IAEA Nuclear Energy Series

No. NP-T-1.5

Protecting against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants

IAEA
International Atomic Energy Agency

IAEA NUCLEAR ENERGY SERIES PUBLICATIONS

STRUCTURE OF THE IAEA NUCLEAR ENERGY SERIES

Under the terms of Articles III.A and VIII.C of its Statute, the IAEA is authorized to foster the exchange of scientific and technical information on the peaceful uses of atomic energy. The publications in the **IAEA Nuclear Energy Series** provide information in the areas of nuclear power, nuclear fuel cycle, radioactive waste management and decommissioning, and on general issues that are relevant to all of the above mentioned areas. The structure of the IAEA Nuclear Energy Series comprises three levels: **1 — Basic Principles and Objectives; 2 — Guides; and 3 — Technical Reports.**

The **Nuclear Energy Basic Principles** publication describes the rationale and vision for the peaceful uses of nuclear energy.

Nuclear Energy Series Objectives publications explain the expectations to be met in various areas at different stages of implementation.

Nuclear Energy Series Guides provide high level guidance on how to achieve the objectives related to the various topics and areas involving the peaceful uses of nuclear energy.

Nuclear Energy Series Technical Reports provide additional, more detailed, information on activities related to the various areas dealt with in the IAEA Nuclear Energy Series.

The IAEA Nuclear Energy Series publications are coded as follows: **NG** — general; **NP** — nuclear power; **NF** — nuclear fuel; **NW** — radioactive waste management and decommissioning. In addition, the publications are available in English on the IAEA's Internet site:

http://www.iaea.org/Publications/index.html

For further information, please contact the IAEA at PO Box 100, Vienna International Centre, 1400 Vienna, Austria.

All users of the IAEA Nuclear Energy Series publications are invited to inform the IAEA of experience in their use for the purpose of ensuring that they continue to meet user needs. Information may be provided via the IAEA Internet site, by post, at the address given above, or by email to Official.Mail@iaea.org.

PROTECTING AGAINST COMMON CAUSE FAILURES IN DIGITAL I&C SYSTEMS OF NUCLEAR POWER PLANTS

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHRAIN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
BURUNDI
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA
VIETNAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

IAEA NUCLEAR ENERGY SERIES No. NP-T-1.5

PROTECTING AGAINST COMMON CAUSE FAILURES IN DIGITAL I&C SYSTEMS OF NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2009

COPYRIGHT NOTICE

Sales and Promotion, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
November 2009
STI/PUB/1410

IAEA Library Cataloguing in Publication Data

Protecting against common cause failures in digital I&C systems of nuclear power plants. — Vienna : International Atomic Energy Agency, 2009.
p. ; 29 cm. — (IAEA nuclear energy series, ISSN 1995–7807 ; no. NP-T-1.5)
STI/PUB/1410
ISBN 978-92-0-106309-0
Includes bibliographical references.

1. Nuclear power plants — Instruments. 2. Nuclear reactors – Computer programs. 3. Nuclear reactors — Control. I. International Atomic Energy Agency. II. Series.

IAEAL 09–00607

FOREWORD

An IAEA programme on Nuclear Power Plant Operating Performance and Life Cycle Management is aimed at improving Member State capabilities in utilizing good engineering and management practices developed and transferred by the IAEA. In particular, it supports activities such as improving nuclear power plant performance, plant life management, training, power uprating, operational licence renewal and the modernization of instrumentation and control (I&C) systems of NPPs.

The subject of preventing common cause failures (CCF) in the digital I&C systems of nuclear power plants was suggested by the Technical Working Group on Nuclear Power Plant Control and Instrumentation (TWG-NPPCI) in 2003 and 2005.

The issue of CCFs in computer-based safety I&C systems is of great interest because an increased number of such systems will be implemented in nuclear power plants in the future. Although computer-based I&C is widely used in non-nuclear industry safety systems, there are uncertainties in the safety assessment of such systems in the nuclear industry. In particular, demonstrating the absence of CCF remains a subject of discussion.

A CCF is the concurrent failure of two or more SSCs due to the triggering of a single systematic fault or causally related faults by a single specific event. The design of I&C systems involves considerable effort to minimize the risk of CCFs which may interfere with the safety functions of the I&C system. For analogue systems, the occurrence of CCF was attributed to slow processes such as corrosion or wear-out; however, with digital systems, the prevalence of software raises new concerns with respect to CCFs triggered by a latent fault in the software.

This report, prepared within the framework of the the Technical Working Group on Nuclear Power Plant Control and Instrumentation, discusses the potential sources of CCFs in I&C systems used for safety along with methods to prevent their occurrence or at least identify and mitigate their effects. Several approaches to evaluating the vulnerability of digital I&C systems to CCFs are presented. The intended audience of this report includes nuclear utilities, vendors, regulatory authorities and others involved in the design and implementation of I&C systems in nuclear power plants.

The IAEA wishes to thank all participants and their Member States for their valuable contributions. The Chairmen of the four meetings held for the development of the report were: A. Lindner from Germany, and S. Arndt and R. Wood from the United States of America.

The IAEA officer responsible for this publication was O. Glöckler of the Division of Nuclear Power.

EDITORIAL NOTE

This report has been edited by the editorial staff of the IAEA to the extent considered necessary for the reader's assistance. It does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Since the early development of digital computer based safety systems for nuclear power plants, the subject of potential for concurrent system failures due to latent errors (or faults) in computer software has been considered. Such failures could defeat the redundancy achieved by hardware architecture. This potential was not present in earlier analogue protection systems because it was assumed that common cause failure (CCF), if it did occur, was due to slow processes such as corrosion or premature wear-out of hardware. This assumption is no longer true for systems containing software. Although software does not wear out, digital instrumentation and control (I&C) systems are potentially vulnerable to CCF caused by software faults.

Software usually does not fail in the sense that hardware components fail in analogue systems. In the case of digital systems, software works incorrectly (i.e. does not perform its intended function), if:

— Its specification was inadequate, incomplete or incorrect;
— Its specification was interpreted incorrectly during implementation; or
— Testing did not include the specific signal trajectory that reveals the fault.

Since software cannot be proven to be 100% error free, software design faults are a credible source of CCF: The choices of software languages, programming rules, software verification processes and system testing for computer-based safety systems lessen the likelihood of CCF. It is also possible to incorporate design features and characteristics of I&C that preclude, avoid or limit the propagation of some types of CCFs (e.g. use of defensive measures). However, the need to maintain an acceptable level of safety necessitates an evaluation of the impact of such malfunctions and the implementation of mitigating features where needed.

As used in this report, CCF is the concurrent failure of two or more structures, systems or components (SSCs) due to: (1) the triggering of a single systematic fault or (2) causally related faults by a single specific event. The triggering event may be related to time, data or hardware. The term “common-mode failure” is not used because CCF is more inclusive of the effects related to the failure.

A systematic fault affects all components of a specific type (hardware or software). The fault may be injected during the design or the manufacturing process, or it may be related to maintenance or modification activities. A triggering mechanism is a specific event or operating condition, which causes SSCs to fail due to the latent fault. Thus, a systematic failure is related in a deterministic way to a certain cause [1]. The failure will always occur when the design fault is challenged by the triggering mechanism. In order for such a failure to occur, the following conditions must be present:

— A systematic fault must exist in multiple components in the integrated system;
— A triggering event must occur to challenge the systematic fault.

A CCF is a systematic failure that occurs when failures of separate SSCs are triggered concurrently. The failures are considered concurrent if the time interval between the failures is too short for repair or recovery measures to be taken.

1.2. OBJECTIVE

The objective of this report is to aid utilities, suppliers/vendors and consultants in the design of I&C systems with minimal susceptibility to CCFs. It discusses potential sources of CCFs in I&C systems used for safety as well as measures that may be taken to prevent CCFs, or at least identify it and control its harmful effects. The discussion includes evaluation of the vulnerability of I&C systems to CCFs as it may be performed by technical safety organizations, third-party groups and regulatory authorities.

1.3. SCOPE

This report addresses concurrent failures in I&C systems, including redundant systems, systems intended to provide diversity for similar tasks and systems performing different tasks. The consideration includes digital as well as analogueue and hybrid I&C systems that are used for safety. Figure 1 illustrates a typical relationship among control and protection systems in an NPP that extensively utilizes digital technology for the human–machine interface (HMI) as well as the signal processing electronics.

The systems addressed in this report are required to perform functions of the same safety significance (e.g. category A as defined in Ref. [2] as well as functions of different safety significance). This report focuses on the safety of the controlled systems rather than their reliability.

The concurrent failures discussed in this report are not limited to IEC 61226 [2] category A devices and the level of defence in depth concept. Other areas covered by the report include complex or advanced computer systems (systems with multiple processors), devices with embedded processors and software such as sensors, actuator controllers and smart uninterruptible power supplies (UPSs). This report is applicable to new plants as well as to retrofits being implemented in existing plants.

1.4. PHILOSOPHY

If an evaluation of CCF vulnerability is performed when a project is virtually complete, there is a serious risk that extensive rework or redesign may be necessary if the system is determined to be susceptible to CCF late in the development life cycle [3]. This is because more personnel and resources are required to address a defect in the later phases of the life cycle.

To avoid this scenario, a strategic approach should be implemented early in the project life cycle. The strategic approach is iterative and can include the steps shown in Fig. 2, which can be performed at different times (e.g. equipment selection, manufacture, integration, implementation, etc.) and by different agencies.

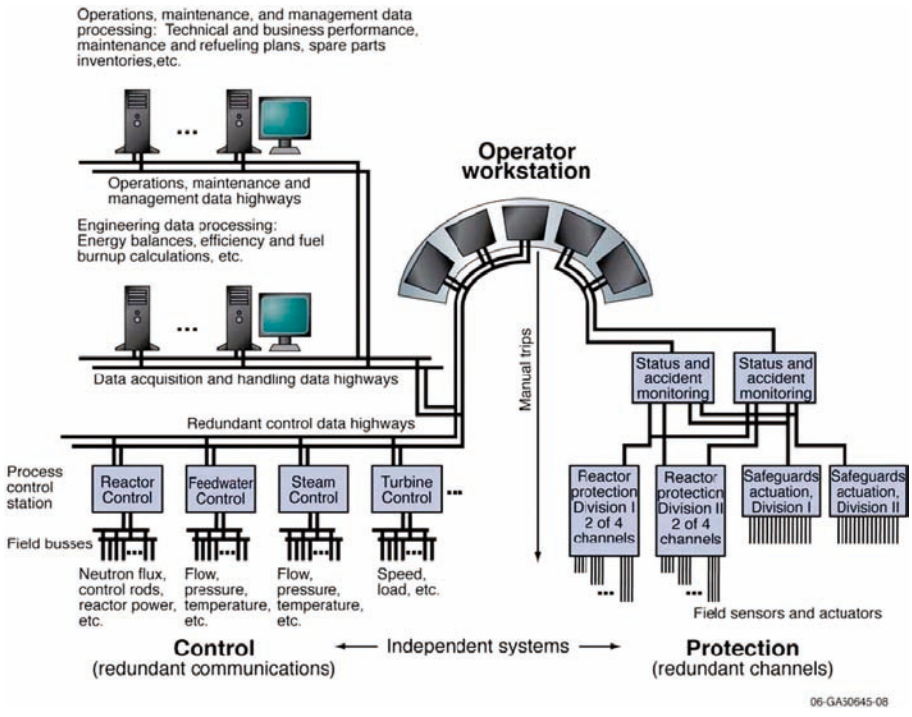


FIG. 1. Typical digital NPP protection, control and HM I&C architecture.

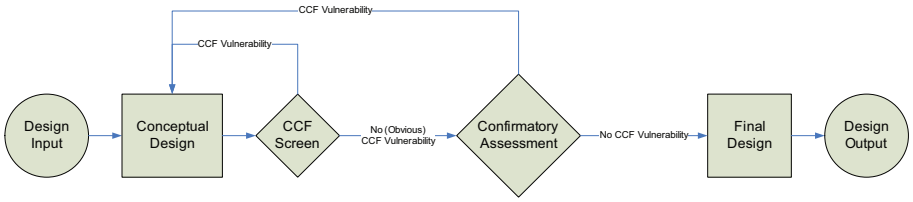


FIG. 2. Iterative CCF evaluation process.

(1) Conceptual design

The conceptual design provides a high-level description of system function, architecture and goals. The conceptual design should contain sufficient detail to identify subsystem boundaries, interfaces and communications, yet not be so detailed that hardware is specified. The conceptual design document should contain descriptions of how the proposed design achieves functional goals, safety goals and preliminary defence in depth and diversity (D3) requirements. The conceptual design will be refined iteratively in the following steps.

(2) CCF screen

A screening evaluation is performed on the conceptual design to determine CCF susceptibility. The evaluation is performed to a depth that is appropriate to the level of detail in the conceptual design. References [4, 5] provide examples of methodologies that may be used to conduct the evaluation. If no harmful[1] vulnerability is found (that is, harmful vulnerabilities "screen out"), the evaluation is complete.

(3) Refinement

The conceptual design is modified (i.e. refined) to correct vulnerabilities identified in the CCF screen. The refined conceptual design is subjected again to the CCF screen identified in the previous step. Thus, refinement is an iterative process of adjusting the conceptual design architecture, scope of system supply or assumptions until the CCF screen identifies no further vulnerabilities.

The intent of this process is to identify and remove (or neutralize) harmful design vulnerabilities (i.e. vulnerabilities that can lead to failure of the I&C system to perform its safety function when that function is required to occur in response to a test or to mitigate a design basis accident or event).

A given system may contain systematic faults. However, the faults do not become failures until they are challenged, and the failures are not harmful unless they impair a safety function when it is required. That is, not all faults become failures, and not all failures are harmful. Further, a given failure is not a CCF until multiple channels of a redundant system are affected.

Therefore, it is not necessary to demonstrate that all software faults have been removed from the system design. It is necessary to develop reasonable assurance that the software does not contain faults that can be triggered to become harmful failures that can, in turn, lead to CCF. Because it is not possible (except in the most simple applications where 100% functional testing can be performed) to assure that all such faults have been removed, defensive measures are incorporated into the design to enable the engineering judgement of reasonable assurance of safety. Defensive measures are discussed later in this report.

(4) Confirmatory assessment

The confirmatory assessment is performed on the conceptual design once it is refined to the extent that no obvious CCF vulnerability can be identified. The confirmatory assessment may include failure modes and

[1] A vulnerability is harmful if it can lead to failure of the I&C system to perform its safety function at the time that function is required in response to a test or to mitigate a design basis accident or event.

effects analysis (FMEA), thermal-hydraulic analysis or other analytical methods required to provide reasonable assurance that the system will perform the required safety function if a design basis event (DBE) occurs concurrent with a CCF that disables multiple channels of the subject redundant system. If vulnerabilities are identified, the design should be refined as described in the above step.

The confirmative assessment is very detailed, and hence expensive to perform. The purpose of performing a CCF screen and iteratively refining the conceptual design is to limit the analytical effort that is performed.

At the end of this process, the refined conceptual design may serve as the basis for specification of functional requirements. In addition, documentation will be available to support application for approval of the system for use in its intended function by the appropriate regulatory body or agency.

1.5. IMPORTANCE OF I&C SYSTEM CCF

In a nuclear power plant, both the potential for CCF of I&C systems and the defence against them need to be considered in different contexts for which there are often very different design constraints and practices. Therefore, the justification of adequate defences against CCF needs to be based on different approaches and to rely on different considerations.

1.5.1. Effects of CCF

Residual software or digital design defects are by definition undetected during the design and implementation phases. Once triggered, the latent software defects become software failures that could lead to CCF. Such failures can cause one of two possible conditions: (1) outputs that change states (or values); or (2) outputs that fail as-is. Spurious state changes (including partial actuations) reveal the failure and need not be considered concurrent with accidents provided that appropriate means remain to assure that any necessary mitigating action will be taken in a timely manner.

An as-is CCF is not revealed until there is a demand failure (whether in response to a test or an accident) whereby the failed system does not perform its design safety function (i.e. trip the reactor, actuate engineered safety functions) and does not generate alarms. Therefore, the defence in depth and diversity (D3) evaluation may be limited to demand failure of the safety function due to CCF. That is, the safety function does not occur when it is expected or required to mitigate the accident or event of concern.

Failure of the protection system to respond (i.e. the fail as-is condition) to the postulated accident will be detected by the operator as he executes emergency procedures or by the technician as he executes the test procedure. During an accident, the operator will also be made aware of the CCF by alarms generated from the diverse actuation system or other plant I&C equipment.

During normal operation, a CCF may cause spurious actuations (fail low/open or fail high/closed). This event will provide indications of abnormal behaviour (e.g. outputs change state, equipment starts/stops) that the operators or automation can detect and correct. Although spurious actuations generally have a limited effect on safety, their impact should be evaluated.

