AECL EACL

Safety Design Guide

SEPARATION OF SYSTEMS AND COMPONENTS

ACR

108-03650-SDG-004

Revision 3

Prepared by
Rédigé par

Dick Jerry

Reviewed by
Vérifié par

Johal Hardev S.

Approved by
Approuvé par

Jaitly Raj | Bonechi Massimo

2004/03/12
Controlled

2004/03/12
Contrôlé

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

2251 rue Speakman
Mississauga (Ontario)
Canada L5K 1B2

AECL EACL

Safety Design Guide

Separation of Systems and Components

ACR

108-03650-SDG-004
Revision 3

2004 March

CONTROLLED

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

Mars 2004

CONTRÔLÉ

2251, rue Speakman
Mississauga (Ontario)
Canada L5K 1B2

AECL EACL

Release and Revision History / Liste des documents et des révisions

0939B Rev. 13

Document Details / Détails sur le document

Title / Titre	Total no. of pages / Nbre total de pages
Separation of Systems and Components	36

CONTROLLED - CONTRÔLÉ

Release and Revision History / Liste des documents et des révisions

Release Document No./N°	Release Document Date	Revision Révision No./N°	Revision Révision Date	Purpose of Release; Details of Rev./Amendement Objet du document; détails des rév. ou des modif.	Prepared by Rédigé par	Reviewed by Examiné par	Approved by Approuvé par
1	00-10-19	D1	00-10-16	Review and Comment	A.H. Stretch	A. Wight	
2		0	00-11-23	Issued as "Approved for Use".	A.H. Stretch	A. Wight	J.M. Hopwood
3		1D1	02-05-06	Issued for Review and Comment.	E. Lemoine	A. H. Stretch	
4		1D2	02-09-12	Issued for Review and Comment. Revised to include the current ACR Safety, Licensing and Design philosophy. Removal of Groups 1 and 2 and revised separation requirements and instrumentation cables routing requirements. Updated to include the ACR systems' design changes.	W. Rabbani	S. D.Nam A. H. Stretch H. Shapiro V. Snell K. Hau E. Choy A. Josefowicz J. Millard M. Elgohary R. Ghai/O. Hines H. Johal	

DCS/RMS Input / Données SCD ou SGD

Rel. Proj. Proj. conn.	Project Projet	SI	Section	Serial Série	Sheet Feuille No. N°	Of De	Unit No.(s) Tranche n°
	108	03650	SDG	004	1	4	

AECL EACL

Release and Revision History / Liste des documents et des révisions

0939B Rev. 13

Document Details / Détails sur le document

Title / Titre	Total no. of pages / Nbre total de pages
Separation of Systems and Components	36

CONTROLLED - CONTRÔLÉ

Release and Revision History / Liste des documents et des révisions

Release Document No./N°	Release Document Date	Revision Révision No./N°	Revision Révision Date	Purpose of Release; Details of Rev./Amendement Objet du document; détails des rév. ou des modif.	Prepared by Rédigé par	Reviewed by Examiné par	Approved by Approuvé par
5		1	02-10-15	Issued as "Approved for Use"	W. Rabbani	S. D.Nam A. H. Stretch H. Shapiro V. Snell K. Hau E. Choy A. Josefowicz J. Millard M. Elgohary R. Ghai/O. Hines H. Johal	M. Bonechi
6		2	03-01-06	Issued as "Approved for Use". Some sentences revised as per resolution of comments from the Technical Review. Changes were mostly of addition of clarifying wording and of an informative nature.	W. Rabbani	J. Tong N. Barkman V. Langman J. Waddington P. Lee H. Johal	M. Bonechi
7		3	04-03-12	Issued as "Approved for Use".	J.E. Dick	H. Johal	R. Jaitly /

DCS/RMS Input / Données SCD ou SGD

Rel. Proj. Proj. conn.	Project Projet	SI	Section	Serial Série	Sheet Feuille No. N°	Of De	Unit No.(s) Tranche n°
	108	03650	SDG	004	2	4	

AECL EACL

Release and Revision History / Liste des documents et des révisions

0939B Rev. 13

Document Details / Détails sur le document

Title / Titre	Total no. of pages / Nbre total de pages
Separation of Systems and Components	36

CONTROLLED - CONTRÔLÉ

Release and Revision History / Liste des documents et des révisions

Release Document No./N°	Release Document Date	Revision Révision No./N°	Revision Révision Date	Purpose of Release; Details of Rev./Amendement Objet du document; détails des rév. ou des modif.	Prepared by Rédigé par	Reviewed by Examiné par	Approved by Approuvé par
				Minor text additions are identified by underlining and major text additions and deletions are noted in this revision history. The major text additions that are not underlined are: 1. Section on definitions 2. Section 3.1, titled “Introduction to Separation Philosophy” 3. Last 2 paragraphs of Section 3.3, “Principles for Achieving Independence”, which provide guidance on sharing of instruments 4. Paragraphs 3 and 4 of Section 3.2, “Categorization of Safety Related Systems by Function”, for additional explanation 5. Section 3.3, “Principles for Achieving Independence”, (except for paragraphs 6 and 7,) also for additional explanation Text deletions from Rev. 2 of this safety design guide are: 1. Section 3.2.5, “Protection of Systems” 2. First two paragraphs of Section 3.1, “General”			M. Bonechi

DCS/RMS Input / Données SCD ou SGD

Rel. Proj. Proj. conn.	Project Projet	SI	Section	Serial Série	Sheet Feuille No. N°	Of De	Unit No.(s) Tranche n°
	108	03650	SDG	004	3	4	

AECL EACL

Release and Revision History / Liste des documents et des révisions

0939B Rev. 13

Document Details / Détails sur le document

Title / Titre	Total no. of pages / Nbre total de pages
Separation of Systems and Components	36

