archive. The SOE (Sequence of Events) is performed by means of RCMS capability)
	First Shutdown System Instrumentation		
8.42.	8.3.3.2 Failure Mode and Effects Analysis	A Failure Modes and Effects Analysis (FMEA) has been conducted for the FSS with results indicating that instrumentation failures do not induce any significant effect on system performance.	What is the reference document or is this included elsewhere in the PSAR?
			Response: The results of the FMEA for the FSS are included in Chapter 5, Section 5.5.3.8. The results of the FMEA for the CRDM are included in Chapter 5, Section 5.5.2.8.
	Second Shutdown System Instrumentation		
8.43.	8.4.3.1 Safety Parameters	The following are the main safety parameters handled by the SSS:	Section 8.3.3.1 for FSSI detailed the number of proximity switches etc. Here there is no mention of how many level switches etc are used. Why is there a difference in the level of detail?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: This section lists parameters monitored by the SRPS. The number of devices used in the SSS can be seen on the supplied figure 8.4/1 except for the triplicated reflector vessel temperature detectors, which were a later addition and did not get incorporated into the drawing in time for issuance with the PSAR. A comparable table to the FSS will be provided showing all sensors associated with status indication of the system. SRPS parameters are described in Section 8.2.
8.44.	8.4.3.2 Failure Mode and Effects Analysis	A Failure Modes and Effects Analysis (FMEA) has been conducted for the SSS with results indicating that instrumentation failures do not induce any significant effect on system performance.	What is the reference document or is this included elsewhere in the PSAR?
			Response: The results of the FMEA for the SSS are included in Chapter 5, Section 5.5.4.9.
8.45.	8.4.4.1.1 Conformance to General Requirements 1 and 2	Operators have access to all signals through the MC of the SRPS and RCMS.	Are the signals also available in the ERC and locally ?
			Response: Yes all signals are available at the ECC as well. Local indication is not available for all signals however since all the SSS instrumentation is fed into the RCMS then where ever there is access to the RCMS VDUs all signals can be monitored. Refer to Section 8.15.1

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
	Reactor Containment Systems Instrumentation		
8.46.	8.5.3.1 Reactor Containment Systems Parameters	Stack Particulate Activity Stack Iodine Activity Stack Noble Gases Activity	Where are these detectors located in the Stack? Are these detectors shared with the FSS?
			Response: See response to Question 8.4. These detectors are connected to the First Reactor Protection System that actuates the CIS when levels in the stack reach the setpoint for isolation. There is no reactor trip associated with the detection of high activity in the stack
8.47.	8.5.4.1.1 Conformance to General Requirement 1	The CIS is fully automatic. Isolation valves are closed in case of: a) command of the FRPS when radioactivity of stack release is b) above the specified limit c) in case of electric power supply failure or compressed air failure to the valves d) by manual action of the operator	The wording of this paragraph appears incorrect. Does it convey the correct message? Does the CIS automatically operate upon manual action by the operator or does this mean to say that the CIS may be manually operated?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: Error in wording. Points a) and b) are one sentence. The CIS operates automatically (without operator intervention) to close the isolation valves when the signal from the stack monitors is high. Additionally the valves may be manually operated from the FRPS. Ref: Sections 8.2.3.4.1.10, 8.2.4.1.28 and 8.5.4.1.6.
8.48.	8.5.4.1.1 Conformance to General Requirement 1	Similarly the CERS is fully automatic. Control system details will be developed during the Detailed Engineering phase.	What are the system requirements of the Control System?
			The requirements are listed in Chapter 7. These are to limit and control pressure in the containment and to keep pressure within the containment to below the design limit. Ref: Section 8.5 and Chapter 7, Section 7.8
8.49.	8.5.4.1.4 Conformance to General Requirements 5 and 6	The CIS monitors the release of fission products by measuring particulate, iodine and noble gas activity in the stack. The monitored parameters provide sufficient information to determine if barriers to fission products have the potential for being breached or have been breached, and the amount of radioactive material released.	These monitors are only located in the Stack, is there potential for radioactive material to exit the Reactor Building via another path?
			Response: The stack is the only penetration from containment where air is exhausted during normal operation. Containment is kept below atmospheric pressure to ensure this sole exit point. Process liquids are monitored by activity monitors of the RMS (eg SAMO, WASMO, LEM). Ref: Section 8.7.3.2.2 and Chapter 7