1.5.2. CCF of multiple lines of defence

Defence in depth is a principle of long standing for the design, construction and operation of nuclear reactors. It may be thought of as requiring a concentric arrangement of protective barriers or means (see Fig. 3); before a hazardous material or dangerous energy can adversely affect human beings or the environment, all of the barriers must be broken. Figure 3 illustrates an example of defence in depth; that is, the three classic physical barriers to radiation release in a reactor — cladding, reactor pressure vessel and containment [5].

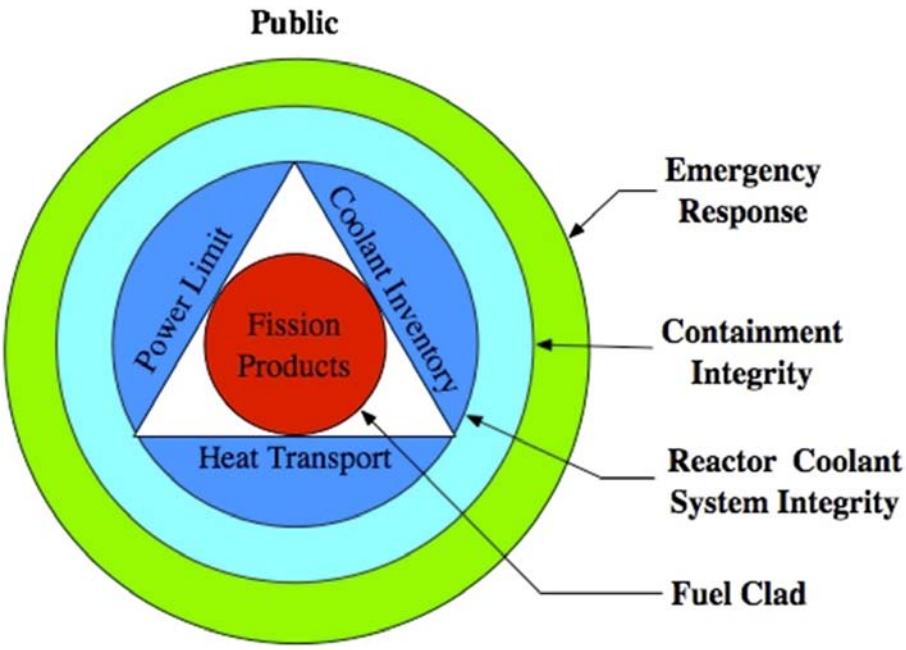


FIG. 3. Defence in depth — barriers to radiation release.

I&C systems have an important role in maintaining the integrity of these barriers. The D3 evaluation should show that CCF within I&C systems that act to protect these barriers cannot lead to unacceptable radioactive release[2].

To do so, the overall NPP I&C architecture includes several independent levels of defence, which usually rely on functional diversity, design diversity and operational diversity as described later in this document. The D3 analysis of the plant I&C should show that CCF within I&C systems that may act to protect these barriers cannot lead to unacceptable radioactive release.

1.5.3. CCF of diverse functions within a safety system

In many safety I&C systems, independent subsystems implement diverse functions in order to cope with the failure of one function or subsystem. Each subsystem has its own internal redundancy. The subsystems may be based on the same equipment platform and use the same system software. Independent (diverse) subsystems may be required to provide alternative functions that will mitigate the harmful effects of an accident or event that is concurrent with the CCF of multiple channels of one or more subsystems.

1.5.4. CCF of channels of redundant systems

Redundancy is a proven approach to achieve safe and dependable systems. However, in most I&C architectures, the channels of a redundant system have identical functionalities and designs, and are based on the same equipment and software components. Therefore, reliance on redundancy alone may not be sufficient to achieve safe and reliable operation when considering the effects of an accident or event that is concurrent with the CCF of multiple channels of one subsystem.

[2] What is considered as unacceptable release may differ between Member States. In some Member States, the acceptable consequences of an event in conjunction with CCF within the protection systems are higher than the levels accepted for the same event in conjunction with only random failures.

1.6. RELATIONSHIP TO OTHER WORK

The presentation of potential sources and effective prevention of CCF in this document is closely related to several existing reports and guidelines such as EPRI 1002835 [4], NUREG/CR-6303 [5], USNRC Branch Technical Position HICB-19 [6] and VDI/VDE 3527 [7]. Ongoing standardization projects including IEC 62340 [8], IEC 60880 [9], IEEE 603 [10] and IEEE 7-4.3.2 [11] address CCF and its mitigation. IEC 62340 [8] is a valuable reference to many other IEC standards related to CCF.

This report does not repeat the information provided by the references cited above. Rather, it focuses on the relationship between potential sources of information regarding CCF and its mitigation. For more details on other aspects of CCF, I&C design and analysis of I&C systems, users of this publication should refer to the reports mentioned above.

2. CONTEXT AND CONSIDERATIONS FOR CCF EVALUATION

The basic approach for ensuring adequate protection against CCF is to evaluate the potential CCF mechanisms against the design characteristics of the I&C system, defensive measures and diversity attributes that will act to preclude, avoid or mitigate them, and then to refine and augment the system as needed. Generally, the process will be iterative, as described in Section 1.4. When a credible susceptibility to CCF is found, changes in the system architecture or other additional measures may be necessary. Added CCF protection may include new design features, development process elements and/or diversity attributes. This evaluation approach is also useful in assessing the adequacy of an existing or proposed system/architecture.

The CCF evaluation should systematically consider the entire I&C architecture, including its functional units, shared resources, interface and communication elements, in the context of their roles in supporting primary and secondary mitigation functions for the various design basis events and anticipated operational occurrences of interest. Different types of architectural elements are subject to different CCF concerns and amenable to different defense measure approaches. For example, for programmable platforms that are used in multiple redundancies or systems, common software modules might be considered potential sources of CCF, depending on the defensive measures that have been implemented.

Communication interfaces will involve different concerns (e.g. the need to ensure that misbehaviour of a mitigating system cannot disable other mitigating systems that are part of the overall defence in depth strategy for the same plant events). Section 4 provides a detailed discussion and examples of CCF assessment techniques.

Utilities, vendors and regulators will address CCF from different perspectives. Vendors of equipment for safety-critical applications will focus on the need to provide a design that includes defensive measures that limit vulnerability to CCF. Utilities will have a broader perspective. They will want to assess the vendor's design measures and perhaps perform independent evaluations to develop reasonable assurance that specific digital components and platforms are adequately protected from CCF. Additionally, they will evaluate the vulnerabilities of specific plant systems and the overall plant I&C architecture to potential CCF mechanisms. The regulator will need to confirm that there is reasonable assurance of adequate protection against credible CCF.

CCF considerations for new and existing plants are somewhat different. Existing plants typically have mostly analogue I&C equipment. As they start to modernize the I&C, replacing analogue equipment with digital, the retained analogue equipment provides a degree of technological diversity, which may be credited in CCF evaluations where it effectively eliminates certain types of CCF susceptibilities. At the same time, operating plants will be constrained in terms of their ability to modify the plant I&C architecture to reduce CCF vulnerability, as the distribution of plant functions, system internal redundancy, diversity, and so on are predetermined and fixed. New plants will use digital I&C almost exclusively; technology diversity will not, for the most part, be a useful CCF protection mechanism. Instead they will rely more heavily on internal design

features and characteristics that protect against CCF and utilize other forms of diversity, such as design or functional diversity, to achieve adequate CCF protection.

2.1. CONDITIONS REQUIRED FOR CCF

For a potentially unsafe CCF to occur, a number of conditions must be met (Fig. 4):

— The system contains one or more faults that can cause functional failure;
— A triggering event, usually an unanticipated or untested operational condition, is present to activate the fault;
— Multiple channels are affected concurrently;
— The failures cause an unsafe plant condition, typically in the form of degradation or loss of a function needed to mitigate a design basis event or an anticipated operational occurrence when mitigation is required. A CCF could disable a mitigating function while simultaneously initiating an event that requires the mitigating function;
— To adversely affect multiple systems, those systems must share the same fault(s) and be susceptible to the same trigger concurrently.

A CCF strategy should reflect careful consideration of which digital systems and components might be credible sources of digital CCF, and which need not be addressed because they can be shown to be highly unlikely contributors to CCF. In implementing diversity and defensive measures, tradeoffs will be needed between adding complexity and enhancing safety. A diversity-only approach has significant drawbacks; it increases functional, design, operational and maintenance complexity. In some cases, it does not ensure adequate protection or provides a less than optimal solution. It can also introduce difficulties in deciding which course of action should be taken when two diverse systems disagree. Therefore, careful assessment of CCF susceptibility is critical in keeping the strategy simple, practical and effective.

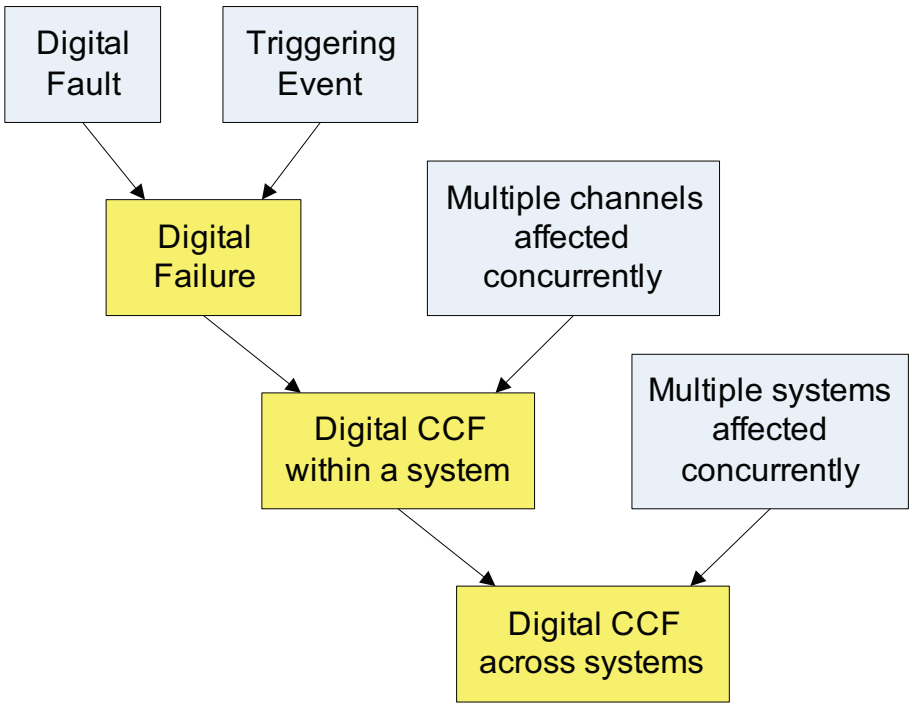


FIG. 4. Conditions required to create a digital CCF.

2.2. CCF SUSCEPTIBILITY EVALUATION

System and equipment designers employ practices that are intended to minimize latent digital faults. As it is virtually impossible to completely preclude the existence of residual faults, designers also use techniques and features that limit the potential for the occurrence of triggering conditions that could activate them. An assessment of CCF susceptibility should systematically consider all the mechanisms that may cause CCF in a specific component or architecture as well as the defensive measures being utilized that effectively reduce digital faults or limit activating conditions for them. The goal is to determine which combinations of faults and triggers are credible in light of the system design characteristics and defensive measures.

The evaluation may involve system decomposition (e.g. into function, logic modules, etc.) to address potential vulnerabilities in a systematic manner. This can be done at whatever level is appropriate, from the global plant I&C architecture down to components or subcomponents that are used in multiple (trains/divisions) or plant systems. Section 4 provides an example of a decomposition approach.

Sections 3 and 5 provide detailed discussion on CCF mechanisms and corresponding defensive measures to address them.

The basic process is to:

— Determine which CCF mechanisms apply, along with the types of faults, failures and CCFs that might be relevant;
— Identify the defensive measures in place to avoid, eliminate or mitigate such failures; and
— Assess the effectiveness and completeness of the defensive measures.

The evaluation will likely involve a review of the design, supplier processes, documentation and operating history to assess the effectiveness and coverage of the defensive measures that are in place and whether there is reasonable assurance that the CCF likelihood is low enough to exclude the component from further consideration in the evaluation. A key consideration will be assessment of component complexity and internal modularity, including their impacts on effectiveness of factors such as testability and operating experience. Because the review addresses a wide range of topics in detail, an interdisciplinary team will be needed to provide the necessary breadth and depth of expertise. Useful disciplines will likely include software design and development; software-based, real-time control; plant system engineering and change control processes; and nuclear quality assurance requirements.

2.3. USE OF RISK INSIGHTS

There is no general consensus on the best ways to model software-based equipment in probabilistic safety analysis (PSA). However, PSA can still offer useful insights to support CCF evaluations and decision making, particularly in regard to a qualitative understanding of:

— Which CCF events are important from a safety perspective;
— Which initiating events, systems and components are important from the CCF perspective;
— Where increasing defence against CCF (e.g. adding diverse backups for the I&C) is of value in the context of the plant design;
— How reliable a digital system needs to be in the nuclear plant context to be a negligible contributor to overall risk.

For example, in current plants, for rare events such as large loss of coolant accidents (LOCAs), PSA will typically show that adding a diverse I&C backup to compensate for CCF vulnerability is of limited value, because the mitigating system reliability is dominated by hardware elements, and improving the I&C reliability has very little effect on the safety system reliability. In fact, a diverse backup might actually cause a slight increase in risk due to its potential for introducing increased complexity, new failure modes and spurious actuations. Conversely, for high-frequency events, such as turbine trip or loss of feedwater, providing diverse I&C in the multiple mitigating systems may result in significant benefit from the risk perspective because it

ensures that existing plant system-to-plant system diversities will be preserved. These insights may be different for new plants, which may use more stringent risk goals and more passive safety system designs with reduced reliance on active mechanical systems.

Estimating failure probabilities of digital equipment has proven problematic. Software-related failures are not random as is the case with hardware failures. Random hardware failure probabilities are typically based on ageing and wear-out of hardware components. Software does not wear out; it behaves deterministically, and identical software modules in redundant trains or systems can be expected to produce identical responses when subjected to the same set of input conditions. Software can then cause malfunctions by generating undesired responses to unanticipated or untested conditions. While such misbehaviours are not, strictly speaking, random, they depend on the combination of particular faults and triggers, the likelihood of which can be influenced by system designers and users. A high-quality software development process will reduce the likelihood of latent faults, and various defensive measures can be used to reduce the potential for the digital equipment to encounter and respond incorrectly to unanticipated conditions (eliminate triggers).

Compiling statistically significant failure data for software in nuclear safety applications is particularly difficult. Safety systems are typically stand-by systems that monitor plant parameters and are called upon to act only when needed to drive the plant to a safe state. Therefore, the statistic of interest is the probability of failure-on-demand. However, nuclear plants generally operate with high reliability, so safety systems are not often called upon to act. Additionally, various quality, design and testing requirements are used to ensure that they will be highly reliable, so failure-on-demand is exceedingly rare. The result is that the statistical approach typically used for hardware components (compiling failure data from many applications) is not generally useful for software in safety systems.

At this point, there are no established correlations between software development practices, use of defensive design measures and digital system reliability. However, qualitative estimates have been made. IEC 61226 [2] states that:

> "For an individual system which incorporates software developed in accordance with the highest quality criteria (IEC 60880 [9] and IEC 60987 [12]), a figure of the order of 10^{-4} failure/demand may be an appropriate limit to place on the reliability that may be claimed."

It has been suggested that further reductions in estimated failure probability may be appropriate if adequate defensive measure design features are used in addition to a high-quality development process (Ref EPRI 1002835 [4]). Even without precise knowledge of digital system reliability, qualitative risk insights can contribute to CCF evaluation and decision making, and ongoing research efforts will likely yield better, more accurate methods in the future.

2.4. USE OF SMALL DEVICES WITH EMBEDDED SOFTWARE

In the electrical and electronic systems in nuclear power plants, there was, and still is, the need to use numerous small devices. In many cases, such devices are commercial-grade, and the suitability of their use is demonstrated by evaluation and testing. Nowadays, the functionality of such devices is usually controlled by embedded software that determines the functionality within the limits set by parameterization. Examples of small devices with embedded software are "smart" transmitters, timing relays or load-limiting relays. These types of devices are often overlooked as sources of potential digital CCF due to their simplicity and use as components within larger systems. However, they may contain latent faults if the range of relevant operating conditions was inadequately tested, for example, or if the ranges for the potential parameters and functionality which could be encountered are too large to be covered by testing.

2.5. AGEING AND LIFE CYCLE ISSUES

Digital I&C equipment becomes obsolete much more rapidly than its analogue predecessors. As a result, it will likely need update and replacement cycles for both obsolete software and hardware components. Such changes could impact CCF protections and should be considered as part of the plant modification processes.

3. POTENTIAL MECHANISMS CAUSING CCFs

3.1. PHENOMENA OF CCFs

The design principle of using diversity and redundancy together with voting mechanisms has proven to be very useful to minimize failures in I&C systems. I&C systems which meet the requirements of the single failure criterion are capable of performing their intended functions even in the presence of a single random failure. This design criterion assures that the likelihood of failure for such I&C systems is very low.