CONTROLLED - CONTRÔLÉ

Release and Revision History / Liste des documents et des révisions

Release Document No./N°	Release Document Date	Revision Révision No./N°	Revision Révision Date	Purpose of Release; Details of Rev./Amendement Objet du document; détails des rév. ou des modif.	Prepared by Rédigé par	Reviewed by Examiné par	Approved by Approuvé par
				3. Item b)1) in Section 4.3, "Separation Inside the Reactor Building" Underlined revisions consist of the following: 1. Requirements for sharing of instruments added, [Sections 1.e), 3.5 (paragraphs 3 and 6), 4.5 (items e)7) and k))] 2. Section titles made more descriptive [Sections 3.2, 3.3, 3.4, 3.4.1, 3.4.2, 3.4.3, 3.5] 3. Additional explanation provided in a number of sections: [added text in Sections 3.4.1, 3.4.2, 3.4.3, 3.5, 3.6, and 4.4] 4. "Secondary Control Building (SCB)" replaced by "Secondary Control Area (SCA)" 5. Tables 1 and 2 revised for additional clarity 6. Acronyms table made more specific to ACR 7. Miscellaneous editorial corrections			

DCS/RMS Input / Données SCD ou SGD

Rel. Proj. Proj. conn.	Project Projet	SI	Section	Serial Série	Sheet Feuille No. N°	Of De	Unit No.(s) Tranche n°
	108	03650	SDG	004	4	4	

TABLE OF CONTENTS

DEFINITIONS

Back-up System: A back-up system, in the present context, is a safety related system that acts to mitigate the failure of another safety related system, frequently by diverse means, and thereby ensures that an essential safety function is successfully accomplished (Note: Back-up systems provide defence-in-depth, as opposed to redundant systems that replicate a function or service.)

Channel: A channel is defined as a set of interconnected hardware and software components that processes one of the duplicated or triplicated signals associated with a single reactor parameter. A channel may include the sensor, data acquisition, signal conditioning, data transmission, bypasses, and logic, up to voters or actuating device inputs. The objective of the channel definition is to define subsets of a reactor instrumentation and control system that can be unambiguously tested or analysed from input to output.

Divisions: Divisions are redundant sets or trains of components that are physically and functionally independent from each other and perform or support the performance of essential safety functions.

Raceway: Any channel-like support that is designed and used expressly for supporting or enclosing wires, cable, or busbars. Raceways consist primarily of, but are not restricted to, cable trays and conduits.

Redundant System (or Equipment): A redundant system, in the present context, duplicates the essential function of another system to the extent that either may perform the required function regardless of the state of operation or failure of the other. (Note: Redundant systems replicate a function or service, as opposed to back-up systems that provide defence-in-depth.)

Route: In the context of this document, a “route” is a path shared by the raceways, stacks of raceways, or multiple stacks of raceways of associated channels. The routing of mechanical tubing may follow the same principle.

Safety Support System: A safety support system provides services required for proper operation of safety related systems and may also be required for normal plant operation. Examples of safety support systems include the systems supplying cooling water, electric power, instrument air and ventilation.

1. PURPOSE

This Safety Design Guide describes the philosophy and safety objective of physical and functional separation for safety related systems, structures, and components in the nuclear power plant (including NSSS, NSP and BOP) and establishes the requirements for the implementation of the philosophy in the detailed plant design.

The specific topics addressed in this guide are:

a) Separation of safety systems from process and control systems,

b) Separation between safety systems,

c) Separation of redundant safety related systems or divisions and their components,

d) Documentation of the separation and any justifiable deviations in the actual plant design, and

e) Guidance regarding requirements for sharing of instrumentation.

2. COMPLIANCE

Compliance with Safety Design Guides is mandatory. A listing of Safety Design Guides is included in Appendix B. Deviations from the requirements identified in this guide may be allowed after an appropriate internal safety review. All deviations shall be documented by completion of a Safety Design Guide Supplement, AECL form 0729-00.

This Safety Design Guide includes a non-mandatory Appendix A, that provides guidance on the application of the mandatory requirements defined in Section 4. Departures from these non-mandatory guidelines do not require completion of a Safety Design Guide Supplement, as long as the mandatory requirements are satisfied.

3. SAFETY RELATED SYSTEMS' SEPARATION PHILOSOPHY

3.1 Introduction to Separation Philosophy

A fundamental method of ensuring reliable execution of essential safety functions in CANDU plants is the provision of systems to duplicate safety functions. However, to prevent propagation of system failures to other systems that perform the same safety function and to reduce the risk from common hazards that could damage multiple systems, it is essential that all such systems be physically and functionally independent of each other. The ACR safety philosophy for separation ensures this independence using principles and methods that are essentially the same as those implemented in past CANDU plants.

The primary safety functions required in all nuclear reactors are reactor shutdown, decay heat removal from the core, containment of radioactivity and plant monitoring and control. In the CANDU design, these functions are performed mostly by the safety systems, i.e., SDS1, SDS2, ECC, and Containment. The importance of independence to these systems is reflected in a fundamental Canadian regulatory requirement that safety systems must be separated from the systems used for power production (process systems). This separation, as defined, was intended to ensure that events affecting a limited area of the plant would not impair the capability to perform the required safety functions for accident conditions.

There are a number of postulated initiating events that could affect a limited area of the plant. These events are referred to as "common mode events" and include fires, floods and missiles. Separation principles and requirements provide an effective defence against such common mode events. The design approach for meeting separation requirements involves the identification and provision of two independent, redundant means of achieving the same safety function, and, where necessary, providing an alternate, diverse means to accomplish a particular safety function.

Tables 1 and 2 of this Safety Design Guide identify major safety related systems and their separation requirements. For example, the systems in the upper part of Table 2 need to be separated from the systems given in lower part of this table. In addition, the ACR design includes independent trains of equipment called divisions. Examples include Emergency Power, Recirculated Cooling Water, Raw Service Water, and Long Term Cooling, each of which consists of two or more redundant divisions. These divisions are treated as separate systems with regard to their separation requirements.

Therefore, even though the traditional CANDU term of "grouping" is not used in the ACR design, the ACR systems are provided with appropriate separation or barriers so that safety functions can be reliably accomplished for all internal and external events considered in the design basis.