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.50.	8.5.4.1.5 Conformance to General Requirements 7	The protective actions performed by the CIS are sufficient to limit the release of radioactive material from the reactor containment during and after accident conditions.	What is the reference document for substantiating the claim that the protective actions are sufficient?
			Response: Chapter 7 of the PSAR describes the operation of the CIS, including building permeability and the location of penetrations. Chapter 16 describes the role of the CIS for scenarios where it prevents releases to the environment. It concludes that releases are below the recommended limits. Ref: Chapter 7, Section 7.8 and Chapter 16, Section 16.9.
	Post Accident Monitoring System		
8.51.	8.6.1 Introduction	Some primary sensors are shared with the FRPS and SRPS, and isolated PAM signals are used by the RCMS to display the PAM parameters.	Why are some primary sensors shared with the FRPS and SRPS? Does this compromise the independence of the systems?
			Response: This statement refers to the sharing of sensors between the FRPS and PAM and the SRPS and PAM. Sensors are not shared between FRPS and SRPS. There are qualified electrical isolators between PAM and RPS signals. Ref: Sections 8.2.4.1.9 and 8.2.4.3.1
8.52.	8.6.2.3 Additional Requirements	Systems that aid re-entry into contaminated areas following a DBA, shall be classified as PAM systems. Such systems include Closed Circuit Television (CCTV) and communication systems.	Communication systems and CCTV are discussed as Auxiliary Systems (Chapter 10). There does not appear to be any reference to the Safety Category of these systems.

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: PAM systems shall be Safety Category 1 thus the CCTV and communications systems must comply with the requirements for Class1E components. Chapter 10 includes all CCTV and communications, some of which are not PAM Ref: Section 8.6.2.2
8.53.	8.6.3.1.2.3 Primary Cooling System (iii)	Water level below this line indicates that a critical core condition has been attained.	Is this an appropriate use of the word "critical"?
			Response: The word critical in this context means that a serious core condition has been reached. The text will be amended.
8.54.	8.6.3.1.2.7 Emergency Control Centre Ventilation and Pressurisation System	The parameters monitored by the PAM system for the ECC Ventilation and Pressurisation System will be developed during the detail design phase.	Why do the parameters need to be developed at the detail design stage?
			Response: Details are not available at the time of PSAR issue other than to include that since the ECC ventilation system is a ESF, then it will require PAM monitoring to indicate operation. Ref: Section 8.6.2.3, Chapter 10, Section 10.4.2 and Chapter 7, Section 7.9.
8.55.	8.6.3.1.2.8 Radiation Monitoring System	The following parameters are monitored: e) Reactor Pool Gamma dose rate. f) Critical occupational area Gamma dose rate (-5 m and +13 m levels).	What is meant by "critical occupational area"?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: This means areas in which staff will be working where there is a risk of radiation exposure. The text will be amended. Ref: Section 8.7.3.2.2.5 and Chapter 12
8.56.	8.6.3.1.2.9 Standby Power System	The parameters monitored by the PAM system for the SPS will be developed during the detail design phase.	Why do the parameters need to be developed at the detail design stage?
			Response: Details are not available at the time of PSAR issue other than to include that since the Standby Power system is an ESF, then it will require PAM monitoring to indicate operation. The Standby Power system was affected by the CERS addition. Ref: 8.6.2.3; 9.3.3, 7.10
8.57.	8.6.3.2.3 Post Accident Mitigation/Surveillance Devices	The following post accident mitigation/surveillance devices are included: a) critical occupational area CCTV b) critical occupational area communication system c) PAM area radiation monitors around the reactor pool area	What are the details of the CCTV and communication systems? What is meant by "critical occupational area"?
			Response: The details of CCTV and communications are not yet available and will be part of the detail engineering phase. For "critical occupation area" see response to question 8.55. Ref: Section 8.7.3.2.2.5
8.58.	8.6.4.1.2 Conformance to General Requirement 3	Requirement 3: Alert operators to take safety actions for initiating a system function that is not automatic.	Are there any safety system functions that are not automatic?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: All safety functions required to take affect at the onset of an incident are automatic (eg, FRPS, SRPS, CIS). However there may be instances where operators observe an abnormal occurrence and activate a safety system prior to or simultaneously with the FRPS or SRPS. Additionally the PAM variables are provided so that the actuation of safety functions can be monitored so that operator action can be taken if an automatic safety function fails. Ref: Sections 8.2.4.3.1, 8.2.4.3.3 and 8.2.4.3.7
8.59.	8.6.4.1.5 Conformance to General Requirement 6	Both channels are physically separated in a way that ensures common mode failures of the system can be neglected.	Is it appropriate to neglect common mode failures simply on the basis of separation? Are there other factors that may lead to a common mode failure (maintenance, suppliers)?
			Response: The aim of separation is to prevent incidents affecting both channels (eg fire or mechanical damage). Ref: Sections 8.6.4.1.7 and 8.6.4.1.8.
8.60.	8.6.4.1.6 Conformance to General Requirement 7	In the case of testing a single component, the channel it belongs to will be disabled,	Will the channel be "disabled" or tripped?
			Response: PAM circuits do not trip, they are for monitoring only and thus are disabled for testing. Ref: Section 8.6.3.1.2
	Reactor Control and Monitoring System		