For I&C systems using the design principles described above, functional failures require two or more redundant channels to fail concurrently. This can result from CCF if a latent fault has been incorporated in some or all channels, and if these faults are triggered by a specific event in multiple channels. The failure of a redundant I&C system occurs if the number of faulted channels results in the voting mechanism making an erroneous selection, such as in causing a spurious actuation or failure to act on demand.

Latent faults that are systematically incorporated in all redundant channels may originate in different phases of an I&C systems life cycle. An overview of the examples of the potential faults most relevant to CCF is given in Section 3.2.

The existence of a triggering mechanism and a latent fault is necessary to cause the coincidental failure of two or more channels. The concurrent triggering of multi-channel failure renders redundancy ineffective in coping with potential CCF.

Because of the large variety of potential latent faults and potential triggering mechanisms, different channels may have correlated but sequential failures. With respect to the resultant system failure, no differentiation is made between such differences in timing, if repair or corrective action, is not possible within the time interval between failures of individual channels. The term of concurrent failures is used to address all such failure sequences.

An overview of the most relevant examples of potential triggering mechanisms is given in Section 3.3.

3.2. POTENTIAL SOURCES OF FAULTS

One of the challenges faced when applying effective design measures to guard against CCF is the difficulty of designing specific measures to guard against latent faults or of proving that the design of an I&C system is free from latent faults. However, since the occurrence of CCF depends on the existence of triggering mechanisms, it is possible to design a line of defence removing potential concurrent triggering mechanisms. This requires a good fundamental understanding and postulating the potential types of faults and triggering mechanisms which are relevant and realistic where the selected technology is utilized.

Some latent faults may be independent of the use of digital I&C; the risk of introducing such faults is unchanged from conditions that apply to traditional analogue I&C designs. Examples of this type of fault are:

— Errors in standard functions, such as trigonometric functions, which can result in incorrect calculations;
— Operating outside the valid parameter bounds of an algorithm or standard function can result in incorrect calculations or out-of-range results;
— Poorly constructed algorithms can result in loss of accuracy;
— Effects in data processing due to poor signal to noise ratio;

— Mismatch of equipment voltages can result in incorrect operation or equipment damage;
— Use of inconsistent engineering units or inconsistent point of reference can result in inaccurate calculation or incorrect trip determinations;
— Improper system design can result in non-safety functions that impact safety functions.

Other latent faults are more important for digital I&C systems; some examples of these are:

— Improper integration of a distributed computing system can result in incorrect operation of the I&C system. Data flow through a distributed computing system typically employs asynchronous operation. The design needs to ensure deterministic functional performance. Where data buses are used, functional priorities need to be ensured.
— Errors in amplitude quantization and sampling frequencies can affect transient response, resulting in incorrect operation of the control system. The interface for both the sensed data and the actuators may be impacted. Asynchronous sampling or different sampling frequencies in distributed systems can increase the complexity of this issue if data are assessed in both time and frequency domains.
— Inconsistencies in data communication protocols can cause incorrect operation. Data protocols must be established to ensure consistent communication. Issues such as word length and parity must be addressed. Communications cannot be treated as a "black box"; the behaviour of the functions in the each device must be understood.
— Errors in software libraries can result in a variety of improper operations. Libraries are used not only for mathematical functions but also for functions such as display icon generation and data transfer protocols. Errors in libraries can impact all application functions using that library function.
— Digital equipment is more susceptible to variations in input voltage and frequency than analogue equipment. Both the connections to the power and connections between modules should be considered.
— Filtering effects on both data and signals need to be understood. Sensors as well as communication modules can act as band pass, high pass or low pass filters and have response times that need consideration when determining system performance.

The identification of potential latent faults should begin at the conceptual design phase. However, faults may be introduced at any phase in the life cycle of an I&C system. Different phases of the life cycle are likely to see the introduction of different types of faults. Therefore, the examination of potential latent faults should be considered at each phase.

3.2.1. Conceptual design

The conceptual design establishes the fundamental architecture of the I&C system and allocates the basic application functions to the elements within the architecture and should establish the conceptual approach employed. This phase of the project defines the scope for the I&C project, including identifying the plant systems to be controlled. A block diagram is developed to identify the key classes of equipment, some high-level relationships and interfaces and an initial estimated number of items in each class.

During this phase of development the potential sources of faults to be considered are:

— An incomplete understanding of the plant processes and the required instrumentation, including types, locations and numbers of sensors;
— Significant uncertainties in the conceptual design specification, causing issues related to the scale or scope of the I&C system;
— Excessive complexity of the conceptual design. This is sometimes due to the desire to have the ability to perform additional functionalities that are in addition to those required for proper system safety functions. The added complexity increases the risk of errors introduced in the overall life cycle of the design;
— Allocation of functions to the architecture, which have a negative impact on the ability of the conceptual design to meet communication and timing requirements of the system.

3.2.2. Requirements specification

During the requirements specification, the interfaces between the sensors, signal conditioning, communication, I&C systems and actuators are established. The functional requirements are established. The requirements specification phase has the potential to introduce latent faults that could be potential causes of CCF. The adequacy of the requirements specification is crucial to the subsequent behaviour and functioning of the integrated I&C system. Cooperation between all stakeholders has been observed to enhance the quality of the system requirements specification.

The following examples address essential sources of errors where the specified requirements may be incomplete or inadequate, causing latent faults in the resulting I&C system:

— Designers responsible for the requirements specification had an incomplete understanding of the plant processes and the necessary instrumentation;
— Requirements specification was not formulated clearly, causing misinterpretations at a later phase in the life cycle;
— The timing design requirements for the system are incomplete or incorrect;
— Excessive complexity can be introduced into the design specification. The desire to introduce added functionality should be carefully considered during all phases of the design.

It is particularly important to facilitate communication between system designers and control engineers; since differences in the educational, professional and language background of those responsible for the requirements specification and the system design may lead to misinterpretations or misunderstandings, thus causing latent faults in the system design. Ongoing communication through all phases of the system development is recommended.

It is good practice to validate all specified functional requirements against validated models of the plant processes, since faults identified in a later phase of the I&C life cycle may have more severe consequences. While requirements assessment provides an important basis for systems development, it is also essential that the individual requirements can be clearly traced back to the requirements specification when considered during the subsequent development phases.

In NPP modernization projects, significant effort may be required to elicit the original design basis of the plant and to give an adequate description of the existing I&C system. One challenge can be addressing large numbers of documents and harmonizing old and additional new requirements, which may include implementation of new standards. At the beginning of some modernization projects, a re-examination of the plant safety analysis may be necessary to identify and then clarify any missing requirements.

3.2.3. Development

In the development process, the selected technology is used to implement a system that meets the requirements. The effects of inadequate design specification can propagate through all phases of the system life cycle, and steps should be taken to adequately assure that the design specification has been properly transferred into the final design. Based on the requirements for the system, different approaches to the design can be used. Some approaches focus on design simplicity, whereas others employ higher levels of complexity and functionality.

In most analogue designs, the flow of information passes through a single path from the sensor, through signal conditioning, to use (display or actuation), and is separate for each parameter.

In digital systems, the functions and communication are more integrated. In this type of system, information is shared in different parts of the system. This allows multiple channels to be used and various voting schemes to be implemented. In integrated systems, precautions should be taken to ensure isolation of key channels and to provide protection from cross-talk, and electromagnetic interference (EMI). The sharing of information between parts of the system adds additional communication functions, and it is necessary to avoid the addition of unintended functions.

In all cases, the benefits of the additional complexity should be evaluated against the potential errors that may be introduced by the additional functions. Some areas to be considered in this evaluation are described in the following sections.

3.2.3.1. Configuration control

Incorrect system configuration and software version management can introduce latent errors into the system. Configuration control of analogue systems is also important, but in a digital system, the number of components that must be under configuration control is increased, and the dependence of the different components is more complex. For example, a change in communication software that is transmitting information may require a change to be made in the interfacing system. The configuration of every hardware and software component should be controlled. The risk of introducing a latent fault into the design is increased when changes are made during the development phases.

3.2.3.2. Verification and validation

The verification and validation (V&V) activities that are required for a digital system are more complex than those required for an analogue system. V&V tools used for digital systems typically contain additional software, and the limits of these tools should be considered when evaluating the ability of the V&V process to identify latent faults. It is good practice to assess required performance against existing software components or off-the-shelf software, and to use software that has already been validated on other projects.

3.2.3.3. On-line monitoring

On-line monitoring within the I&C system adds complexity, but it also enhances the system's situation awareness and reliability; it also provides the potential to add enhanced functionality that can potentially impact PSA. The ability to identify components with "ageing" or other changes, before performance is impacted, can enhance both the safety and reliability, as well as help provide early identification of both stressors and effects that can potentially cause CCF. Most modern digital systems now use some level of automated self-testing, diagnostics and/or protective measures. These features are designed to mitigate the effects of faults in digital systems, but, if not properly implemented, they can cause system failures and because they are designed to protect the entire system, they can also cause CCFs. Some of the ways in which diagnostics or self-test features can cause CCFs are:

(1) Causing the system to be unavailable when safety action is required;
(2) Taking the system off-line when it is not degraded and could be available;
(3) Reconfiguring the systems (switching to a backup computer, etc.), which leads to an unusual system state or initiating condition.

These potential root causes for CCFs can be introduced in various ways (e.g. incomplete or inaccurate requirements specification and design). Reviews have historically focused on ensuring that all requirements have been incorporated. It is important that these reviews now include the evaluation of the potential for introducing latent faults into the system.

3.2.3.4. Out of range data

Signals from sensors or subsequent data processing can be outside designed calculation range during accidents, plant transients or failures. In analogue systems, when a parameter values goes out of range, its value is limited by the physical properties of the systems (such as the voltage limit on an amplifier). In a digital system, the value of the data is limited by the mathematical operations that are being performed. It is important to understand how a calculation responds to these input conditions and to ensure the operator understands how to interpret the information that is presented.

3.2.3.5. Human–machine interface

As digital I&C systems are being developed, it's important to consider how operators interact with the digital I&C system. Some of the key elements to consider include:

— The effects of new displays and resulting HMI interactions versus traditional machine control and operator intervention;
— The effects of new digital (computer-based) integrated systems (control rooms) on human performance;
— Availability of important data for operator use;
— Identification of operators' need for specific data points;
— Design of displays so that key data, warnings and alarms are apparent.

3.2.4. Manufacturing

Manufacturing encompasses a variety of processes and therefore can be the root cause for various sources of faults. These faults may be in equipment that is installed in multiple parts of the system. Some sources of faults are:

(1) Insufficient quality control, including tests on elementary components, intermediate control on subassemblies and final control;
(2) Changes in the component design or manufacturing process without sufficient information regarding the manufacturer engineering organization;
(3) Flawed manufacturing process. This could include assembly errors due to inappropriate configuration management.

3.2.5. Installation and commissioning

The installation and commissioning process can introduce latent faults into the I&C system. This can occur with both analogue and digital systems, but digital systems have a higher risk due to the more complex communication within the system.

Some examples of installation and commission issues include:

— Inadequate equipment identification;
— Failure to remove test equipment and wiring;
— Incorrect wiring;
— Wrong parameter settings (e.g. set points for smart sensors);
— Inadequate configuration management;
— Inadequate commissioning test.

3.2.6. Post-installation modifications

All the errors that have been discussed in the previous sections are also applicable to modifications. Since the preparation of the modification includes all of the design and installation phases, the same risks exist. Since the modification will be focused on the part of the system that is being changed, there is an added risk that an impact on a different part of the system could occur. This should be considered during the preparation of the modification. Some causes of error during the modification stage are:

— Inadequate configuration management;
— Unknown impacts of the change on other parts of the system;
— Incomplete testing (results in undetected interface, problems or undesired functional changes);
— Documentation that does not reflect the actual state of the plant.

3.2.7. Maintenance and operation

Maintenance of the I&C System introduces risks that are similar to those in the initial design, manufacturing and installation stages. Some of these risks could be greater in an analogue system because these systems typically use older technology, which does not include modern human interface and error detection technology. Examples of problems that could take place within the maintenance and operation process are:

— Maintenance of the wrong piece of equipment;
— Incorrect procedure or incorrect application of the procedure;
— Failing to remove maintenance equipment and wiring or otherwise return the I&C system back to normal operating conditions;
— Damage to the system/equipment;
— Installation of the wrong spare parts or spare parts with embedded software containing an incorrect version or release;
— Inadequate training of the maintenance staff;
— Use of tools that may introduce errors;
— Loss of configuration control.

3.3. TRIGGERING MECHANISMS

Triggering mechanisms are a necessary factor to activate a latent fault that causes the coincidental failure of some or all components concerned. Therefore, the avoidance of common triggering mechanisms is of equal importance as the avoidance of latent faults to minimize the potential for CCF.

3.3.1. Human actions

Experience with CCF in a variety of industries has shown that human actions are one of the most important triggers initiating latent faults. Human actions can place two or more channels or system elements into an unanalyzed/untested state in which the latent CCFs will be initiated. The following are the most common reasons for human failures that will trigger otherwise latent faults:

— Insufficient procedures for the execution of specific maintenance activities;
— Insufficient training or experience of maintenance personnel;
— Ambiguous design in the human-machine interface for systems involved; this may include test equipment, I&C cabinets and panels of units in the main control room.

A possible result of these deficiencies is that a procedure is performed incorrectly or applied to the wrong component or in the wrong element in a set of redundant modules.

A strong human–machine interface design programme can reduce the potential for triggering events initiated by human action. Considerations of features such as consistency of the interface and the prioritization of data will minimize the potential for incorrect action that could trigger a CCF.

3.3.2. Signal trajectory

Signal trajectory describes the combination of all factors that can influence the behaviour of the system. It includes the time history of inputs to the system from both instrumentation and human actions and the time history of the system states, including the state of hardware failures. Strongly variable signal trajectories may occur during safety demands and under superposition with system internal states from maintenance activities. These signal trajectories are the primary sources of stressors that may cause CCFs.

A digital failure of an operating I&C system that has passed the established system tests (including Factory Acceptance Testing, Site Acceptance Testing) and been commissioned will likely be triggered only by a signal trajectory untried in testing or during operation prior to the failure.

Such previously untested signal trajectories can be caused by a rare plant condition or by inconsistent input data. For example, data from a sensor or transducer fault or faulty data transmission between redundant units may represent "physically impossible" plant conditions. The triggering of CCFs may additionally be dependent on specific internal states of the I&C system.

Introduction of diversity in the signal trajectory between channels or other elements of the I&C system can minimize the potential for CCFs due to specific signal trajectories. For example, such diversity can be provided via procedures that prohibit modifying parameters in multiple channels or functional elements at the same time.

3.3.3. External events

There are possible triggering mechanisms caused by events external to the I&C system that may directly influence only the hardware of I&C systems. The most relevant events in this category to be considered during the design of the I&C systems are:

— Seismic events or strong vibrations from off-normal events;
— Extreme ambient conditions (high temperature, high humidity, freezing, etc.) in the rooms, cabinets or cable trays containing I&C equipment;
— Maintenance activities, such as welding, startup of pumps or engines;
— EMI and RFI interference, including
  • EMI by cordless phone or paging systems;
  • EMI by (future) wireless technique of sensors or other components;
— Flooding or fire in the rooms, cabinets or cable trays containing I&C equipment;
— Surges in the power supplies to I&C equipment.

3.3.4. Temporal effects

Specific calendar date or timing conditions can be triggering mechanisms. Relevant examples are:

— Special calendar dates that have not been handled properly in the software design (e.g. 29 February or switch-over between daylight saving and normal local time);
— Run-time overflow of the scheduled processing cycle;
— Synchronization between the processing units of one I&C system or synchronization of an I&C system to an external clock.

Latent errors do not have to be permanent to affect digital systems; transient conditions can also affect the behaviour of digital systems. The effects of transient off-normal conditions or errors, which might not clear before another off-normal or error condition is encountered, need to be avoided. This is particularly true if system restarts might be triggered by the off-normal conditions or errors.

In projects developed to update or replace I&C within an existing plant, it is necessary to consider potential implications of the ageing effects on electronics. This is particularly important when a hybrid system is being designed and elements of an analogue system will be retained and utilized.

Experience with NPP legacy I&C systems has found that significant degradation can occur. For example, there can be metal migration or "tin whiskers" on printed circuit boards. A full discussion of ageing for electronic systems is outside the scope of this document. There are major reports and papers that address the specific topics of cable ageing, sensor ageing as well as electronic I&C equipment. With growing interest in longer design life (now 60 years) and life extension (30–40 and 40–60 years), as well as the potential for "life beyond 60," adequate consideration should be given to I&C life cycle management, including sensors, actuators, cables, communication modules and data processing and display. For new plants, life cycle plans for computer and software replacement and upgrades should be addressed in the design specification.

3.4. PROPAGATION OF FAILURES BETWEEN I&C SYSTEMS

Many digital systems share resources, including power supplies, communication buses, protective measures such as watchdog timers, memory devices, etc. Failures can propagate through these shared resources, potentially leading to CCFs of the digital systems.