3.2 Categorization of Safety Related Systems by Function

This section of the Safety Design Guide describes the safety concept and safety design philosophy used to develop the safety requirements for separation. It is to be considered as information for the interpretation and application of the safety requirements listed in Section 4.

The function and categories of safety related systems are described in the Safety Design Guide 108-03650-SDG-001, Safety Related Systems. These are of the following type:

1. Preventative: Systems and structures that perform safety functions during the normal operation of the plant, to ensure that radioactive materials remain within their normal boundaries.
2. Protective: Systems and structures that perform safety functions to mitigate events caused by failure of the normally operating systems or by naturally occurring phenomena. Protective systems are further divided into:
   a) Safety Systems, which are Shutdown System One, Shutdown System Two, Emergency Core Cooling and Containment.
   b) Safety Support Systems, which provide services needed for proper operation of the safety systems and other normal plant operation (e.g., cooling water, electric power, instrument air).

The purpose of categorizing safety related systems by function is to:

a) Identify systems that perform essential safety functions,

b) Distinguish systems that perform essential safety functions from ordinary process systems,

c) Identify systems that are either redundant, provide independent back-up safety functions for other systems, or provide essential safety support functions.

This information is used to determine the degree of independence required between specific safety related systems and to select appropriate means of achieving this independence.

3.3 Principles for Achieving Independence

The two purposes for providing independence between safety related systems or components are:

a) Ensuring that a failure in one system will not cause a failure in another system, and,

b) Reducing the risk that common mode hazards like missiles, flooding, fire or earthquake, and internal events such as LOCA or MSLB will incapacitate multiple safety related systems.

The first of the above purposes is reflected in CNSC Regulatory Documents R-7, R-8 and R-9 (see Section 4.6) which require that Safety Systems, as far as practicable, be separated from each other and from all process systems.

The second purpose is to ensure that essential safety functions are accomplished despite common cause hazards that could affect multiple systems within a limited area of the plant (e.g., events that damage equipment within a local area, such as fires; failure of a common process such as cooling water; or the occurrence of a common adverse environment such as that caused by a loss of ventilation).

The two main techniques for achieving such independence and the methods typically used are:

a) Physical separation by methods such as distance or barriers and,

b) Functional isolation by methods such as isolation devices, buffers, etc.

The design process for achieving independence requires:

a) Selection of the systems or components that require separation, and,

b) Choice of the means of separation.

These design steps require consideration of both the category of the system safety functions defined in the previous section and the specific initiating events that must be considered in the design basis (see Appendix A).

The types of safety related systems (including their instrumentation, control and power supply) to be considered in this process are:

1. Safety Systems,
2. Safety Support Systems,
3. Process Systems (power production systems),
4. Electrical Systems,
5. Plant Services Systems, and
6. Other Safety Related Systems.

Choice of the method of separation for these types of systems is frequently governed by the bounding conditions associated with internal hazards and external events, such as tornadoes, aircraft crash, hurricanes etc., as applicable for the particular site. Appropriate methods range from physical separation, protection via barriers, including use of conduit, qualifying the systems to withstand the expected environmental conditions, or by a combination of each, as indicated in Safety Design Guides or other documents for those events.

The above categorization of safety related systems and the considerations required to determine the amount of separation needed are also relevant to the sharing of instrumentation among systems. In particular, when selecting the systems for which instrument sharing is considered, the designers must ensure that the systems do not provide either redundant or back-up safety functions for each other or have cross-links to other Safety Systems. An example of two systems that meet these requirements is SDS1, which is a Safety System and the Process Control System, which is a Process System. Assurance that the safety functions for these systems are unrelated

can be verified by the system function lists in Table 2 of Safety Design Guide 108-03650-SDG-001.

Regarding the means of separation, the requirements for physical separation (i.e., distance apart, barriers, and qualification, see above) are the same as for systems that do not share instrumentation. The choice of functional separation will involve the selection of suitable buffering or isolation devices and assurance of their protection or environmental qualification for the design basis events of interest.

3.4 ACR Provisions for Redundancy and Defence-in-Depth

3.4.1 Divisions

Protection against the more frequent types of common cause events, which include internally generated events affecting a limited area of the plant, is provided by having additional safety related systems or two redundant sets or trains of components called "Divisions". Redundant Divisions within the ACR are designed to be physically and functionally independent of each other to the maximum extent practical, and can independently perform or support essential safety functions.

3.4.2 Back-Up Systems

A listing of the ACR™* major safety related systems and their primary safety functions is provided in Safety Design Guide 108-03650-SDG-001, Safety Related Systems. The safety functions may be used to identify safety related systems that serve as back-up systems and to choose appropriate separation means for these systems.

Back-up safety related systems should be designed such that, if one system is lost due to a common cause event, the remaining system will mitigate the failure or duplicate the essential safety function. Events occurring in one of the systems or divisions should not impair the capability of its back-up system to maintain the plant in a safe condition.

One example is the Secondary Control Area (SCA) which contains duplicate control and monitoring instrumentation for essential safety related systems. The operator will be able to shut down and maintain the plant in a safe state from that location if the Main Control Room (MCR) becomes unavailable.

3.4.3 Redundant Equipment Within Systems

Within each system, redundancy is achieved by multiple components (e.g., pumps, motors, valves, etc), multiple channels (e.g., triplicated channels D, E, F for SDS1 and K, L, M for the ECC), or multiple trains of components (e.g., Divisions 1 and 2 for the RSW/RCW systems and the "ODD" and "EVEN" divisions of electrical subsystems). Redundancy is applied to the

* ACR™ (Advanced CANDU Reactor™) is a trademark of Atomic Energy of Canada Limited (AECL).

extent required to satisfy the reliability targets derived from Probabilistic Safety Assessments (PSA) or regulatory requirements. Separation principles, applied in conjunction with redundancy, ensure maximum protection against both single failures and common cause events. This objective must be qualified by recognition that there may be practical and economic reasons which limit application of these principles.

3.5 Methods of Separation

Independence between components, systems, and divisions of safety related systems is achieved through functional and physical separation, as described below.