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.61.	8.7.1 Introduction	FRPS and SRPS signals are only sent to the RCMS, without feedback, using galvanic de-coupling devices. The RCMS does not perform any Safety Category 1 functions.	What Standard do galvanic de-coupling devices comply with?
			Response: The isolation devices (galvanic or otherwise) will be required to satisfy the requirements for Safety Category I equipment. These are namely the IEEE Standards for Class 1E equipment. Ref: Sections 8.2.3.3.2 and 8.2.4.3.6
8.62.	8.7.1 Introduction	The RCMS complies with applicable ISO 8802 series and IEEE standards.	Which IEEE Standards does the RCMS comply with?
			Response: The development of the RCMS will comply with the requirements of IEEE 730, 829, 830 and 845 Ref: Section 8.1.4.2.
8.63.	8.7.2.1 General Requirements	Maintenance shall be eased by the low diversity of hardware components.	Can this statement be justified? Diverse equipment with similar maintenance requirements will have a neutral effect on maintenance levels.
			Response: Areas such as spare parts inventory, maintenance instructions, ILS and supplier support are simplified by the standardisation of components. Ref: Sections 8.7.4.1.3 and 8.7.4.1.19
8.64.	8.7.3.1 Architecture	The RCMS architecture is shown in Figure 8.7/1.	Where are the Engineering Workstations located? What are the capabilities of the Engineering Workstations?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: The engineering workstations will be located in restricted-access rooms, details of which have not yet been finalised. Modifications can be entered and tested and maintenance can be carried out from the engineering workstation without disruption to the operator stations. Ref: Section 8.7.3.1.9
8.65.	8.7.3.1.2 Control Level	While one CU acts as the operating unit, the other remains in a hot standby state.	Figure 8.7/1 seems to show nine CP60FT units, is this correct?
			Response: The figure was included to show the architecture of the system and the number of units shown is not relevant at this stage. The CP60FTs are shown in pairs on the figure thus there are actually 18 shown. Ref: Section 8.7.3.1.2 (first paragraph)
8.66.	8.7.3.1.5 Redundancy	Dual redundant processor units in the RCMS equipment	Is it correct to state "dual" redundancy. Is it not really single (100%) redundancy?
			Response: Dual is used to differentiate from triplicated redundancy. The processors are 100% redundant.
8.67.	8.7.3.1.6 Availability	The RCMS availability for reactor operation is greater than 99.9%.	Can it be claimed that the availability is greater than 99.9%? Does the system already exist?
			Response: This is a contract requirement. The system will undergo availability testing per the contract. The installation will not be complete until the system is proven to have an availability of 99.9%. Ref: Section 8.7.3.1.6 paragraph 2