The failures in digital systems generally fall into one of three categories:

— No response is given on demand;
— An erroneous response is given, causing either a spurious response or an incorrect response;
— A system exception occurs, causing the system to stop.

How these failures are propagated through the system depends on the interrelationship between the elements of the digital system.

One important issue to consider for CCFs is the propagation of failures through the I&C systems. These failures could be propagated in different ways, such as:

— Propagation of faults between the redundant channels of I&C systems that are designed to meet the single failure criterion. The likelihood that failures propagate between the separate channels of a multi-channel I&C system depends on the design of the I&C systems and the features for separating the redundant channels in the system.
— Propagation of faults between I&C systems that are intended to be diverse. Particular care should be taken to ensure that the effects of shared resources are addressed such that the intended diversity is not compromised.
— Propagation of faults between I&C systems assigned to different protection barriers that are intended to perform their functions independently. As in the case for systems intended to be diverse, care should be given to ensure that the effects of shared resources are addressed. Some commonality between I&C systems in this case may be acceptable if the impact of faults is well understood.

3.4.1. Propagation of electrical effects

The propagation of failures based on electrical effects mainly concerns I&C systems where copper cables are used for signal exchange or data communication between the elements of the I&C systems. The physical phenomena involved in failure propagation are well understood, and measures for physical separation can be introduced according to specific design limits. Failure propagation by electrical effects may occur if a barrier against higher voltages fails in one redundant channel or unit (e.g. from the switch gear via coupling relays) and if the erroneously introduced voltage becomes higher than the design limit for a particular physical separation.

3.4.2. Propagation of logical failures

Measures to guard against the potential for propagation of logical failures are required in the design of computer-based I&C systems. The analysis of the possible paths for potential failure propagation may be difficult to determine. Therefore, the propagation paths through the system should be carefully evaluated in the development of the system. Propagation of logical failures may take many forms, including:

— Propagation of timing failures:
  The single failure of any processing unit within an I&C system with redundant elements may lead to consequential failure of the other redundant processing units within the same I&C system or even of other I&C systems if interdependencies exist. For example, at the start of the next processing cycle, the availability of specific input data that should have been sent from the first failed processing unit may be required. The single failure of a processing unit may cause the transfer of a required message to be performed too late, too early, in a repetitive manner or to be totally omitted.

If the timing conditions for the redundant processing units of an I&C system depend on the correct operation of a common system (e.g. a clock system), a single failure of this common system could potentially cause consequential timing failures of some or all redundant processing units.

— Communication failures or performance failures depending on the plant process:
Specific difficulties exist in predicting the time-dependent behaviour of a processor-based I&C system if the processing time for the application functions or the bus load (volume of transferred messages) depends on the plant process (e.g. in the case of a demand situation or if manual commands are required for accident management).

— Data failures: A received message may contain incorrect data. The faults in the data may be caused by:

— The originating sensor (transducer);
— The sending of distributed data conditioning (processing unit);
— The data communication transmission.

3.5. PROPAGATION OF FAILURES BY COMMON I&C SUBSYSTEMS

The operating conditions of nuclear power plants require the application of I&C subsystems, which perform their assigned functions for some or all processing units in a redundant I&C system or even for different I&C systems. Uses for such common subsystems include:

— To provide adequate information for operator displays in the main control room;
— To provide a way for the manual actuation of the components in the plant safety systems of the main control room so as to control the plant and bring it into the sub-critical cold status after the end of the automatic safety measures performed by the I&C systems;
— To ensure software maintenance by traceable procedures, which may include:
  • the adaptation of safety set-points during power operation that are dependent on operating conditions (e.g. during stretch-out operation to prolong a fuel cycle);
  • the implementation of software upgrades (application or system software) during outages;
— To support maintenance of the I&C system in the case of component failure, such as with the identification of faulty components or the tracing of faulty signals;
— To support the performance of recurring tests for those parts which are not included in the scope of self-supervision (e.g. sensors (transducers) for input signals or the actuation of the plant safety system components).

These subsystems need communication links to the processing units of all the redundant channels in the I&C systems that perform important safety functions.

4. ASSESSMENT OF SUSCEPTIBILITY TO CCFs

The approach to determine CCF susceptibility within the I&C architecture of a nuclear power plant is based on representation of the architecture in a suitable form for analysis, articulation of the relevant safety goals and associated I&C functions, knowledge of the credible CCF mechanisms and determination of dependencies and commonalities among multiple elements (e.g. systems, channels, modules, components) of the architecture. The conduct of such assessments involves several elements or steps, which include the following activities: decomposition of the I&C architecture, identification of CCF mechanisms (e.g. fault-trigger combinations) to be considered, determination of the impact of CCF occurrence in terms of relevant safety goals or design criteria and introduction of additional design and implementation measures to resolve potential CCF vulnerabilities (e.g. avoidance or mitigation).

The assessment of CCF susceptibility of the I&C architecture can occur at various life cycle phases of a nuclear power plant I&C system and can be performed by different organizations or entities. Examples include manufacturer evaluation of technologies and components for product line development, utility or supplier determination of CCF potential for specific system applications, utility analysis of CCF vulnerability mitigation within a plant I&C architecture or regulator acceptance evaluation of CCF mitigation strategies proposed for I&C system licensing review. The sequence and depth of analysis stages can vary depending on the development stage of the architecture, the architectural level (overall, system, channel, subsystem, module, or component) under consideration and the decision or confirmation goal to be achieved. Such assessments may be performed in an iterative process whereby very conservative assumptions are made at first, and the analysis is iterated with design changes or refined analytical assumptions.

4.1. DECOMPOSITION OF THE SYSTEM

To enable the assessment, a model or representation of the I&C architecture is necessary. The model decomposes the I&C architecture to the necessary granularity to support the depth of analysis appropriate at the current stage of architectural development. Architectural granularity, in this sense, means that the architecture can be decomposed at a high level, with individual blocks subdivided into lower levels of detail, such as system decompositions, module decompositions or lower. This choice among different levels of abstraction permits more focused assessment of particular susceptibilities associated with specific technical details. The intended analysis can be the driver for choosing different granularity in the decomposition of an architecture to allow consideration of specific CCF susceptibilities, such as at the interconnected system level, individual system level, subsystem level, module level or component level. For example, consideration of CCF potential related to common components used for different applications may require a more finely decomposed representation of the specific instances of that component than is required for a more general assessment of the overall architecture.

One method of performing an assessment of CCF susceptibility is to focus on the consequences of CCF occurrences while representing the plant I&C architecture from a top-down perspective. An alternate approach to CCF susceptibility assessment is to focus on the mechanisms of failure (latent faults triggered by specific conditions) while decomposing the plant I&C architecture from a bottom-up perspective. There are other means of decomposing the plant I&C architecture, and performing the desired assessment is possible. However, this report will discuss the two cited approaches to illustrate the process.

4.1.1. Consequence-focused top-down decomposition

The main criterion for defining blocks and decomposing the I&C architecture to support a top-down assessment is that failures within a block can be assumed to be confined to the block. In making this assessment, the mechanisms for propagation of component failures discussed in Section 3 should be considered.

Initially, very large blocks may be selected (e.g. the control system and the protection system). Such a coarse analysis might eliminate a number of CCFs so that subsequent models can provide additional detail only where needed. In at least one instance such a coarse analysis demonstrated sufficient diverse functionality between protection and control systems that further analysis was unnecessary.

Once blocks are established, the blocks that may be subject to CCFs should be identified. Blocks are subject to the same CCFs if:

— They may have the same systematic fault in common, and
— They may experience the same triggering mechanism.

Some methodologies make this determination by considering a set of defined diversity attributes. For example, NUREG/CR/6303 [5] identifies design diversity, equipment diversity, functional diversity, human diversity and software diversity as a useful set of attributes to consider. The existence of one or more of these diversity attributes between a pair of blocks may be basis for arguing that those blocks are not subject to the same CCF. Another similar approach would be to identify the systematic faults and triggering mechanisms that

are common to blocks as discussed in chapter 2 [5] and then to consider if defensive measures as described in chapter 4 [5] are sufficient to provide reasonable assurance that the faults of concern do not exist or that the common triggering mechanisms cannot cause failure. These two techniques are not mutually exclusive. The former might be used in an initial analysis to determine diversity between blocks without the need for extensive knowledge about the internal design of a block. The latter approach may then be used to refine the analysis in areas where the initial assumptions of CCF susceptibility are problematical.

Once the assumptions about the CCF susceptibility of blocks are known, CCFs are postulated, and the effect on safety functions is determined. For each set of blocks susceptible to the same CCF, the failure in the most adverse way should be postulated and the effect on plant safety functions (when they are needed to mitigate postulated accidents or transients) determined. A useful means for presenting the results of the analysis is by a matrix of systems or safety groups vs. design basis events indicating in each case the systems or safety groups that needed to respond to the event and that are vulnerable to CCFs and the other systems or safety groups that can respond to the event but are not vulnerable to the same CCF.

4.1.2. Mechanism focused bottom-up decomposition

Decomposition of the I&C architecture into a representation suitable for CCF susceptibility assessment using the bottom-up approach aims at the identification of the context: design, system, interfaces (e.g. physical interconnects, digital communication), equipment and component characteristics, system hardware and software specifications, as well as operational procedures. Several views of the decomposition may be needed to support the evaluation. Examples of decomposition are as follows:

— Decomposition according to safety levels;
— Decomposition according to the hardware structure, software structure and the interfaces between them;
— Decomposition according to safety functions;
— Decomposition according to the logical components and their interaction;
— Decomposition according to fault containment zones.

Representation of the I&C architecture as a collection of elements through aggregation or decomposition of components, modules and/or systems results in formulations that are suitable for analysis. These elements or aggregations are termed as blocks for the architectural decomposition performed in some assessment approaches.

Decomposing the I&C system architecture based on physical components does not necessarily account for functional assignment/responsibilities and dependencies. Functional/logical diagrams do not necessarily identify physical boundaries, groupings and interconnections. An abstract representation of the I&C system(s) and their interconnections is needed to enable partitioning/grouping into functional units whose concurrent failure is significant while maintaining information about the logical and physical characteristics associated with those elements and the interconnections that may exist among them.

All of these representations have the capability to identify blocks (e.g. systems, aggregation of functional units). The identification of the blocks can be performed at different levels of abstraction (e.g. architectural granularity) and may be tailored according to the type of CCF mechanism and differences in operational conditions or system configurations that are being considered. The level of abstraction and grouping of functional units into a block structure must be suitable for the life cycle phase of the I&C architecture and the intended technical depth of analysis (e.g. high-level, consequence-driven analysis, detailed technology-driven analysis). Additionally, iterations of the assessment may require refinement of the architecture decomposition to permit more detailed consideration of unresolved CCF susceptibilities.

The decomposition of the overall I&C architecture should consider the:

— Defence in depth principles;
— The redundancy in the different levels of defence;
— The diversity principles;
— Interconnections such as digital communication systems.

An example of an architectural decomposition from the physical perspective is given in Fig. 5. This decomposition of a generic four-channel programmable logic controller (PLC)-based safety system takes into account the four redundancies R_1 to R_4. These redundancies are spatially separated and isolated by barriers (e.g. walls, cabinet boundaries). In each redundancy, two PLC modules are provided that are logically separated. The PLCs, denoted as PLC_{AX} and PLC_{BX}, can be combined throughout the redundancies to form the subsystems or groups A and B. The system may have the set I of input values, which typically are diverse. The decomposition can be refined if needed.

A functional perspective for decomposition of an I&C architecture will be different. An example is given in Fig. 6. This decomposition can be based on the relevant safety goals (e.g. reactivity control, residual heat removal) and the design basis events that pose challenges to satisfying the safety goals. The necessary mitigating functions (MF) can be identified and their relation to safety goals (SGs) and design basis events (DBEs) established. Fig. 7 presents an international approach to defining DBEs.

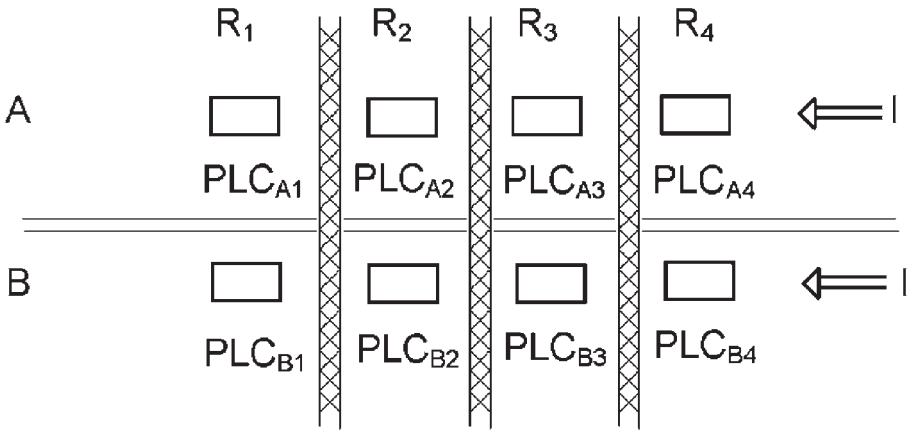


FIG. 5. Physical decomposition.

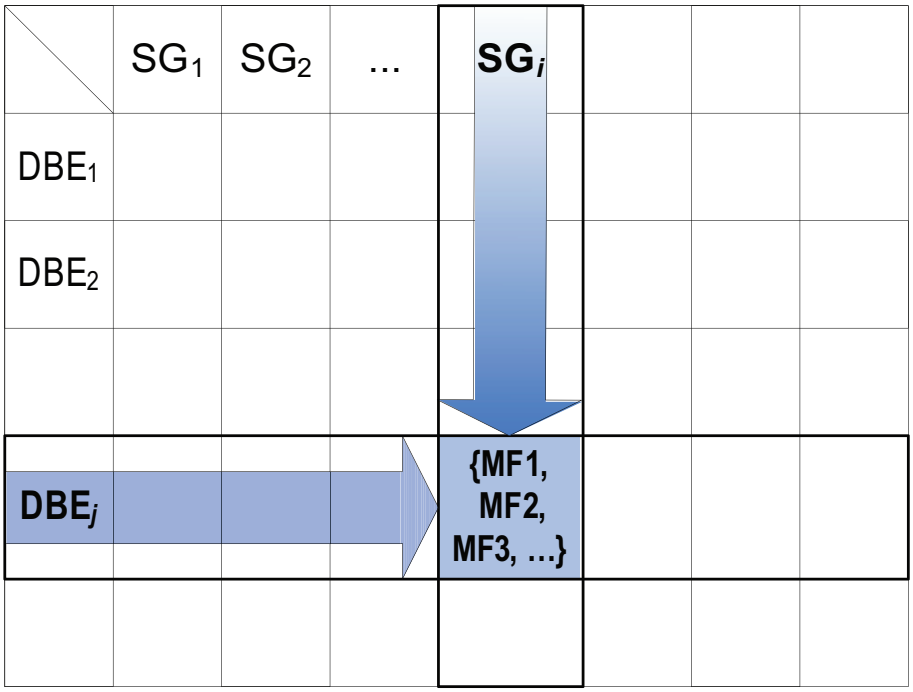


FIG. 6. Functional decomposition.

<table>
<tr><td colspan="2">Operational states</td><td colspan="3">Accident conditions</td></tr>
<tr><td></td><td colspan="2">Design basis events</td><td colspan="2" rowspan="2">Beyond design basis accidents</td></tr>
<tr><td rowspan="2">Normal operation</td><td rowspan="2">Anticipated operational occurrences</td><td rowspan="2">a)</td><td rowspan="2">Design basis accidents</td></tr>
<tr><td>b)</td><td>Severe accidents</td></tr>
<tr><td></td><td></td><td colspan="2"></td><td colspan="2">Accident management</td></tr>
<tr><td colspan="5">a) Accident conditions which are not explicitly considered design basis accidents but which are encompassed by them.
b) Beyond design basis accidents without significant core degradation.</td></tr>
</table>

FIG. 7. Design basis events [9].

After the I&C architecture has been decomposed, the characteristics of each block and its possible interactions must be understood. These characteristics can be used to identify vulnerabilities by finding prospective faults/trigger combinations.

Typical characteristics that can be associated with blocks include:

— Safety classification;
— Reliability data;
— Functions (macro; micro);
— Quality (V&V, status of qualification);
— Physical HW components (equipment type, product, key constituent elements, version identification);
— SW components/modules (system SW, application software, version identification);
— Pre-developed components;
— Internal structure/architecture;
— Internal communications/data management;
— Time characteristics (real time behaviour, date and clock functions, synchronization);
— Interconnections with external systems (inputs and outputs; functional or physical);
— Operational conditions;
— Self-supervision capabilities;
— Failure behaviour;
— Changeable elements/components (e.g. configuration data);
— Maintainability.

Typical interaction characteristics between the blocks are:

— Shared components;
— Data communication (e.g. data communication between parallel blocks, data communication between blocks in a chain);
— Shared data;
— Shared auxiliary systems (power supply, air conditioning, etc.).