Functional separation means that the functions (e.g., shutdown, fuel cooling) performed by redundant systems are not dependent on each other or on a single common service. Functional separation is achieved by minimizing the number of interconnections between systems, by avoiding complete reliance on common services, and by designing interconnections to avoid propagation of faults from one system to another. Functional separation is provided between the safety systems and other safety related systems as necessary and practical.

Functional separation in the case of shared instrumentation can be accomplished by a variety of buffering devices such as auxiliary relays and breakers, fibre optic couplers and solid state signal isolators.

Physical separation is provided, by installing barriers between safety systems or components, or by providing sufficient distance between systems or components. The design of the barrier, or the distance provided, must be based on consideration of the severity and extent of the anticipated common cause events that may affect the systems or components being separated (e.g., fire, flooding, missiles, adverse environment). Barriers are also installed within redundant systems or divisions if needed to satisfy a PSA target or design objective.

For example, the MCR and the SCB are separated by a barrier for protection against common cause events such as missiles, fire or flooding. However, assurance of independence between the control centre functions would also necessitate a protected cable path for the cables between the Main Control Room and the Secondary Control Area. (Alternatively, redundant MCR to SCA cable routes could be considered.) Within the protected path, the triplicated instrumentation routes of the individual safety related systems, would again require additional separation by distance or barriers.

At the “end-points” of instrumentation and control systems, and some process systems, the degree of physical separation provided elsewhere cannot be maintained due to practical constraints (e.g., redundant instrumentation on the same header of the reactor, indications from all three instrument channels provided in a common cabinet in the control rooms, and shared instrumentation such as measurement sensors, transmitters and buffers). In these areas, the designer provides as much separation and/or physical barriers, as the practical situation allows. This principle applies to areas near the reactor, in the control rooms, and in control equipment rooms where cables are directed to the control room panels. The control rooms and control equipment rooms have fewer common mode hazards as there are no high voltage (HV) loads or power cables and no process piping in the MCR complex. In the control equipment rooms, the

safety system equipment is separated from that of other systems. In the Main Control Room, the safety systems and other safety related systems are provided with separate cabinets.

Where separation cannot be achieved due to physical or operational constraints, an assessment must be carried out to show that there are no hazards that could impair essential safety functions. Alternatively, components may be qualified to withstand the hazard, or designed to fail to a state where the required safety function will be performed.

Protection against less frequent types of common cause events, which include site related external events such as earthquakes, tornadoes and external flooding, is provided by protecting systems or components from the hazard (e.g., tornado), or by qualifying the systems or components to withstand the effects of the hazard (e.g., earthquake).

Where justified by the low frequency of an event and the reliability of the mitigating systems, only one set of systems or components may need to be qualified or protected. Such systems should be qualified or protected to the extent necessary to ensure that the essential safety functions can be maintained.

Outside the Reactor Building, systems are generally protected by separation or barriers. Inside the Reactor Building, the consequences of the postulated events are less severe (since the reactor building protects the systems against events occurring outside the building). Protection can also be addressed by measures other than physical protection or separation (e.g., qualification). Generally, separation by distance or local barriers is used both inside and outside the Reactor Building.

3.6 Interconnections Between Systems

It is recognized that in many cases interconnections between systems can serve the purpose of increasing the overall reliability of the systems. In such cases, functional separation is provided by interconnections that ensure that a failure occurring in one system will not impair the capability of the other system to perform its safety function. For example, cooling water to the heat exchangers of several safety related systems may be provided by both Division 1 and Division 2 of the recirculated cooling water (RCW) system but failure of the Division 1 RCW equipment must not interfere with the capability of the Division 2 RCW to provide the cooling water to the heat exchangers. Interconnections, between divisions and between systems, may be minimized, by providing independent support services within each system, and by providing separately protected power distribution and control cables. The status of interconnections that could cause an impairment should be monitored or periodically tested.

Electrical interconnections between back-up safety related systems or between their divisions must be buffered, such that a common cause event in one system/division will not affect the function of the other system/division. The buffering must be located in the system/division that is not affected by the event (i.e., the system/division being protected from the event). The buffered cables then become part of the unprotected system, and the normal separation requirements between systems do not apply for these components (e.g., a buffered cable for control of systems from the Main Control Room may be routed with other cables). Where

electrical power from one system/division must be supplied to isolated equipment in the other system/division (e.g., panels in the MCR, manual trip pushbuttons), a fused connection in the protected system is considered to be adequate buffering. (See Section 4.6, IEEE Standard 384, Clause 7.1.2.4).

4. SEPARATION REQUIREMENTS

4.1 General

a) Safety related systems and components that provide redundant or back-up safety functions and are considered to be independent, shall be physically and functionally separated from each other. This separation shall be to the extent that conditions resulting from plant component failures due to internal events or site related external events shall not impair the required safety functions.

b) The designer shall review the system and its surroundings to identify any common cause hazards that could cause loss of the safety function of the system. A list of typical events that should be considered in the separation of safety related systems is shown in the (non-mandatory) Appendix A. Other events considered to be relevant by the designer of a system shall also be considered as applicable (e.g., loss of ventilation, dropped loads, piping failure or leakage, electromagnetic or radiofrequency interference).

c) The following types of conditions shall be considered in determining the adequacy of the separation barrier or distance:

   1) Fire (For detailed fire protection evaluation and separation requirements, refer to 108-03650-SDG-005, Fire Protection),

   2) Missiles (including pipe whip),

   3) Extreme structural loads (e.g., due to tornado),

   4) Local adverse environmental conditions (temperature, pressure, humidity, radiation), caused by the failure of components in the area. (For this condition, the designer may qualify the affected components to withstand the condition, as outlined in 108-03650-SDG-003, Environmental Qualification.),

   5) Failure of nearby seismically unqualified systems or components (also see 108-03650-SDG-002, Seismic Requirements),

   6) High voltage transients, generated during normal and failed conditions shall be considered in determining the adequacy of isolation and/or surge protection for downstream equipment.