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.68.	8.7.3.1.11 System Interfaces	Connection of the RCMS onto the existing LHSTC LAN system (via the Reactor Facility LAN) is provided.	Additional Requirement 5 (8.7.2.3) The reactor control system shall be equipped with a dedicated LAN system, which shall be totally independent of the reactor facility LAN system.
			Response: The Reactor Facility LAN is electrically and physically independent and separated from the RCMS LAN. These separations are achieved by the use of electronic isolation devices and a physical fire-rated wall. The connection of the RCMS to the Facility LAN and the LHSTC LAN is for access to plant data as read only. Ref: Chapter 10, Section 10.3.5.1.
8.69.	8.7.3.2.2 Radiation Monitoring System	For RMS channels connected to the FRPS and PAM system, isolated hard-wired signals are generated, with all equipment qualified to Safety Category 1 standards.	RMS channels that have inputs to the FRPS should do so directly, the additional signal to the RCMS should go through isolating devices – is this correct?.
			Response: This is correct. Ref: Sections 8.2.3.4.4 and 8.7.1
8.70.	8.7.3.2.2 Radiation Monitoring System	The RMS forms part of the RCMS and has inputs from all the radiation monitoring systems detailed below.	Part of the RMS is considered to be part of the FRPS (see 8.2.3.1.7.2)
			Response: The RMS which are part of the RCMS are described. These are Category 2 systems not connected to the FRPS or PAM. Ref: Sections 8.7.3.2.2.1 to 7
8.71.	8.7.3.3.2 Limitation Functions	The limitation system has limit control mechanisms that protect the plant from operational perturbations that could occur if operational parameters were allowed to be outside predetermined ranges.	What is the margin between the operational ranges and the FRPS Trip parameters?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: Margins will be developed during the detailed engineering phase
8.72.	8.7.3.3.4 Absorber Rod Functions	The assignment of rod function (the function of each of the four rods can be selected to be exclusively safety or safety and control) and rod movement are continuously supervised by the system, which monitors sequences and movements with interlock logic.	What are "Absorber Rods"? How many rods are there – 4 or 5? How is the function of the rods assigned? How many rods can be simultaneously assigned to both safety and control functions and under what operational modes? Does the ergonomic design of the control panel prevent the control rods being driven out simultaneously?
			Response: Absorber rods are the Control Rods. Text will be amended. There are 5. Normally the centre rod is used to control power while all 5 are to shutdown the reactor. Ref: Chapter 5, Section 5.5.2. Details not available at this stage but are more appropriately located in Chapter 5. Power regulation is performed by the centre, control rod. If more absorption is required through the cycle, the outer control (absorber) rods may be used for power regulation. This does not prevent operation of the FSS to drop all control rods. Ref: Chapter 5, Section 5.7.4.1 The RCMS logic and CRDM electronics do not allow bank extraction of the rods. Ref: Chapter 5, Section 5.5.2.8, Chapter 16, Sections 16.8.3.2 and 16.8.3.4

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.73.	8.7.3.3.5 Alarm Management	The alarm inhibition process is implemented in order to avoid non-significant alarm messages and the system inhibits the triggering of some alarms according to process states. For example, if a component is not in service all associated alarms are disabled.	Is there a list of the inhibited alarms? Are alarms actually disabled or simply inhibited?
			Response: The list will be developed during the detailed engineering phase. Alarms can be masked (ie they do not appear), for example, if they are a secondary effect of a problem. These alarms are available to the operator on demand. Alarms can be disabled (not generated) depending on process or even plant states (eg plant out of service or plant shutdown). Ref: Section 8.7.3.3.5, paragraph 3 and paragraph 10
8.74.	8.7.4.1.4 Compliance with General Requirement 4	The RCMS structure has a horizontal logic thus allowing for a simple interconnection structure between system components.	What is a "horizontal logic structure"? How does this result in a simple interconnection structure?
			Response: This phrase refers to the bus topology (as opposed to star or ring topologies) of the system, as shown in figure 8.7/1 which shows the bus type structure. All components of the RCMS are connected to a Nodebus. Nodebuses are connected together at one point. Ref: Section 8.7.3.1

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.75.	8.7.4.1.5 Compliance with general Requirement 5	All processors use similar platforms thus minimising the number of software components according to the simplicity criterion.	What is a "software component"?
			Response: Software Components can be programs or files used in the system.
8.76.	8.7.4.1.9 Compliance with General Requirement 9	All hardware complies with the reliability requirements.	What are the reliability requirements – have they been stated as a quantified performance criteria?
			Response: The RCMS must achieve 99.9% availability per the contract. Ref: Section 8.7.3.1.6 paragraph 2
8.77.	8.7.4.1.10 Compliance with General Requirement 10	The functions of the system shall be permanently distributed among the different units or processors	Due to the software-based nature of the system surely the functions can be distributed or centralised depending on system configuration?
			Response: Referring to Figure 8.7/1, Field Units and Control Processors have dedicated functions associated with the plant they are connected to. This is the distributed part of the system. Operation of the plant can be carried out through any of the operator workstations. However these will, most likely, be assigned dedicated roles. Ref: Sections 8.7.3.1.2, 8.7.3.1.3 and 8.7.3.1.8