After the characteristics have been identified, the analysis for potential common faults and triggers can be performed in the context of the I&C architecture.

4.2. IDENTIFICATION OF THE POTENTIAL FOR CCFs

Given a representation of the I&C architecture based on the decomposition principles discussed above, the screening of potential CCFs can occur in an informed context. The basic goal is to determine which blocks may be subject to which potential faults and which potential triggers, and whether fault-trigger combinations

that lead to potential CCFs are present for each instance. The possibility of a fault or trigger for a particular block depends on whether defensive design measures, including available diversity, have been included in functional units incorporated within the block. Based on understanding of the fault-trigger combinations that lead to credible potential failures, it can be determined which blocks may be subject to the same potential failure. As a result, potential CCFs can be identified.

To execute this stage of the assessment, each block is examined to determine fault types. The potential failures to be considered can be derived from detailed fault analyses of the functional units through integrated architecture, considering the sources of CCF identified in Section 3 (e.g. analyses such as failure modes and effects analysis (FMEA), fault tree analysis (FTA), hazard analysis, risk analysis and so forth). The fault types must be very specifically defined in order that commonalities and communication interdependencies may be identified. For example, it is not sufficient to identify manufacturing as a potential fault; the characteristics (e.g. manufactured to a specific procedure) of the manufacturing that may cause the fault to be common with other blocks should be identified.

After the list of faults has been created for each block, the triggering events should be identified with respect to their effect on the blocks and their boundaries. The information contained in Section 3 on triggering conditions may be used as a starting point for this stage of the analysis.

Again, the triggering conditions must be described very specifically so that common trigger mechanisms may be recognized. Also, the specific fault types that may be triggered by a specific mechanism must be understood.

Given the definition of the faults and triggering conditions, a fault-trigger matrix (see Fig. 8) can be developed to identify potential failure mechanisms that should be considered in the assessment. Essentially, the matrix captures the fault-trigger combinations that represent potential failures that can result in CCFs.

It is recognized that it is not currently possible to prove that all potential faults and triggers are identified up front. It is frequently the unanticipated states or interrelationships and unpredictable uncertainties and misinterpretations that are the source or activating condition that result in failures. The goal is to be systematic and thorough while providing assurance that credible failures, which can be reasonably anticipated, are adequately addressed.

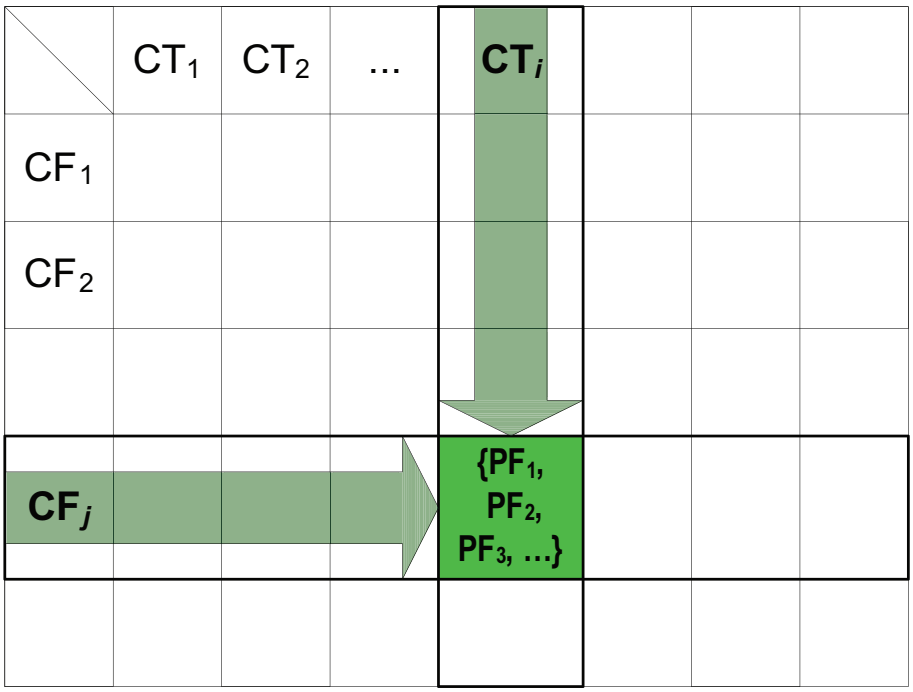


FIG. 8. Fault-trigger matrix.

Blocks subject to a common fault mechanism (i.e. the same fault-trigger combination is present) have the potential for CCF susceptibility. The I&C system representation is then used to identify the functions that are affected by each pair of faults and triggering conditions. This analysis involves systematically parsing through each credible combination of fault and triggering condition for each block and determining whether any design measures or diversities (see Section 5) are present that would preclude the occurrence of either. If no such measures are provided, then the block is subject to the corresponding potential failure (PF). These may be documented in a table, such as given in Fig. 9, which shows the functions that are affected by each identified potential failure. This table can be used to determine not only CCF susceptibility but also whether lines of defence are independent in terms of the CCF in question.

4.3. ASSESSMENT OF CCF IMPACT ON PLANT EVENT MITIGATION

The assessment should answer the question of whether a single trigger can affect mitigating functions to a sufficient degree to degrade the level of defence below an acceptable level. Thus, it is necessary to understand how the different credible CCFs affect the plant (e.g. blocking or delay of mitigating functions, unintended change of other functions and unintended activation of safety systems).

As captured in the matrix in Fig. 8, identify all potential failures associated with each credible fault-trigger combination. For each potential failure, identify all blocks affected by the corresponding set of fault-trigger combinations (see Fig. 9). For each set of blocks identified, ensure that they do not defeat the ability of the plant to perform its function based on the I&C architecture decomposition. This can be accomplished by combining the information about common failures outlined in the table of Fig. 9 with the matrix of events, safety goals and mitigating functions given in Fig. 6. The result can be captured in tabular form as shown in Fig. 10.

The result of this assessment is a determination of whether any CCFs are credible and whether any compensating block (e.g. line of defence) is unaffected in the case of each CCF.

If the assessment shows that the remaining mitigating functions are sufficient to maintain the consequences within stated acceptance criteria, the assessment has successfully demonstrated that the design has sufficiently dealt with the susceptibility to CCFs.

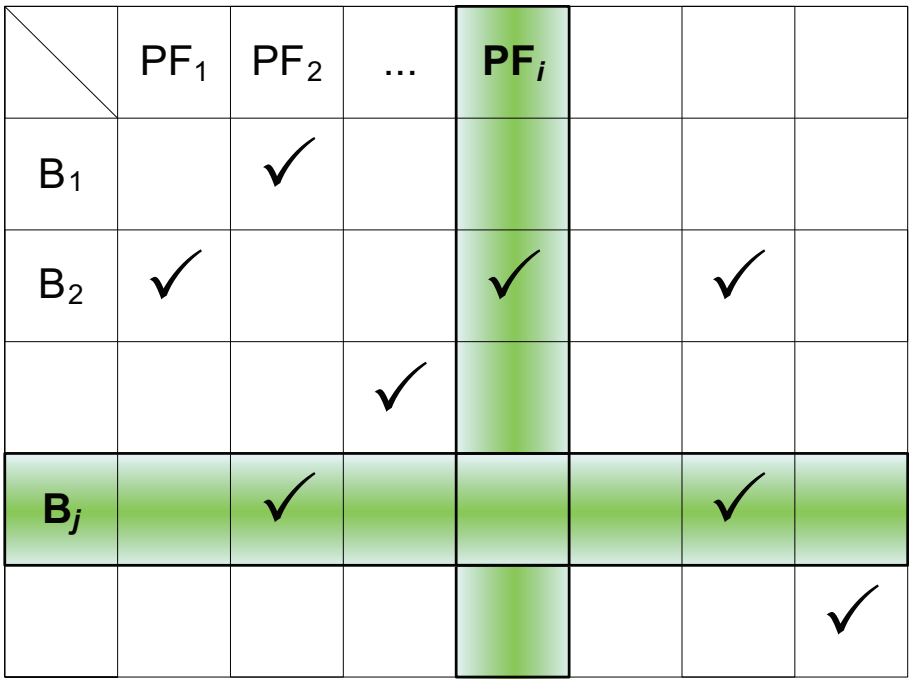


FIG. 9. Mapping of postulated failures to blocks.

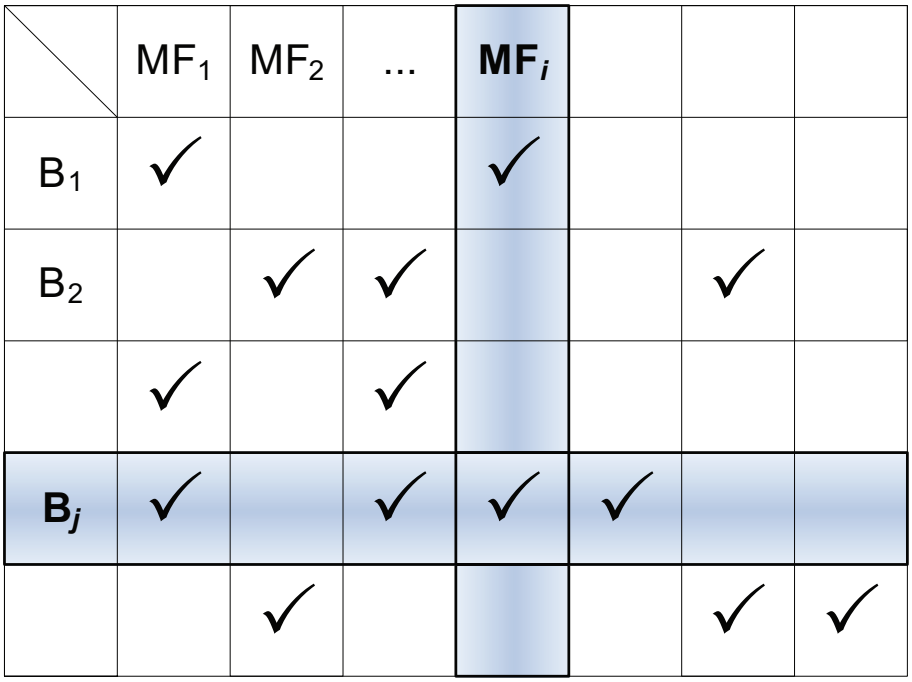


FIG. 10. Mapping of mitigating functions to blocks.

If this conclusion cannot be reached, there are a number of alternatives available. For example:

— Refine the decomposition of the I&C architecture (e.g. focus on specific architectural elements and/or increase the level of detail in the representation using a finer granularity);
— Further investigate the defensive design measures against CCFs in the blocks of concern to better understand the credibility of the assumed CCFs;
— Provide additional design measures within the blocks of concern to eliminate or reduce the commonality of systematic faults or the commonality of triggering conditions;
— Provide additional diversity within the I&C system architecture.

It may also be an option to justify acceptance of a CCF mechanism based upon its low safety significance. In this case, risk insights from PSA may prove invaluable.

Section 5 further discusses the rationale for making decisions about how to address identified CCF vulnerabilities.

4.4. USE OF COMMON SOFTWARE MODULES

The following subsections offer brief descriptions of how the question of CCF susceptibility might be addressed for typical digital components for which the use of common software modules is the primary concern. The evaluations are based on critical reviews of the designs, supplier processes and documentation and operating history to assess the effectiveness and coverage of the defensive measures that are in place and whether there is reasonable assurance that CCF likelihood is low enough to exclude the component from further consideration. Component complexity is a key consideration, including its impact on effectiveness of factors such as testability and operating experience.

4.4.1. ‘Smart’ transmitter

Identical ‘smart’ transmitters are used to monitor pressure in redundant divisions of multiple safety and critical-to-operation non-safety systems. They are widely used, commercially available devices that have been evaluated and qualified for use in nuclear safety applications using the applicable regulatory guidance. In the plant implementations, they do not share common resources or communications networks, so potential CCF susceptibilities of interest involve only identical components and global stressing conditions. Software errors and designed-in susceptibilities to selected global stressors are the fault types of interest. The defensive measures list in Table 3 is used as a starting point for the evaluation.

The evaluation shows that the device has important simplicity attributes (e.g. single function, fixed number of inputs and outputs, few configuration parameters, highly testable, software architecture with no branching and minimal interrupts, etc.). The configuration procedure uses a proven software tool that includes human factor features designed to reduce the likelihood of configuration errors. The software does not include date or time tracking features that might introduce susceptibilities to global stressors. It is not practical to perform 100% testing, but various self-testing and diagnostics features are included, and data validation routines are used to check output values before they are used by the downstream control devices. Because it is based on a commercial device, there is extensive, successful experience in operation, and the software has been stable for many years, as evidenced by the vendor records of problem reports and configuration management. Also, because the device has only one function, all the operating experience is relevant to the nuclear plant applications.

Engineering judgment, based on the preponderance of the evidence, is that there is reasonable assurance that this smart device is not a likely source of CCF and need not be considered further in CCF evaluation. If this device had been shown to be 100% testable, that, along with documentation of the testing might have provided sufficient assurance by itself that it is not a credible source of digital CCF.

4.4.2. Programmable controller

Identical, programmable platforms are planned for use in redundant divisions of safety systems as well as critical-to-protection, non-safety systems. The software elements include the operating system (OS) and function block modules, which are the same in every device and application code and which provide the application-specific instructions and sequence calls to the function block modules for specific calculations and operations. The CCF evaluation indicates that diverse backups for some of these platforms may be needed to conform to regulatory guidance; therefore an evaluation is performed to determine which of the software components are credible sources of digital CCF.

4.4.3. Operating system

Again the failure mechanisms are those that involve common software faults and vulnerabilities to global stressors. A review of the platform, starting with the defensive measures list in Table 2, reveals that the operating system is used in a deterministic fashion that restricts software trajectory, facilitates testing and guarantees adequate response times. The operating system executes the same sequence of instructions regardless of plant operating mode or data input values; there are no process-driven interrupts. The OS is effectively “blind” to plant transients. This ensures that residual faults in the operating system software, though likely to exist, are extremely unlikely to be activated by plant transients. Further, susceptibilities to global stressors have been systematically eliminated by avoiding use of features that might create such vulnerabilities (e.g. there is no management of time and date; there are minimal interrupts, etc.). Note that diverse operating systems would be susceptible to CCFs if they shared vulnerabilities to the same global stressors. The OS version has been stable and has extensive successful experience in operation. Based on the preponderance of the evidence, the OS is judged not to be a likely source of digital CCFs and may be used in a diverse backup system.

4.4.4. Function block modules

The function block modules execute standard elementary functions such as mathematical functions. Assurance of adequate detection and elimination of design faults is based on their low complexity (elementary functions are usually independent from one another, use little or no memory and few parameters, and are based on well-understood and proven algorithms), stability (they are rarely modified) and extensive experience in operation. In this case, review of the platform confirms that all the function block modules are simple, stable and mature, with extensive operating history. They are therefore judged not to be likely sources of digital CCF and are considered allowable for use in diverse backup systems for CCF purposes.

4.4.5. Application code

For application specific or configuration software, some design faults may be avoided or made less likely using devices such as data validation routines that flag out-of-range input data values, trusted code generation tools that simplify programming, and deterministic programming techniques (the next steps and their timing can be predicted depending only on the current state) that facilitate testing and guarantee adequate response times (Table 2). However, the application code is where the functional requirements are communicated to the control system and is therefore also susceptible to specification faults.

Evaluation of the application code, including its development process and documentation, reveals that the requirements specification was subjected to systematic reviews to address concerns of correctness, completeness and ambiguity (Table 1). Further, applicable defensive measures from Table 2 have been incorporated in the design, and test coverage is close to 100%. While the application code is relatively simple compared to most control system algorithms, it is not trivial. Also, as it was custom developed for the nuclear plant application, it has little experience in operation. Because of the potential for undetected specification errors and the limited operating experience, it is judged that the application code should not be eliminated as a potential CCF source. This conclusion would remain the same even if diverse hardware platforms were proposed for redundant trains with identical functionality, as the potential for CCFs originating in specification errors would be unchanged.

5. I&C DESIGN MEASURES AGAINST CCF

5.1. PRINCIPLES

Prevention of CCFs in nuclear I&C systems starts at the top level of the whole I&C architecture. According to the defence in depth design principle, different lines of defence provide protection against initiating events by preventing, terminating and mitigating the effects of those events. Within a line of defence, multiple functions may be provided to detect those events and take appropriate actions according to different (diverse) principles of operation. These functionally diverse features are implemented in independent I&C systems that are ensured by rigorous design and operating practices so as not to share common faults or common fault activation triggers. Within any one system performing functions important to safety, CCF of redundant portions of the system is prevented by avoiding or removing faults, by providing tolerance of faults that remain and by preventing propagation of the effects of faults between those redundant portions.

5.1.1. Minimizing faults in structures, systems and components

Two main approaches are used to minimize the number of faults in SSCs: fault voidance, fault detection and removal.