d) The layout of components in the areas of the plant shall minimize the requirements for barriers, wherever practical. For example, the turbine should be oriented to minimize the probability of turbine missiles striking the safety systems or their components such as the containment structure.

e) The Main Control Room (MCR), Reactor Auxiliary Building (RAB) and the Secondary Control Area (SCA), shall be protected from the effects of component failures, such as turbine missiles or steam line breaks, and from the effects of external events, to the extent that operating staff can control and monitor the plant from the MCR for the duration of the event. For events that might disable the MCR, the operator would shut down the plant and maintain it in a safe shutdown condition from the SCA until the MCR function is restored.

f) Operating staff in the MCR shall be protected from the effects of a radioactive release for the duration of an event, as described in 108-03650-SDG-007, Radiation Protection. In the SCA, operators shall be protected from the effects of a radioactive release until the MCR becomes available.

g) Component failures occurring in a safety related system shall not impair the capability of another redundant system to maintain the plant in a safe condition, nor impair its safety functions.

h) Safety related equipment shall be located above flood levels which may occur due to a component failure (e.g., cooling water line break in the Reactor Building), or shall be physically separated from the flood (e.g., when one system or division floods, the other alternate system/division performs the function, or when a component within a system floods, the other redundant component can be protected). In cases where this is not practical, it shall be demonstrated that the equipment can perform its required safety function, as required by the Probabilistic Safety Assessment, despite a flooded condition, through qualification (see 108-03650-SDG-003, Environmental Qualification). Qualification conditions for submerged equipment shall be determined on a case-by-case basis.

   The minimum requirements for separation are shown in Table 1. These apply to separation outside the reactor building, inside the reactor building (where the need for pressure equalization after a LOCA precludes extensive use of barriers), between safety related systems, between redundant divisions/equipment, between routes of associated channels and between trays or stacks of trays in the same route.

i) Where the specified separation requirement, as summarized in Table 1, cannot be maintained, the greatest practical separation shall be provided and justified by completion of design documentation, as follows:

   1) Documented review of hazards in the area indicating that no hazards exist that would impair the required safety function, or

   2) Provision of another component or system of equivalent capability outside the area influenced by the hazard, or

   3) Protection of the component or system from the hazard by a barrier, or

   4) Qualification of the component to withstand the hazard, or

   5) Design of the component or system to fail to a state where the required safety function will be performed.

j) Systems, structures, and components shall be seismically qualified to either operate or maintain their structural integrity, as specified in 108-03650-SDG-002, Seismic Requirements. Seismically qualified components shall be protected against the potential failure of non-qualified components.

k) Seismically qualified cable trays and tubing shall not be routed underneath trays or components that are either not qualified, or qualified to a lower level. Where this is not possible, adequate protection for the seismically qualified tray shall be provided.

l) Redundant instrument and power supply channels for the same safety related system shall be identified, separated and routed so their independence from each other is maintained as specified in Table 1. Triplicated instrument channels may be identified as shown in Table 2, or in a similar manner. The "ODD", "EVEN" and "THIRD" electrical distribution cables may be associated with the channels shown. These electrical distribution cables shall not be routed in the same cable tray and/or conduit as instrumentation channels. This last requirement not only ensures appropriate separation but also reduces electrical hazards to personnel and the potential for electromagnetic interference, in accordance with good engineering practice.

m) Power supply cables shall be routed at least 0.5 metres above or 2 metres below control or instrumentation cables, to minimize the hazard to the instrumentation cables posed by a cable fault and/or fire in the power supply cable.

n) Separation of redundant components shall be provided, as appropriate for the particular situation, where the designer identifies a likely failure mode in one component that could cause the failure of the redundant components at a frequency greater than predicted in reliability analysis or probabilistic safety assessments.

o) Where it is not practical to provide a separation, or an equivalent barrier, as specified in Table 1, an assessment (per 4.1(i)) of nearby hazards shall be used to justify a smaller separation distance. A Safety Design Guide Supplement (AECL form 0729-00) shall be completed and approved to document this deviation.

4.2 Separation Outside the Reactor Building

a) Safety related systems and components shall be protected from the effects of common cause and external events or component failures occurring in other systems by separation or by a barrier designed to withstand identified hazards in the area, as specified in Table 1. Barriers shall be capable of withstanding the effects of component failures on either side of the barrier. For fire hazards, they shall be designed with a fire resistance specified by 108-03650-SDG-005, Fire Protection.

b) The MCR and the SCA shall be protected from hazards occurring in the plant (e.g., fire or flooding) and from the effects of site related events, excluding random equipment failures within the Main Control Room or its supporting systems which cause it to become unavailable or uninhabitable.

c) Components may be placed in close proximity to each other at end devices in the Control Equipment Room, Main Control Room or Secondary Control Area, where practical constraints do not allow normal separation. In such cases, the greatest possible separation shall be maintained for redundant channels/systems and suitable barriers, such as enclosed panels, shall be provided.

4.3 Separation Inside the Reactor Building

a) The Reactor Building shall be designed to physically protect safety related systems and components within the building from the effects of site related events and plant component failures occurring outside the building.

b) Safety related systems, their divisions and components, shall be separated from each other by a distance as specified in Table 1, or by a barrier designed to withstand identified hazards in the area.

c) Safety related systems and components may be placed in close proximity to each other at end devices, where practical constraints do not allow normal separation.

d) Passive components such as piping or tanks (e.g., reserve water tanks, RCW piping) can be shared between safety related systems, as long as the required safety function can be performed without reliance on the other system, and the performance of safety functions of one system will not affect the performance of safety functions by the other system.

4.4 Separation Within Safety Related Systems

a) Triplicated instrument channels associated with the same safety system and safety support system shall be separated as noted in Section 4.1 (l).

b) The Main Control Room shall remain available for common cause events occurring in the vicinity, including a steam line failure, and turbine failure. Separation of the Odd and Even electrical power divisions shall be such that an electrical supply remains available to maintain the MCR in an operable and habitable condition for such events.

c) The access route from the Main Control Room to the Secondary Control Area shall be maintained for random component failures or events causing the MCR to become unavailable.

d) Where one route crosses over another route, the separation requirements apply. Protective barriers shall be used where the separation cannot be maintained.

e) Cables for systems associated with a route, as identified in Table 2, may be carried in the same cable tray except for instrument power cables, which must be carried in different trays. Individual cables shall not contain wiring for more than one safety system. These cable trays shall be separated as per the requirements listed in Table 1.