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.78.	8.7.4.1.16 Compliance with General Requirement 16	The RCMS is designed to achieve an overall RCMS availability equal to or greater than 99.9%.	This indicates that the system is already designed. Does it really have an Availability of 99.9%?
			Response: This is a contract requirement. As explained in the following paragraph, the system will undergo availability monitoring following commissioning. Commissioning will not be complete until the system is shown to have availability of 99.9%. Ref: Section 8.7.3.1.6, paragraph 2
8.79.	8.7.5.1.4 Compliance with Additional Requirement 4	All microprocessor-based control systems and equipment dedicated to RCMS are located in such a way that they are not affected in their performance by any DBA.	What is the reference document for this statement?
			Response: The RCMS is a Safety Category 2 system and thus not required to be functional during DBAs. However, due to the distributed nature of the field units, most would be available during DBAs. The control processors are located in a dedicated instrument room, also outside containment, and would be operational during all DBAs. Ref: Chapter 4, Section 4.4.2 and Figures 4.4/4 to 8
	Primary Cooling System Instrumentation		
8.80.	8.8.3 Description	Differential Pressure Transmitters - Reactor core inlet/outlet	Are these separate units for the FRPS & SRPS?
			Response: Yes. Ref: Section 8.2.3.1.2.1

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
8.81.	8.3.3 Description	Level switches - Pool	Are these separate units for the FRPS & SRPS?
			Response: Yes Ref: Section 8.2.3.1.2.1
	Secondary Cooling System Instrumentation		
8.82.	8.9.5.1.3 Compliance with Design Requirement 3	All instrumentation of the SCS is qualified according to the requirements of Safety Category 2. This will ensure that the instrumentation will fulfil their function during and after abnormal occurrences.	What are the requirements for qualifying Safety Category 2 systems?
			Response: There are no IEEE requirements for qualification of Safety category 2 equipment. INVAP has developed requirements for this category. This category generally requires the provision of quality assurance documentation from manufacturers. Ref: Chapter 2, Section 2.5.1.2
	Main Control Room Design		
8.83.	8.14.1.1.3.3 Location Aides - Grouping	All displayed information and controls are logically grouped to facilitate their location and use. Particular care is taken to avoid conflicts of grouping and to be consistent with the user's model of the system.	Will somebody with the appropriate qualifications be used to review the ergonomic design? Who is going to review the wording of the actual messages received?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: The ergonomic design will be reviewed by ANSTO with respect to IEE 845 and ISA-RP60.3-1985/IEEE 1023, Human Factors for Control Centres. ANSTO will also review the wording of the messages and alarms. A specialist Human Factors organisation will train ANSTO I&C staff in human factors aspects.
8.84.	8.14.1.1.3.3 Location Aides - Coding	Information Coding - Coding of displays is used to improve the usability of the information by enhancing discrimination and aiding comprehension and assimilation. The code employed is simple and clear. Arbitrary abstract codes are avoided because they are difficult to learn and use.	Please explain this further, giving examples.
			Response: Information coding is the method of displaying the plant on the displays and the naming of plant items. For example a pump on the Primary Cooling system is labelled 1010-AB-001A. 1000 is the primary cooling system, 1010 related to equipment and piping, AB indicates a pump and 001 refers to the primary pump, "A" indicates it is of a redundant set
8.85.	8.14.1.1.3.4 Information Systems	Information shown is clearly understood by the operators.	How will this be achieved? What are the training requirements?

Question reference	Section number and name	Topic	ARPANSA Comments, Issue or Question and ANSTO's response
			Response: Clarity and comprehension of the operator displays and messages is aided by the coding methods described above. It is also intended that the Operators will be involved in the development of the graphics they will be using. Operator training requirements will be developed during the detailed engineering phase. Training of operators leading to accreditation will form an essential part of familiarisation. Ref: Section 8.14.1.1.3.4