5.1.1.1. Fault avoidance

Fault avoidance or prevention approaches are employed during design and development to reduce the number of faults introduced during this phase of the system life cycle. These avoidance or prevention approaches should address the different potential sources of faults listed in Section 3.2.

The main fault avoidance principles are:

— Avoidance of unnecessary complexity in functional specification, in system/software design and in selected off-the-shelf components and platforms;
— Application of well defined development processes with defined activities, well-specified deliverables and documentation, and clear attribution of responsibilities;
— Use of appropriate methods and tools. For example, the use of high-level, application-oriented specification and/or design languages with unambiguous syntax and semantics, and supported by reliable simulation, verification and translation tools is usually a very effective means for fault avoidance;
— Use of competent, knowledgeable personnel, having sufficient resources, equipment and time;
— Application of suitable rules and guidelines for each activity of the development process, providing reasonable defence against faults and CCFs. The rest of this section gives examples of guidelines applicable to various development activities;
— Use of dependable and well understood components and platforms. Components may be software components, hardware components or equipment integrating hardware and software. It is to be noted that even dependable, proven components may be misused (due to insufficient understanding of their capabilities, interfaces, needs and/or limits);
— Taking into consideration lessons learned from past mistakes and faults in similar systems in order to improve development processes, methods and tools, rules and guidelines, as well as training.

Guidelines for functional specifications

Experience has shown that the requirements specification for the functions to be performed by the I&C systems is a significant contributor to CCFs of the channels in a redundant system. Two main types of mistakes may lead to faults in the functional specification for the application of a digital system:

— Functional mistakes arise when incorrect understanding of the desired behaviour of the digital system or of the behaviours of other plant systems or components is reflected in the functional specification. Such mistakes are usually not specific to digital systems and have been found in the functional specifications of analogue systems.
— Technical mistakes arise when the desired behaviours and functionality of the digital system are inaccurately or incompletely translated into the functional specification. Such mistakes result from various causes, including use of inappropriate functional specification methods and tools or from insufficient or incorrect understanding of these methods and tools.

Table 1, reproduced from EPRI TR 1002835 [4], lists a set of defensive measures that are often useful against specification faults and resulting CCFs. This table is not intended to be all-inclusive or to be used as a check list of adequate defensive measures because the appropriate set of defensive measures for an actual system is likely to be application-specific and may involve detailed measures not listed here.

Guidelines for programmable equipment

With an appropriate set of measures, design faults are very unlikely to be a dominant cause of failure and CCFs, even when different SSCs contain identical software modules. Table 2, also reproduced from EPRI TR 1002835 [4], provides an example of a set of measures that would be appropriate for programmable equipment. It relies heavily on designed-in features that are particularly effective against failures triggered by unanticipated operating conditions. These features are often recommended for high-quality programmable equipment.

TABLE 1. EXAMPLES OF MEASURES FOR FUNCTIONAL SPECIFICATIONS

Defensive measures	Benefits
Functional specification focused on what is strictly necessary for safety and for the operation of the digital system. Static and rigorous determination of all the entities interacting with the digital system, and of their different states. Functional specification addressing all resulting operational conditions. Simplicity of interfaces and interactions. Identification and examination of the differences with the I&C system to be replaced or with similar I&C systems that have proven to be adequate.	Avoid functional mistakes, including: • Oversight of some of the operational conditions that may face the digital system; • Incorrect characterization of anticipated operational conditions; • Incorrect characterization of interfaces and interactions; • Specification of inappropriate behaviour for some operational conditions; • Failure to specify actions and operational concerns for faults and failures; • Failure to extend an existing system's logic into all operating conditions.
Functional specification languages, elementary functions and tools with clearly defined and simple syntax and semantics. Specification methods and tools well adapted to application domain, allowing simple functional specification. Specification methods and tools that can help avoid or detect incompleteness and intrinsically unsound expressions (e.g. expressions that could lead to divisions by zero). Functional specification process guaranteeing that relevant functional studies are taken into account correctly. Functional specification process providing clear guidance regarding effects of digitization.	Avoid technical mistakes, for example: • Incompleteness; • Ambiguousness; • Insufficient accuracy; • Oversight of possible effects of digitization; • Oversight of possible adverse side-effects; • Intrinsically unsound expressions; • Incorrect translation of results of functional studies into functional specification.
Systematic verification of correctness and completeness of functional specification versus plant functional and safety requirements.	Reveals and removes existing functional specification faults.
Existence of an unequivocal and easy-to-reach safe failure position. Boolean safety outputs with clearly identified failure modes and unsafe failure modes. Plant operating conditions ensuring that potentially unsafe failures can occur only in particular situations (e.g. only during plant transients). Verification of functional specification particularly focused on potentially unsafe outputs. Specification of the conditions that should be satisfied by inputs (pre-conditions), and of conditions that must be satisfied by outputs (post-conditions).	Reduce the likelihood of potentially unsafe failures.

Guidelines for smart devices with simple, fixed functionality

Table 3, also reproduced from EPRI TR 1002835 [4], lists a set of measures that are particularly appropriate for simple devices. It includes process-related measures, designed-in features and measures that can be applied by the user of the device to limit susceptibilities. While the measures listed in Table 2 are generally for more complex devices, they may also be useful in simple devices.

TABLE 2. EXAMPLES OF DESIGN FEATURES FOR PROGRAMMABLE EQUIPMENT

Defensive measures	Benefits
Rigorous development and modification processes. Focus on safety, avoidance of non-required components and capabilities. No generic susceptibilities (e.g. no management of time and date). Static allocation of resources.	Low level of residual digital design faults.
Deterministic behaviour. Invariability of software during operation. Validation of inputs prior to further processing. Clearly identified short-term memory. Interrupts only for exceptions and clock.	Rigorous identification and characterization of factors that can influence the functioning of software.
Cyclic functioning. Single-tasking. Limited amount of short-term memory.	Among all these factors, only infrequent events are susceptible to cause digital failures.
Non-software watchdogs (failure of the digital system or channel to periodically reset a watchdog results in a specified safe action within a specified time frame). Surveillance of short and long-term memory. Defensive programming.	Software deviations and failures are detected and lead rapidly to a safe position.
Rigorous operational procedures for operator requests (one channel at a time, only when absolutely necessary).	Service requests prevented from causing digital CCFs.
"Dissociation" of operating system from application software. Transparency of operating system to plant transients.	Operating system prevented by design from causing potentially unsafe digital CCFs triggered by plant transients.
Further decomposition of operating system into dissociated modules.	Reduction of the likelihood of design faults in the operating system.
Application Function Library composed of dissociated, simple, stateless, well-proven modules.	Application Function Library very unlikely to contain design faults that could lead to digital failures.

5.1.1.2. Fault removal

Fault removal techniques are dependability-enhancing techniques employed during system/software development, mainly in verification and validation (V&V) activities. Three main categories of techniques may be used: testing, formal inspection and formal design proofs. Their effectiveness is usually significantly enhanced when they are performed by independent personnel.

Testing

The most common fault removal technique involves testing. The difficulties encountered in testing digital systems and software are often related to the prohibitive cost and complexity of exhaustive testing, as this requires testing under all circumstances using all possible input sets. The key to efficient testing is to define an appropriate test strategy (from component testing, to the final testing of the integrated system in its final environment, through integration testing and validation testing against specified requirements), to achieve adequate test coverage, to use suitable support tools, and to derive appropriate test quality measures.

TABLE 3. EXAMPLES OF MEASURES FOR SMART DEVICES WITH SIMPLE FIXED FUNCTIONALITY

Defensive measures	Benefits
Application of documented and rigorous configuration management programme. Track record for control of changes and versions, and notification of changes (especially software fixes).	Precise identification of the item, assuring that items with the same identification are identical.
Complete and unambiguous documentation. Accurate documentation consistent with actual design.	Characterization of the item, stating, in particular, what it does, how well it does it, what is guaranteed that it will not do, how it can fail, how it should be used and what it needs for correct operation.
Adequacy to support needed functionality. Unneeded/unused capabilities shown to have no adverse impact on required functionality.	Fitness to purpose.
Rigorous development, manufacturing and modification processes. Functional and technical simplicity. Sufficient amount of credible, relevant and successful operating history. Testing in expected operational conditions.	Low level of residual digital design faults.
Error handling capabilities, built-in protective features, ability to handle expected and unforeseen errors, and abnormal conditions and events.	Robustness, fault-tolerance.
Technical assurance that the device is used in narrow operational conditions, consistent with the bounds of its qualification. External surveillance by other portions of the I&C system, which increases the likelihood that failures or drifts are rapidly detected.	Safe use of the device.

Minimizing component and system size, and interrelationships maximizes accurate testing. Particular attention may be given to components identified as critical to the system.

Formal inspection

Formal inspection is another practical fault removal technique that has been implemented in some industries and that has shown success in many companies. This technique is a rigorous process, accompanied by documentation that focuses on examining design and software code to find faults, correcting the faults, and then verifying the corrections. Formal inspection is usually performed by small peer groups prior to the testing phase of the life cycle.

Formal design proofs

Formal design proofs are closely related to formal methods. This emerging technique attempts to achieve mathematical proof of correctness for designs and software. Using executable specifications, test cases can be automatically generated to improve the software verification process. This technique is not currently fully developed and, as with formal methods, may be a costly and complex technique to use.

5.1.2. Avoiding common faults

Despite the measures taken to eliminate faults from I&C designs (quality aspects), it is still postulated that there remain residual faults. For systems that are supposedly independent from one another, it is important to ensure that common faults do not exist or are not triggered at the same time. Diversity is the principle means of achieving this.

Although literature introduced many system diversity attributes, this paper considers three types of system diversity that subsume them all:

(1) Human diversity;
(2) Functional diversity;
(3) Design diversity.

5.1.2.1. Human diversity

Human diversity is the employment of several people with different backgrounds, affiliations, experience, etc. (but all of them being above a certain level of required expertise) to solve either the same problem or separate instances of the same problem independently. Examples are the employment of independent designers to design separate, functionally diverse parts of safety systems, and independent V&V personnel to verify and validate the deliverable of designers, etc.

Factors contributing to human diversity:

— Different (specification/design/development/integration/installation/maintenance) organizations;
— Different management teams in the same organization;
— Different execution personnel (designer/engineer/programmer/maintainer);
— Different evaluation personnel (tester/V&V/certifier).

5.1.2.2. Functional diversity

Two systems are functionally diverse if they perform different physical functions though they may have overlapping safety effects. Functional diversity may include signal diversity, which is the use of different sensed phenomena or parameters to detect an abnormal condition (of the process or equipment) in order to activate a fault tolerance mechanism or to initiate a protective action.

For example, cooling systems normally intended to function when containment is isolated are functionally different from other liquid control systems intended to inject coolant or borated water for other reasons. However, the other liquid control systems may have a useful cooling effect, while the isolation cooling systems may have useful coolant makeup side effects.

Functional diversity is often useful when determining if sufficient mitigation means have been employed in a postulated accident; a combination of alternative systems in the face of primary system failure may be enough to mitigate the effects of an accident.

Factors contributing to functional diversity:

— Different underlying mechanism (e.g. rod insertion versus boron poisoning);
— Different purpose, function (control rod vs. reactor trip rod), control logic or actuation;
— Different response time scale;
— Different process parameters sensed by different physical phenomena;
— Different process parameters sensed by the same physical phenomena;
— The same process parameters sensed by a different set of sensors.

5.1.2.3. Design diversity

Design diversity is the use of different solutions to solve the same problem or the separate instances of the same problem. The rationale of design diversity is that the different, independent solutions obtained through

design diversity are expected to have different faults and different failure modes, thus reducing the potential for a CCF. Nevertheless, there is a certain level of commonality in every set of independent design processes due to similarities of human factors (education, experience, practice, etc.) that weakens the effectiveness of design diversity.

Factors contributing to design diversity:

— Different technologies (that give comparable results; may add disadvantageous complexity);
— Different approaches/methodologies (even within the same technology);
— Different platforms (may add disadvantageous complexity);
— Different architecture (structure and interconnection of components);
— Different algorithms;
— Different data and execution structure;
— Different timing;
— Different manufacturers that produce equipment of fundamentally different designs;
— Same manufacturer of fundamentally different designs;
— Different manufacturers of similar designs.

With regard to the diversity of software, experience indicates that independence of failure modes may not be achieved if multiple versions of software are developed to the same software requirements specification. In particular, it is possible that independently developed versions of programmes may have common faults.

With regard to the diversity of hardware, the use of equipment from different vendors may not be sufficient. For example, different vendors may use the same electronic components. A detailed analysis is usually necessary to determine the degree of diversity of equipment from different vendors.

5.1.2.4. Combining diversity types

A single type of diversity helps, but usually does not guarantee, to avoid CCFs. Incorporating several types of diversity may be most effective in dealing with this limitation. However, it is important to note that:

— Human diversity by itself does not add complexity to the I&C architecture and I&C systems;
— Functional diversity is essentially determined by the overall design of the plant systems;
— Design diversity may increase the complexity of the I&C architecture and/or the I&C system, and thus the risk of spurious actuations.

5.1.3. Avoiding concurrent activation

Even in the presence of common faults in independent functional units, CCFs can be avoided if those faults are not activated concurrently. To this end, besides the minimization of common faults as discussed in the preceding section, two main complementary approaches may be used:

— Avoidance of fault activation;
— Avoidance of concurrent fault activation.

5.1.3.1. Avoidance of fault activation

Specific design measures may be taken to minimize the likelihood of activating a postulated residual fault in an SSC. For example, measures may be taken to restrict the variability of possible signal trajectories, ensuring that the SSC operates in a narrow set of operating conditions and that it not likely to encounter unexpected and untried conditions.

To this end, it is usually worthwhile to identify and characterize the factors that can influence the functioning and the outputs of an SSC (e.g. equipment conditions, internal states, input signals and operator inputs) and that collectively constitute the signal trajectories. Specific design measures targeting each of these influence factors may then be taken. For example, measures may be taken to restrict the number and range of

input signals and operator inputs, and to limit the number of internal states. Also, cyclic operation with fixed execution sequences and sufficient timing margins, and static allocation of resources (e.g. memory) usually limit the likelihood of unexpected situations and fault activation.

5.1.3.2. Avoidance of concurrent fault activations

The risk of concurrent activation of the same fault in multiple SSCs may be reduced by diversifying operating conditions, which limits the likelihood of common signal trajectories. For example, different SSCs may be started at different times, so that any failure triggered by elapsed time would affect only one SSC at a time. In the same way, different SSCs may be maintained, modified or reset at different times, so that failures triggered by maintenance routines are less likely to occur concurrently.

To identify an effective set of the operational diversity measures, it is usually worthwhile to identify the influence factors common to multiple SSCs, such as operator inputs. Measures may then be taken to ensure that the common influence factors are diverse and/or occur at different times.

Influence factors may also be identified at the level of components, and measures may be taken to ensure that components that are identical across multiple SSCs are not affected by common influence factors. For example, operating systems not influenced by plant conditions are also not likely to cause concurrent failures during plant transient and demand conditions.

Also, it is usually worthwhile to systematically identify the stress factors that could concurrently and adversely affect multiple SSCs. Besides stresses arising from data communication, two typical common stressors are special dates and times, and environmental stresses.

I&C systems performing safety functions can be designed so their operational behaviour is free of unintended dependencies from any environmental information such as specific calendar dates.

Ensuring sufficient robustness of I&C systems performing functions important to safety is essential. All known failure mechanisms caused by environmental effects jeopardize the hardware components of I&C systems. To handle CCFs, there is no need for additional requirements to those of established standards. Therefore, this group of failure mechanisms is mentioned only from the viewpoint of completeness.

5.1.4. Avoidance of failure propagation

The design of I&C systems performing safety functions must ensure protection against propagation of failure from one SSC to another. Failures may propagate through electrical effects and transmission of logical failures. Design measures to avoid propagation of logical failures may be taken at various levels:

— At the level of the overall I&C and data communication architecture;
— At the level of data communication subsystem(s);
— At the level of communicating SSCs.

5.1.4.1. Avoiding propagation of electrical effects

Proven measures for the protection against the propagation of electrical effects are:

— Spatial separation equipment and cables;
— Avoidance of common subsystems, especially of common power supply systems;
— Magnetic isolation amplifiers for analogue signals;
— Optic couplers for binary signals.

The use of optical fibre cables for communication between redundant trains is the most effective measure against electric effects, however this is applicable mainly for digital I&C systems.

5.1.4.2. Design measures for the overall I&C and data communication architecture

Hereafter are measures that may be considered regarding the overall I&C and data communication architectures:

— Absence of data communication link: this is the radical measure to prevent propagation of logical failures between two SSCs.
— Separated data communication links and networks: this may be used to prevent propagation of logical failures between parts of the I&C architecture. The separation often reflects the overall redundancy, separation and diversity in plant design.
— Diverse data communication subsystems and/or data communication patterns: this may be used to avoid common faults and/or concurrent triggers in data communication subsystems.
— Redundant data communication links and networks: this allows communicating SSCs to detect and tolerate the loss or failure of a link.
— Asynchronous operation of SSCs: loose time coupling between communicating SSCs may be used against propagation of timing failure. Each SSC may operate at its own timing, not depending on any common clock and without synchronizing with other SSCs. Lost messages may be tolerated up to a specified level. Erroneous multiple transmissions may be ignored.
— In the particular case of common subsystems that can download modifications to SSCs performing I&C functions, data communications may be designed so that at any time, communication is limited to a single SSC. To activate the communication, a specific release mechanism may be provided based on technical and/or administrative means. Before allowing communication to another SSC, the release mechanism may require that the current SSC operates in normal conditions.