4.5 Interconnections Between Safety Related Systems or Divisions

a) Interconnections between safety related systems backing up one another, or their divisions, shall be provided with isolation devices that ensure that a failure occurring in one system/division will not impair the capability of the other system/division to perform its safety function.

b) A random single active failure of an isolation device shall not impair the safety function of both systems/divisions.

c) Electrical circuits shall be provided with suitable buffering or isolation so that a fault occurring in either system/division would not cause faults or spurious signals that would cause failure of the power supplies to the other system/division.

d) For isolation devices controlling the supply of safety support services (cooling water, electrical power, instrument air) between redundant safety related systems or divisions, the status of the isolation device shall be monitored. Where monitoring is not practical, the device shall be tested at appropriate intervals to demonstrate that the isolation function is available.

e) Interconnections between back-up or redundant safety related systems or their divisions, shall be limited to the following:

   1) Electrically buffered control and instrumentation cables for redundant systems or divisions between the Main Control Room and the Secondary Control Area to enable accident conditions to be controlled from the Main Control Room and the Secondary Control Area.

   2) Electrically buffered post-accident monitoring and control cables,

   3) Electrical power supply connection between the Class III buses,

   4) Cooling water supply to components which must remain available to mitigate the consequences of an accident, or for long-term reliability,

   5) Compressed air supply to local air tanks needed to perform safety functions,

   6) Ventilation ducting, where it is not practical to eliminate this interconnection entirely. Fire/smoke dampers shall be installed in supply and return air ducts where necessary (see 108-03650-SDG-005, Fire Protection for more information).

   7) Measurement made by SDS1 may be shared with process control systems.

f) Electrical buffering of control and instrumentation signals between safety related systems or divisions, shall prevent a failure in one system or division from impairing the required safety function in the other system or division. Electrical buffering devices shall be located in a protected environment.

g) Acceptable means of buffering of control and instrumentation shall include, but are not limited to:

   1) Current-to-current isolators (i.e., isolation by transformer coil),

   2) Relays, separate from the other redundant system/division relays, to avoid “welding” of the other redundant system/division relay contacts during an overcurrent/overvoltage event,

   3) Optical links,

   4) Isolation amplifiers.

h) Power supply cables connecting the safety related systems or their divisions’ Class III buses, shall be provided with isolation breakers that will automatically interrupt the electrical supply

on a condition that could cause impairment of either system/divisions electrical system, or downstream I&C equipment.

i) Fluid piping connecting redundant safety related systems or divisions, shall be provided with isolation valves that can be operated from the Main Control Room, and from the Secondary Control Area to the extent needed to protect the necessary safety function in each system (e.g., interconnection of Divisions 1 and 2 cooling water supplies).

j) The status of all isolation valves and breakers, required for interconnections between redundant safety related systems or divisions, shall be monitored in the Main Control Room.

k) When safety related systems share instrumentation, the shared instrumentation and its associated isolation devices shall be designated as part of whichever system has the stricter requirements and designed to those stricter requirements. The sharing of instrument devices shall be assessed for defence-in-depth and diversity with guidance taken from the U.S. Standard Review Plan, Appendix 7-1A.

4.6 Applicable Codes and Standards

The design shall comply with the following standards, which also contain requirements relevant to separation of safety related systems:

a) CAN3-N290.1 "Requirements for the Shutdown Systems of CANDU Nuclear Power Plants".

b) CAN3-N290.4 "Requirements for the Reactor Regulating Systems of CANDU Nuclear Power Plants".

c) CAN3-N289.3 "Design Procedures for Seismic Qualification of CANDU Nuclear Power Plants".

d) CAN3-N290.5 "Requirements for the Support Power Systems of CANDU Nuclear Power Plants".

e) CAN3-N293 "Fire Protection for CANDU Nuclear Power Plants".

f) CAN3-N290.6 "Requirements for Monitoring and Display of CANDU Nuclear Power Plant Status in the Event of an Accident".

g) CNSC Regulatory Document R-7, "Requirements for Containment Systems for CANDU Nuclear Power Plants".

h) CNSC Regulatory Document R-8, "Requirements for Shutdown Systems for CANDU Nuclear Power Plants".

i) CNSC Regulatory Document R-9, "Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants".

j) IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits", Institute of Electrical and Electronics Engineers, Inc., New York, N.Y.

5. DOCUMENTATION

a) Deviations from the requirements of this Safety Design Guide shall be recorded and approved using the Safety Design Guide Supplement AECL Form 0729-00.

b) Common cause hazards such as major missile, pipe whip, and fire hazards shall be identified and recorded in the system's design documentation.

c) The separation requirements of individual systems shall be identified in system Design Requirements documents and Design Descriptions.

Table 1
Summary of Separation Requirements

Type of Separation	Minimum Requirements
Outside Reactor Building	
Protection of back-up safety related systems and their redundant divisions and equipment from external events.	Barriers
Flood protection	Locate equipment above the flood level.
Both Inside and Outside Reactor Building	
Separation between safety related systems, between redundant equipment, between cable Routes 1 and Routes 2 and Routes 3, and between cable Routes 4 and Routes 5 and Routes 6, see Table 2	6 m with fire hazard[1], 2 m with other hazards, 1 m horizontal or vertical with no identifiable hazards, or barrier.
Separation between redundant divisions, separation of the safety related systems and raceways of cable Routes 1, 2 and 3 from the safety related systems and raceways of cable Routes 4, 5 and 6, see Table 2	6 m with fire hazard[1], 2 m with other hazards, or barrier.
Separation between trays or between stacks of multiple trays in the same route, Note: Where the above separation cannot be met, the specific location shall be reviewed for hazards, (e.g., fire) and appropriate barriers shall be provided.	0.5 m horizontal or vertical, or barrier.
Separation between trays for instrument electrical power and trays for control cables when located above or below each other in the same stack	0.5 m with power cable located on top, or 2 m with power cable below.
Separation between tubing routes for safety related systems	0.5 m horizontal or vertical.
Flooding Hazard	Locate equipment above the flood level.