5.1.4.3. Design measures for data communication subsystems

Hereafter are measures that may be considered regarding the data communication subsystems:

— Transparency to plant conditions: data communication subsystems may be designed so that processing loads, and data communication loads and patterns do not depend on the state of the plant processes being controlled.
— Tolerance to failures of communicating SSCs: the interface may be designed to minimize coupling between the data communication subsystems and the communicating SSCs, so that misbehaviours, failures, disappearances and reappearances of either side of the interface are detected by the other side and cannot adversely affect it.

5.1.4.4. Design measures for communicating SSCs

Hereafter are measures that may be considered regarding the communicating SSCs:

— Checking of received messages and data, either by comparison with redundant information (from redundant communication links and/or error detection and correction codes) or by plausibility calculation. Application-specific criteria may be used to exclude incorrect values from any further processing.
— Defined behaviour in the case of incorrect or missing data; incorrect interaction with data communication subsystems; disappearance, (re)appearance or misbehaviour of other communicating SSCs.

5.1.5. Use of common subsystems

In order to avoid CCFs, one approach is to avoid subsystems common to multiple SSCs. However, this is not always possible or practical. In such cases, defence against CCFs may be provided using two possibly complementary approaches:

— Sufficient simplicity and adequate defensive measures to provide a high level of assurance that the subsystem is not a significant source of CCFs;
— Measures guaranteeing that any failure of a common subsystem will have acceptable consequences ('safe' failures).

5.1.6. Fault tolerance

Fault tolerance techniques enable a system to tolerate misbehaviours occurring during operation. Effective and complementary tolerance approaches include:

— Detection. Fault tolerance strategies often start with detection of deviations from the intended behaviour. Various techniques exist, from self-testing and assertion checking to monitoring by external means (e.g. watchdogs). Detection may be continuous or periodic.
— Containment is also an important ingredient of fault tolerance to prevent minor misoperation from becoming system failures. The basic technique for containment is modular design.
— Masking hides the effects of non-fatal misoperation. To this end, redundant copies of correct information may be used to outweigh the incorrect information. Retry (a second attempt at an operation) may also be used and may be effective against transient faults that cause no physical damage.
— Safe fallback.
— Recovery allows a system to restore normal functioning after some misoperation. Recovery may be active (e.g. reinitialization) or passive (the system may be designed so that the normal, continued operation 'repairs' transient faults that may cause misoperation).
— Signalling of misoperation, particularly when masking is employed, is important to prevent random faults from accumulating and overwhelming tolerance measures, and to give designers useful information to detect and eliminate systematic faults.

5.2. DEFENCE IN DEPTH IN I&C SYSTEMS

'Lines of defence' are specific applications of the principle of defence in depth to the arrangement of I&C systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it.

Table 4 gives an example of defence in depth provided by the INSAG 12 [13]. It is also applicable to the I&C of the plant. It comprises five lines of defence.

The following gives another example with four lines of defence:

(1) Control system — The control line of defence consists of that non-safety equipment which routinely prevents reactor excursions toward unsafe regimes of operation, and is used for normal operation of the reactor.

TABLE 4. EXAMPLE OF LINES OF DEFENCE

Level	Objective	Essential means
1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
2	Control of abnormal operation and detection of failures	Control limiting and protection systems and other surveillance features
3	Control of accidents within the design basis	Engineered safety features and accident procedures
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
5	Mitigation of radiobiological consequences of significant releases of radioactive material	Off-site emergency response

(2) RTS – The reactor trip line of defence consists of that safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.
(3) ESFAS – The ESFAS line of defence consists of that safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel and containment).
(4) Monitoring and indicators – The monitoring and indication line of defence consists of sensors, displays, data communication systems and manual controls required for operators to respond to reactor events.

5.3. INDEPENDENCE OF SSCs

As mentioned in Section 1.5, an I&C architecture usually includes different levels of SSCs between which CCFs might be of concern: lines of defence, subsystems implementing diverse functions within a safety I&C system, redundant channels of a safety I&C (sub)system.

Different approaches may be used to guarantee the independence of these various types of SSCs. For example, although separation is applicable to all cases:

— Functional, design, human and operational diversity, and no or very limited and controlled data communication may be the main strategy to prevent CCFs of multiple lines of defence;
— Functional, human and operational diversity, and no or very limited and controlled data communication may be applied to subsystems of a safety I&C system, in complement to limited design diversity (same equipment used in the subsystems) and design measures that provide reasonable assurance that the equipment used will not be a significant source of CCFs (see Table 2, for example);
— Human and operational diversity may be applied to the redundant channels of safety I&C system (which are usually identical or nearly identical), in complement to design measures that provide reasonable assurance that the equipment and data communication subsystems used will not be a significant source of CCFs (see Table 2, for example).

5.4. MAINTENANCE AND MODIFICATION

For I&C systems performing functions important to safety, the prevention of simultaneous activities on different redundant units avoids a resulting failure of more than one of the redundant subsystems.

Analysis of potential side effects of maintenance activities during power operation, with a view to the chance for unintended dependencies between independent systems, can be used to develop procedures with appropriate measure to prevent, detect and/or mitigate these side effects.

In cases where a hardware component needs to be replaced by a substitute, it can be ensured by adequate qualification of hardware and software features and by verification of compatibility between replaced and existing components that the reliability of the I&C safety systems is not reduced and new failure modes are not introduced. The adequacy of the qualification must be justified, taking into account the complexity of the components.

Implementation of a systematic approach to testing and replacement can make CCFs unlikely within those parts of the I&C architecture which are subjected to changed environmental conditions in the event of an accident. The approach should ensure that those parts subject to radiation and thereby to rapid ageing or changes in physical properties (cables, sensors) or whose loading is changed in response to a challenge (e.g. switching of power amplifiers, relays) cannot result in undetected failures. Replacement intervals may be determined by accelerated ageing.

Where maintenance activities involve the adjustment of configuration or calibration data, these activities should be controlled by documented procedures ensuring that:

— Maintenance adjustments are within defined limits (such limits may be imposed by the system design in which case no formal restrictions need to be placed upon the maintenance staff);

— Where such adjustments are performed while a system is in use, the effect on the readiness of the system to perform its functions is evaluated; and
— A record of all maintenance adjustments is maintained.

It must be assured that after any maintenance activity, the effected I&C system is brought back to the correct operational mode.

5.5. SECURITY ASPECTS

Internal or external threats can introduce faults or trigger latent faults to cause CCFs in I&C systems of NPPs. In general, these issues are dealt with in the overall security plan of an NPP or a more specific system security plan. The latter determines the requirements regarding the protection, the accessibility, the confidentiality and the integrity of data and functions of the I&C system. Compliance to a properly formulated system security plan guarantees that

— Unauthorized persons and systems can neither modify the state of the I&C system (or any of its subsystems) or its functionality (e.g. the system or application software and their data) nor gain access to the system functions, while
— These actions are not denied to authorized persons and systems.

Subclauses 5.4.2 and 6.2.2 of IEC 61513 [1] provide requirements for security at the level of the I&C architecture and at the level of an individual I&C system.

The plan includes security provisions to be applied during the various phases of the system life cycle (including development, operation and maintenance) based on the analysis of the security threats and vulnerabilities regarding the software aspects of the I&C system. These may include:

— Identification of, access control to, and management of security critical data and functions, including communication barriers;
— Configuration and parameterization of the software so as to avoid unnecessary causes of vulnerability;
— Recruitment and screening of personnel and other related human resource (HR) practices;
— Identification and authentication of personnel;
— Traceability of security related actions to personnel.

The plan should include provisions for the evaluation of the effectiveness of the solutions implemented.

6. RATIONALE AND DECISION ON MEASURES AGAINST CCFs

Common wisdom has said that nuclear safety functions should be as simple as possible. This wisdom is based on the presumption that when a design is simple, there is less chance for error to be introduced or for failures to occur. Also, if a design can be easily understood by others then the chance to detect errors is enhanced. However, measures taken as defence against CCFs can add complexity to the design. For example, line filters that suppress power transients introduce new components and failure modes to the system. Therefore, using a design that is intended to cope with CCFs will mean that trade-offs must be made.

Design measures to defend against CCF can aim at removing the chance of common fault, or removing the chance of a common trigger event, or both. Deciding on which approach will be more effective should be driven by the vulnerability analysis described in Section 3.

The following example of alternate design approaches illustrates the difference of targeting the faults and the triggers.

Analysis of the safety system reveals vulnerability to CCFs of key protective functions due to uncertainty of the relation of the process measurements to the event. Using plant transient analysis, a set of alternate functions is found to provide adequate protection against the event. These functionally diverse actuations are assigned to two independent subsystems of the same safety category. Since the two subsystems will be processing a different set of variables, the input signal trajectories of the two subsystems will be inherently different. Thus the combination of signal diversity and functional diversity may be analysed to sufficiently address the potential for CCFs by elimination of the common trigger means.

An alternative design approach to the one outlined above would place all of the safety actuation functions, including identified functionally diverse actuations, in a primary safety system. A subset of functions is implemented in a smaller independent system (secondary). Because it is not necessary to assume a single failure of the secondary system concurrent with CCFs within the primary system, redundancy in the secondary system is not needed. Also, because the reliability requirements of the secondary system are lower than those of the primary system, the secondary system can be implemented with a lower safety classification. However, since the primary and secondary system will be processing some of the same variables, the potential for common signal trajectory may not have been adequately addressed. In this case, other measures of diversity may be necessary to reduce the chance of a common fault in the two systems.

Other trade-offs involving targeting the faults or the trigger events are possible. For instance, in removing the potential for CCFs due to electromagnetic interference, it is possible to increase the resistance of the system to disturbances or to eliminate disturbance sources from the vicinity of the system.

In making design trade-off decisions, many factors must be considered, including:

— Assessed CCF vulnerabilities of the system;
— Level of complexity of alternative designs;
— Potential to introduce new failure modes to the plant;
— Impact on maintenance activities;
— Cost of analysis vs. cost of implementing diversity;
— Reliability of the resulting system;
— Resulting improvement in plant safety;
— Effectiveness of existing multiple levels of safety;
— Effectiveness of measure taken to avoid, remove and tolerate faults.

Once a design is proposed, it should be analysed to determine the residual risk of CCF as well as for other impacts on plant safety.

6.1. SAFETY IMPACTS

Design trade-offs to address potential CCF involves making decisions with incomplete or uncertain information. Many papers have been written on this topic. Most methods proposed involve the use of probabilistic analysis to select among alternative choices.

IEC 61508-6 provides guidance on estimating CCFs employing the Beta Factor method. Based on the assessment of various factors that could contribute to CCFs, a factor (β) is estimated, which is then used as a multiplier of the single channel failure rate to determine an estimate of the CCF frequency. While this method has been shown to be appropriate for hardware-based I&C systems, its application to software-based computer I&C is of limited usefulness. Quantitative assessment of software reliability is not easy; estimating the fraction of failures that could lead to CCFs is even harder.

Probabilistic safety analysis (PSA) is often performed to assess the overall safety of the nuclear plant. Such analyses identify accident scenarios to assess the consequences of various combinations of failure events. The resulting figures, such as core damage frequency and frequency of large radioactive release, provide measures of the ‘goodness’ of the plant design that is analysed.

PSA calculations used in sensitivity studies can provide useful insight to guide the designer in addressing CCF potentials. By modelling the proposed independent functions or systems that respond to a given event with a dependence coupling factor (β), the values of this coupling factor that result in acceptable core damage frequency can be determined. If the value of β is large (approaching 1.0) and the core damage frequency remains acceptable, then the need to address CCFs between the two systems is minimal. If, on the other hand, the acceptable β is near zero, then special measures to ensure independence of the functions or systems are needed.

PSA studies include the benefits of the multiple levels of defence provided by the various control and safety systems of the plant. Thus, in addition to providing guidance as to where additional diversity may be needed, such studies evaluate the effectiveness of defence in depth as a measure to cope with CCFs.

Design to address CCFs is a form of risk management. In risk management, risk is determined as the product of probability and consequences. If either the probability or the consequence is low, the product of the two is low and hence the overall risk is low. As either or both of the factors increase, risk increases. A number of risk sources can be compared in this way to prioritize the actions to be taken to reduce risk.

Since the analysis of CCF vulnerability includes much uncertainty, it is not practical to estimate precise probabilities for use in risk prioritization. Nevertheless, general qualitative assessment of the likelihood of various CCF causes may be possible. For example, since millions of Intel microprocessors are in use in a wide variety of applications throughout the world, the likelihood of CCFs due to hardware faults of the CPU is much lower than that of CFFs due to a software fault in a single application programme.

In assessing the probability and consequences of a CCF occurrence, the effectiveness of fault tolerance measures should be taken into consideration. For instance, many computer faults will lead to a condition of cessation of programme execution, which can be easily detected by watchdog timers. If fail safe action can be taken in such conditions, the ultimate risk is low, even if it occurs in multiple channels.

When ranking various risk elements against each other, risks other than those involving CCF should also be included. In this way, the impact of increased complexity on the functional reliability of a safety function versus the reduction of risk by applying diversity can be assessed.

Once risk elements are prioritized, a decision is made on each as to its disposition. The four possible choices are:

(1) **Eliminate the risk**. This requires positive action, and residual risk is zero. For CCFs, this is generally not practical because of the uncertainty in the vulnerability. If one is not sure of the existence of the problem in the beginning, one cannot be certain that it has been eliminated.
(2) **Mitigate the risk**. This also requires positive action, and some residual risk remains. To determine the residual risk, it will be necessary to assess how effective any measures taken to remove CCFs have been.
(3) **Transfer the risk**. Generally this is not possible for nuclear safety since the public must ultimately be protected from adverse effects of plant accidents.
(4) **Accept the risk**. This means the residual risk is the same as the original risk. If the product of failure probability and consequences is acceptably low, then resources can be better spent in other areas to improve plant safety. This is where PSA studies can help guide the CCF design process.

Thus, design to address CCF generally is reduced to trade-offs between mitigating and accepting risk. In either case, the residual risk is not zero and should be assessed by the methods described in Section 3.

6.2. COST–BENEFIT

Design trade-off studies often include cost/benefit analysis. This is also the case in addressing CCF. A common view of nuclear safety is that cost is no object. In some countries, it is not allowed to compare human life to money. However, in practice, this may not be a totally practical view. Costs involved in eliminating the potential extend beyond monetary issues. Increases in system complexity and maintenance complexity caused by diversity can cost the overall design by a reduction in the reliability resulting from random failures. Resources spent on defensive measures, including processing time and memory, can impact the overall performance of a safety function.

Costs can be compared to decide whether it is more cost effective to evaluate the potential for CCFs or to implement diverse means to mitigate an undefined CCF. However, in both cases, there is uncertainty in the success of the result, which must be taken into consideration in the cost comparison.

The benefit side of the equation is also difficult to assess in designing to address CCFs. One can never be certain that a design feature included to eliminate common faults or common triggers is 100 per cent effective. Also, features included in the design that address vulnerabilities that in reality do not exist (or are of a very low probability) provide no benefit in the ultimate safety of the plant.

Thus a CCF cost–benefit analysis cannot in general be a clear-cut quantitative calculation. Rather, it will be a subjective reasoning that supports design decisions that are made. Such reasoning is not possible without also combining the results of the CCF vulnerability analysis discussed in Section 3 into the scope of the analysis.

7. CONCLUSIONS AND RECOMMENDATIONS

The current generation of I&C systems for nuclear power plant applications are highly integrated digital systems. The interactions of these digital I&C systems are much more complex than the analogue systems that have been deployed previously. This complexity of interaction between subsystems increases the possibility that a latent fault can exist in the system that could be triggered and propagate and thus cause the system to not perform as expected.

Several organizations have been working on methods to analyse, identify and protect against the effects of CCFs in I&C systems. This work is continuing, and there are several approaches being developed and employed that are currently being evaluated for effectiveness. At this time, a qualitative method to evaluate a system for CCF potential has not been established, and information on the topic is still evolving.

Currently, different methodologies are being used within different organizations and regions. The differences in methodology are driven from differences in regulatory guidance and requirements from different regulatory environments. Different approaches are also required for new plant designs and plant upgrades. These different applications have some common elements. With all of the methods, the system is decomposed into elements so that the signal–software–hardware interactions can be evaluated. To ensure that all of the potential common areas of the system are evaluated, this review should include experts from various engineering disciplines.