[1] For detailed fire protection evaluation and separation requirements, refer to 108-03650-SDG-005: Fire Protection.

Table 2
Permitted Routes Assignments for the Channels of Major Safety Related Systems

Major Safety Related Systems			
	Routes 1	Routes 2	Routes 3
Reactor Regulating System, Control and Process Systems	A	B	C
Shutdown System #1	D	E	F
Ventilation Isolation System	NN	PP	QQ
Emergency Coolant Injection System	K	L	M
Long Term Cooling System	KK	LL	MM
Instrument Electrical Power (Instrument power cables may follow the same routes as I & C cables but shall not share raceways)	ODD	THIRD	EVEN
	Routes 4	Routes 5	Routes 6
Shutdown System #2	G	H	J
Containment System	N	P	Q
Second Crash Cooldown System	X	Y	Z
Reserve Water System, Post Accident Monitoring (dedicated)	R	S	T
Instrument Electrical Power (Instrument power cables may follow the same routes as I & C cables but shall not share raceways)	ODD	THIRD	EVEN

NOTES:

1. Cables in the above associated channels (e.g., A, D, NN, K, KK, ODD) can follow the same cable routes and, with the exception of power cables, can also share raceways.
2. Channels must maintain the association prescribed above with the exception of buffered signals in Routes 4, 5 and 6, which may acquire association with Routes 1, 2 and 3 respectively, beyond the buffering device.
3. Power cables, once associated with a particular route, must maintain this association. For example, an ODD power cable initially associated with channels A, D, NN, K and KK in Routes 1 cannot subsequently be routed with channels G, N, X and R in Routes 4.
4. Cable and equipment identification shall be sufficient to ensure compliance with separation requirements.
5. In the common building, the cable routes shall include identification of the originating unit in order to maintain proper separation as described above.

Appendix A

Typical Events to be Considered for Separation of Safety Related Systems

The following table outlines the typical events to be considered in the plant design to provide adequate separation between safety related systems and between components within each safety related system.

The events and separation considerations are typical and non-mandatory. For specific plant sites, refer to the "Systematic Review of the Plant Design for Initiating Events" for the applicable list of events.

EVENT	TYPICAL CONSEQUENCE	SEPARATION CONSIDERATION
A. OUTSIDE REACTOR BUILDING		
a) External Events 1) Earthquake 2) Site specific events (if applicable, tornado, explosions near the site)	Failure of unqualified or unprotected systems, including: ▪ turbine failure ▪ steam line failure ▪ feedwater line failure ▪ raw service water component failure ▪ recirculated cooling water component failure ▪ condenser cooling water component failure ▪ electrical system failure ▪ instrument air system failure ▪ Main Control Room impairment	▪ Protect or qualify Main Control Room and its essential support services to withstand the event (shut down the plant and maintain in a safe shutdown condition). ▪ Protect or qualify safety related systems components to withstand the event. ▪ Protect safety related systems components from effects of component failures, including fire, missiles, flooding, and adverse environment which occur as a consequence of the event. (Also see 108-03650-SDG-002, 003, 005)
3) Chemical spills or release, Smoke and Biological Hazards (if applicable)	Uninhabitable areas	Provide detection and alarm, and Main Control Room protection.

EVENT	TYPICAL CONSEQUENCE	SEPARATION CONSIDERATION
4) External Flood	Flooding of plant areas	Protect Main Control Room, its support services, from flooding by site grading, and/or barriers, and/or systems to prevent flooding of components, and/or locating systems and components above flood level.
b) Internal Events 1) Large Fires Due to identified hazards, such as: turbine lube oil system generator H_2 cooling system large electrical transformers electric motors with more than 100 litres of lube oil diesel generator fuel supply	Destruction of systems or components within a limited area	▪ Provide fire barriers to protect safety related systems, as defined in 108-03650-SDG-005 ▪ Arrange layout and fire barriers to maintain Main Control Room availability and to ensure access to the Secondary Control Area. This requires fire separation between the ODD and EVEN electric power distribution systems.
2) Small Fires Due to events such as: cable faults in electrical supply or instrumentation systems electrical equipment fires (motors, panels, etc.) Failure of hydrogen addition system components	Destruction of components within a small area	Provide separation between safety related systems components, as outlined in Sections 4.1 and 4.2. ▪ Arrange layout and fire barriers to maintain Main Control Room availability and to ensure access. This requires fire separation between the ODD and EVEN electrical distribution systems. ▪ If separation cannot be maintained, assess fire hazards in the area of the components and systems.

EVENT	TYPICAL CONSEQUENCE	SEPARATION CONSIDERATION
3) Missiles Due to failure of high energy systems (e.g., fluid conditions > 2000 kPa and/or 100°C, or large rotating equipment), such as: steam lines air receivers HP ECC pressurized tanks turbine disintegration	Damage to nearby systems	▪ Provide barrier to protect Main Control Room. ▪ Safety related systems should not be damaged by missiles originating in other systems, local barriers may be provided in the reactor building. ▪ System/plant layout to minimize extent of damage possible.
4) Loss of MCR	Loss of all control functions from Main Control Room, possibility of active control causing an unsafe situation	Provide alternative control and monitoring functions in the Secondary Control Building (shutdown the plant and maintain in a safe shutdown condition). Provide means to switch control to the Secondary Control Building, to the extent that the plant can be shut down and maintained in a safe shutdown condition.

EVENT	TYPICAL CONSEQUENCE	SEPARATION CONSIDERATION
5) Flooding Due to failure of systems containing substantial amounts of water, such as: raw service water systems recirculated cooling water systems condenser cooling water systems backup or upsurge from floor drains reserve water tank	Damage to systems in lower elevations	▪ Provide barrier or sump to protect safety related systems. ▪ Provide a barrier or sump to maintain the availability of the Main Control Room to monitor and control the event (shutdown the plant and maintain in a safe shutdown condition). ▪ Arrange component layout to be above the water level.
6) Adverse Environment (e.g., steam line break) Due to failure of high energy systems, such as: steam lines feedwater lines	Extreme operating conditions for systems in large areas	Provide barriers to protect safety related systems or environmentally qualify the components, to maintain the capability to monitor and control the event from the Main Control Room (shutdown the plant and maintain in a safe shutdown condition).

EVENT	TYPICAL CONSEQUENCE	SEPARATION CONSIDERATION
B. INSIDE REACTOR BUILDING		
a) External Events 1) Earthquake	Failure of unqualified components	▪ Seismically qualify as necessary safety related systems' components to maintain the capability to monitor and control the event from the Main Control Room (shut down the plant and maintain in a safe shutdown condition). ▪ Locate qualified components to avoid damage due to unqualified components.
b) Internal Events 1) Large Fires Due to identified hazards, such as: heat transport pump lube oil large concentrations of cables	Destruction of systems or components within a defined area	▪ Provide separation barriers or distance between safety related components and hazards identified in fire hazard assessment (see 108-03650-SDG-005). ▪ If necessary to protect other components that must perform a safety function for the event, remove smoke and heat from the area of the fire until fire suppression is achieved.
2) Small Fires Due to events such as: cable faults in electrical supply or instrumentation systems electrical equipment fires failure of hydrogen addition system components	Destruction of components within a small area	▪ Provide separation between safety related systems components, as outlined in Section 4. ▪ Provide separation between components within safety related systems' divisions, as outlined in Section 4.4.

EVENT	TYPICAL CONSEQUENCE	SEPARATION CONSIDERATION
3) Missiles/Pipe Whip/Jet Impingement Due to failure of high energy systems (e.g., fluid conditions > 2000 kPa and/or 100°C), such as: steam lines heat transport system components feedwater lines	Damage to nearby components	▪ Provide separation between redundant safety related systems or divisions' components, so not more than one system/division is impaired. ▪ Provide protection barriers for safety related systems/components. ▪ Alternatively, where components of both system/divisions may be damaged, redundant components within system or fail safe design may be used to ensure performance of the safety function.
4) Flooding Due to failure of systems containing substantial amounts of water, such as: recirculated cooling water system heat transport system (include effect of Emergency Coolant Injection)	Damage to systems in lower elevations	Locate essential safety related systems' components above the flood level, or show that the safety function can be performed despite flooding.

EVENT	TYPICAL CONSEQUENCE	SEPARATION CONSIDERATION
5) Adverse Environment Due to failure of high energy fluid system, such as: heat transport system steam supply system feedwater system reserve water tank	Extreme operating conditions for systems in the Reactor Building.	▪ Locate essential safety related systems outside of affected area, where possible. ▪ Qualify safety related systems to withstand the conditions. ▪ For more localized events, separate safety related systems' components with local barriers.

Appendix B

List of Safety Design Guides

Identification	Title
108-03650-SDG-001	Safety Related Systems
108-03650-SDG-002	Seismic Requirements
108-03650-SDG-003	Environmental Qualification
108-03650-SDG-004	Separation of Systems and Components
108-03650-SDG-005	Fire Protection
108-03650-SDG-006	Containment
108-03650-SDG-007	Radiation Protection

Appendix C

Acronyms

AC	Alternating Current
ACR™*	Advanced CANDU Reactor™
AECL	Atomic Energy of Canada Limited
ALARA	As Low As Reasonably Achievable
ASDV	Atmospheric Steam Discharge Valves
BOP	Balance Of Plant
CA	Control Absorber
CANDU®	Canadian Deuterium Uranium®
CCP	Critical Channel Power
CCW	Condenser Cooling Water
CHF	Critical Heat Flux
CNSC	Canadian Nuclear Safety Commission
COG	CANDU Owners Group
CSA	Canadian Standards Association
D_2O	Heavy Water
DBE	Design Basis Earthquake
DC	Direct Current
DCS	Distributed Control System
DEL	Derived Emission Limit
DG	Diesel Generator
EAB	Exclusion Area Boundary
ECC	Emergency Core Cooling
ECI	Emergency Coolant Injection
EDS	Electrical power Distribution System
HTS	Heat Transport System
HV	High Voltage
IAEA	International Atomic Energy Agency
ICRP	International Commission for Radiation Protection
ISO	International Organization for Standardization
LCDA	Limited Core Damage Accident
LOCA	Loss Of Coolant Accident

* ACR™ (Advanced CANDU Reactor™) is a trademark of Atomic Energy of Canada Limited (AECL).

® CANDU is a registered trademark of Atomic Energy of Canada Limited.

LTC	Long Term Cooling
LV	Low Voltage
LWR	Light Water Reactor
MCR	Main Control Room
MOT	Main Output Transformer
MSIV	Main Steam Isolation Valves
MSSV	Main Steam Safety Valves
NEW	Nuclear Energy Worker
NSP	Nuclear Steam Plant
NSSS	Nuclear Steam Supply System
OM&A	Operation, Maintenance and Administration
PAM	Post Accident Monitoring
PSA	Probabilistic Safety Assessment
PTR	Pressure Tube Reactor
PWR	Pressurized Water Reactor
RAB	Reactor Auxiliary Building
RB	Reactor Building
RCU	Reactivity Control Unit
RCW	Recirculated Cooling Water
RSW	Raw Service Water
RWS	Reserve Water System
SCA	Secondary Control Area
SDE	Site Design Earthquake
SDS 1	ShutDown System 1
SDS 2	ShutDown System 2
SEU	Slightly Enriched Uranium
SFC	Single Failure Criterion
SST	System Service Transformer
SU	Shutoff Unit
ULC	Underwriter's Laboratories Canada
UPS	Uninterruptible Power Supply
UST	Unit Service Transformer
ZCU	Zone Control Unit