Experience with evaluating existing systems is currently being investigated, and as these results are published, they are incorporated into the IAEA's work that is continuing on the topic.

REFERENCES

[1] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — General Requirements for Systems, Rep. IEC 61513, Edition 1.0, IEC, Geneva (2001).

[2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important To Safety — Classification of Instrumentation and Control Functions, Rep. IEC 61226, Edition 2.0, IEC, Geneva (2005).

[3] BOEHM, B., Software Engineering Economics, Prentice Hall, Inc., Englewood Cliffs, NJ, (1981).

[4] ELECTRIC POWER RESEARCH INSTITUTE, Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades: Applying Risk-Informed and Deterministic Methods, Rep. 1002835, EPRI, Palo Alto, CA, (2004).

[5] NUCLEAR REGULATORY COMMISSION, Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems, Rep. NUREG/CR 6303, NRC, Washington, DC.

[6] NUCLEAR REGULATORY COMMISSION, Guideline for Performing Defence-in-Depth and Diversity Assessments for Digital Upgrades, Rep. NUREG-0800, Chapter 7, Appendix 7-A, USNRC Branch Technical Position HICB-19, NRC, Washington, DC.

[7] Design Criteria Serving to Ensure Independence of I & C Safety Functions, VDI/VDE 3527 (2002).

[8] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Requirements for Coping with Common cause Failure (CCF), Rep. 62340, IEC, Geneva.

[9] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer-Based Systems Performing Category A Functions, Rep. 60880, IEC, Geneva

[10] INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE 603, IEEE, New York.

[11] INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Rep. 7-4.3.2, IEEE, New York.

[12] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Important to Safety — Hardware Design Requirements for Computer-Based Systems, Rep. 60987, IEC, Geneva (2007).

[13] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, INSAG-1275-INSAG-3 Rev. 1, IAEA, Vienna, (1999).

ABBREVIATIONS

CPU	central processing unit
DBE	design basis event
EMI	electromagnetic interference
ESFAS	engineered safety features actuation system
FAT	factory acceptance test
FMEA	failure modes and effects analysis
FTA	fault tree analysis
HW	hardware
NUREG	USNRC regulatory guide
OS	operating system
PLC	programmable logic controller
PRA	probabilistic risk analysis
RFI	radio frequency interference
RTS	reactor trip system
SAR	safety analysis report
SAT	site acceptance test
SW	software

GLOSSARY

block. A block is a fundamental element of an analysis-oriented decomposition of an I&C architecture or system for the purpose of CCF analysis.

Note 1. A block is associated with required functions that are relevant to safety. The granularity provided by the block representation depends upon the scope of the analysis and the function required.

Note 2. A block can be a physical subset of equipment and software for which it can be reasonably determined that internal failures will not adversely affect other blocks.

Note 3. One train of the three or four redundant trains of an I&C system that is designed to meet the single failure criterion may form a block.

channel. An arrangement of interconnected components within a system that initiates an output. Note that this term is used in the general sense and not in the more restrictive sense where a channel loses its identity or where single output signals are combined with signals from other channels.

common cause failure (CCF). Concurrent failure of two or more structures, systems or components due to the triggering of a single systematic fault or causally related faults by a single specific event.

Note 1. Failures are concurrent when the time interval between the failures is too short for repair measures.

Note 2. See also the definitions of failure and systematic fault.

defence in depth.

The application of more than one protective measure for a given safety objective, so the objective is achieved even if one of the protective measures fails (see also IAEA Safety Glossary V1 from April 2000 and IEC 61513 - A3).

Note. The protective measures for defence in depth may involve one or several of the following elements:

The existence of several groups of safety functions so that each individual group ensures compliance with the design specifications:

—The existence of passive systems and active safety systems in parallel;
—The existence of safety systems and operational systems if these are mutually independent and have actions that are cumulative in case of a request;
—The existence of different design methods in parallel to increase system robustness and fault tolerance.

diversity. Existence of two or more different ways or means of achieving a specified objective (source: IEC 60880).

Note. Diversity is specifically provided as a defence against CCF. It may be achieved by providing systems that are physically different from each other or by functional diversity, where systems implemented with similar equipment achieve the specified objective in different ways (see also ‘functional diversity’).

error. Discrepancy between a computed, observed or measured (output) value and the true, specified or theoretical correct value due to a nonconformity or interference.

failure. Deviation of the delivered service from the intended service such that the acceptance criteria are no longer satisfied.

Note. A failure is the result of the activation of a fault by a triggering event.

fault. Defect in a hardware, software or system component (source: IEC 61513).

Note 1. Faults may be subdivided into random faults that result, for example, from hardware degradation due to ageing and systematic faults (e.g. software faults, which result from design errors).

Note 2. A fault (notably a design fault) may remain undetected in a system until specific conditions are such that the result produced does not conform to the intended function (i.e. a failure occurs).

independent I&C systems. Systems that are independent possess both of the following characteristics:

— The ability of one system to perform its required function is unaffected by the operation or the failure of another system;
— The ability of one system to perform its function is unaffected by the presence of the potential effects resulting from the postulated initiating event for which it is required to function (source: definition on 'independent equipment' from IEC 61513 [1]).

Note. Means to achieve design independence in accordance with proper design principles are electrical isolation, physical separation, communications independence and freedom of interference from the process to be controlled.

input signal transient. Time behaviour of all input signals that are fed into the I&C system to be processed (source: IEC 62340).

Note. The behaviour of an I&C system is finally determined by the signal trajectory, which also includes the internal states of the I&C equipment; the requirement specification, however, defines the safety related reactions of the I&C system in response to "input signal transients".

latent fault. Fault that is undetected in a system (source: IEC 62340).

Note. Latent faults may result from errors during specification, design or from manufacturing defects and may be of any physical or technical type which it is reasonable to be assumed. In the case of specification or design faults, it should be assumed that latent faults may be implemented in all redundant subsystems in the same way so that a specific signal trajectory could trigger CCF of the concerned I&C system.

physical separation. Separation by geometry (distance, orientation, etc.), by appropriate barriers or by a combination thereof.

redundancy. Provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other.

signal trajectory. Time histories of all equipment conditions, internal states, input signals and operator inputs that determine the outputs of a system (source: IEC 60880).

single failure. A failure which results in the loss of capability of a system or component to perform its intended safety function(s), and any consequential failure(s) which results from it.

systematic failure. Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors (source: IEC 61513)

Note. The common cause failure is a subtype of systematic failure such that the failures of separate systems, redundancies or components can be triggered coincidentally.

systematic fault. Fault that affects all components of a specific type (hardware or software) and is caused during the design of the manufacturing process or is related to maintenance or modification activities.

triggering mechanism. Specific event or operating condition that causes structures, systems or components to fail due to a latent fault.

Note. Triggering mechanisms can cause the failure of two or more separate structures, subsystems or components in a time-correlated way.

CONTRIBUTORS TO DRAFTING AND REVIEW

Arndt, S.	Nuclear Regulatory Commission, United States of America
Barbaud, M.	EDF, France
Bartha, T.	MTA SZTAKI, Hungary
Bitsit, F.T.	International Atomic Energy Agency
Bock, H.-W.	Areva NP, Germany
Bond, L.J.	Pacific Northwest National Laboratory, United States of America
Buchholz, C.	GEH Nuclear Energy, United States of America
Cook, B.M.	Westinghouse Electric Co., United States of America
Esmenjaud, C.	Data Systems & Solution, France
Glöckler, O.	International Atomic Energy Agency
Graf, A.	AREVA NP, Germany
Gran, B.A.	OECD Halden Reactor Project, Norway
Harber, J	Atomic Energy of Canada Limited, Canada
Hefler, J.	Altran Solutions, Inc., United States of America
Jiang. J.	University of Western Ontario, Canada
Johansson, K.A.M.	Swedish Nuclear Power Inspectorate, Sweden
Johnson, G.	International Atomic Energy Agency
Kim, B.R.	Korea Institute of Nuclear Safety, Republic of Korea
Koo, I.S.	Korea Atomic Energy Research Institute, Republic of Korea
Kunito, S.	Tokyo Electric Power Co., Japan
Lee, J.S.	Korea Atomic Energy Research Institute, Republic of Korea
Lindner, A.	Institute for Safety Technology Gmbh, Germany
Märzendorfer, M.	Kernkraftwerk Leibstadt AG, Switzerland
Murray, J.	INVENSYS, United States of America
Naser, J.	Electric Power Research Institute, United States of America
Orme, S.	British Energy Generation Ltd, United Kingdom
Park, H.-S.	Korea Institute of Nuclear Safety, Republic of Korea

Quinn, E.	Longenecker and Associates, United States of America
Rasmussen, B.	Kurz Technical Services, Inc., United States of America
Seaman, S.G.	Westinghouse Electric Company, United States of America
Sohn, K.Y.	Samchang, Republic of Korea
Thunem, A.P.-J.	OECD, Halden Reactor Project, Norway
Thuy, N.	EdF, France
Török, R.	Electric Power Research Institute, United States of America
Tuszynski, J.	OKG AB, Sweden
Waedt, K.	Areva NP, Germany
Wahlström, B.	Technical Research Centre of Finland, Finland
Wood, R.	ORNL, United States of America

Consultants Meetings

Vienna, Austria: 27–30 March 2006

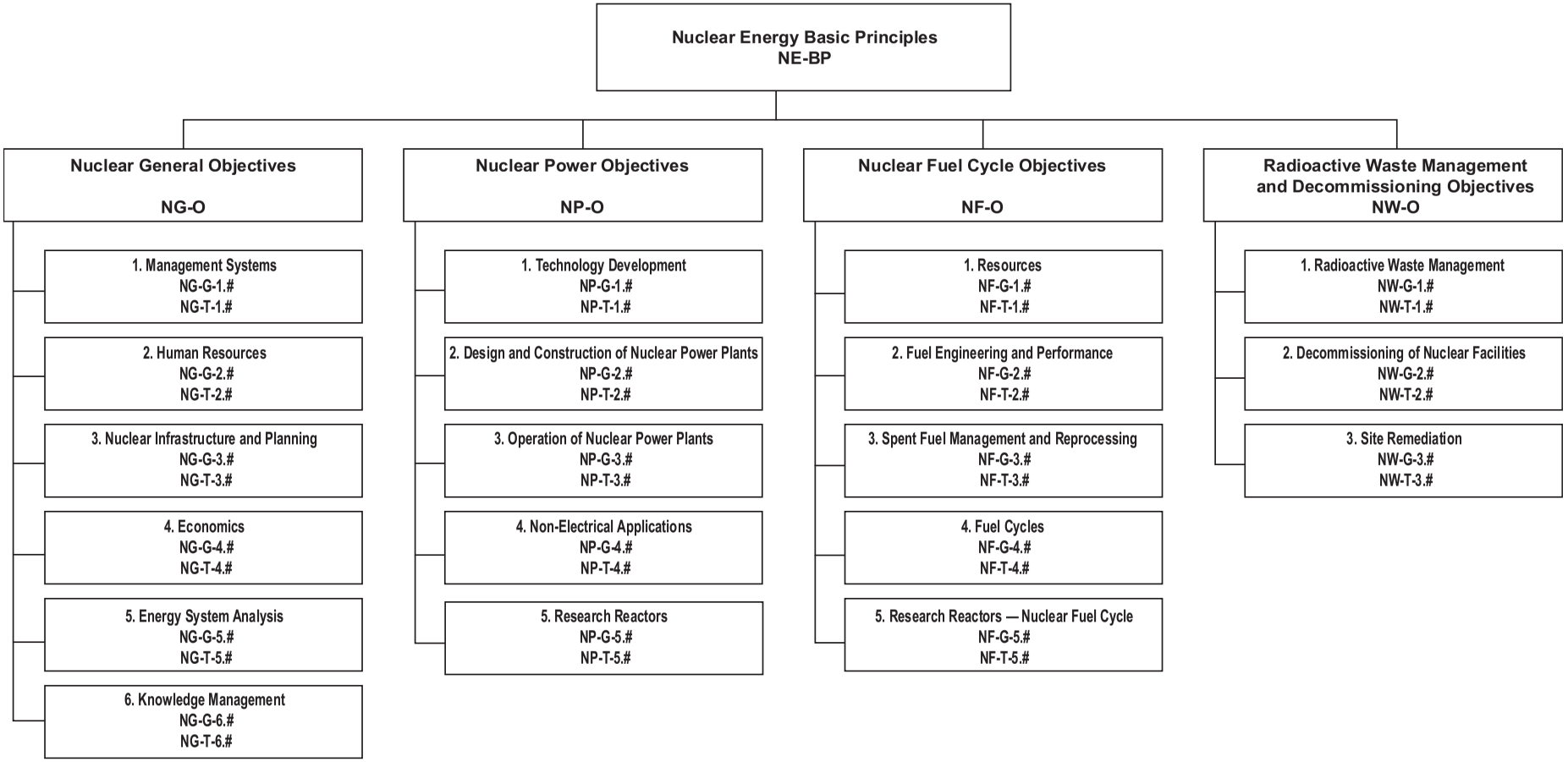
Berlin, Germany: 8–9 June 2007

Technical Meetings

Bethesda, Maryland, USA: 19–21 June 2007

Vienna, Austria: 26–30 November 2007

Structure of the IAEA Nuclear Energy Series



Key

BP: Basic Principles
O: Objectives
G: Guides
T: Technical Reports
Nos. 1-6: Topic designations
#: Guide or Report number (1, 2, 3, 4, etc.)

Examples

NG-G-3.1: Nuclear General (**NG**), **G**uide, Nuclear Infrastructure and Planning (topic **3**), **#1**
NP-T-5.4: Nuclear Power (**NP**), Report (**T**), Research Reactors (topic **5**), **#4**
NF-T-3.6: Nuclear Fuel (**NF**), Report (**T**), Spent Fuel Management and Reprocessing, **#6**
NW-G-1.1: Radioactive Waste Management and Decommissioning (**NW**), **G**uide, Radioactive Waste (topic **1**), **#1**

No. 21, July 2006

IAEA
International Atomic Energy Agency

Where to order IAEA publications

In the following countries IAEA publications may be purchased from the sources listed below, or from major local booksellers. Payment may be made in local currency or with UNESCO coupons.

Australia
DA Information Services, 648 Whitehorse Road, Mitcham Victoria 3132
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

Belgium
Jean de Lannoy, avenue du Roi 202, B-1190 Brussels
Telephone: +32 2 538 43 08 • Fax: +32 2 538 08 41
Email: jean.de.lannoy@infoboard.be • Web site: http://www.jean-de-lannoy.be

Canada
Bernan Associates, 4611-F Assembly Drive, Lanham, MD 20706-4391, USA
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: order@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 1-5369 Canotek Rd., Ottawa, Ontario, K1J 9J3
Telephone: +613 745 2665 • Fax: +613 745 7660
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

China
IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing

Czech Republic
Suweco CZ, S.R.O. Klecakova 347, 180 21 Praha 9
Telephone: +420 26603 5364 • Fax: +420 28482 1646
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

Finland
Akateeminen Kirjakauppa, PL 128 (Keskuskatu 1), FIN-00101 Helsinki
Telephone: +358 9 121 41 • Fax: +358 9 121 4450
Email: akatilaus@akateeminen.com • Web site: http://www.akateeminen.com

France
Form-Edit, 5, rue Janssen, P.O. Box 25, F-75921 Paris Cedex 19
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90 • Email: formedit@formedit.fr

Lavoisier SAS, 14 rue de Provigny, 94236 Cachan Cedex
Telephone: + 33 1 47 40 67 00 • Fax +33 1 47 40 67 02
Email: livres@lavoisier.fr • Web site: http://www.lavoisier.fr

Germany
UNO-Verlag, Vertriebs- und Verlags GmbH, August-Bebel-Allee 6, D-53175 Bonn
Telephone: +49 02 28 949 02-0 • Fax: +49 02 28 949 02-22
Email: info@uno-verlag.de • Web site: http://www.uno-verlag.de

Hungary
Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
Telephone: +36 1 257 7777 • Fax: +36 1 257 7472 • Email: books@librotrade.hu

India
Allied Publishers Group, 1st Floor, Dubash House, 15, J. N. Heredia Marg, Ballard Estate, Mumbai 400 001,
Telephone: +91 22 22617926/27 • Fax: +91 22 22617928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell, 24/4800, Ansari Road, Darya Ganj, New Delhi 110002
Telephone: +91 11 23268786, +91 11 23257264 • Fax: +91 11 23281315
Email: bookwell@vsnl.net • Web site: http://www.bookwellindia.com

Italy
Libreria Scientifica Dott. Lucio di Biasio “AEIOU”, Via Coronelli 6, I-20146 Milan
Telephone: +39 02 48 95 45 52 or 48 95 45 62 • Fax: +39 02 48 95 45 48

Japan
Maruzen Company, Ltd., 13-6 Nihonbashi, 3 chome, Chuo-ku, Tokyo 103-0027
Telephone: +81 3 3275 8582 • Fax: +81 3 3275 9072
Email: journal@maruzen.co.jp • Web site: http://www.maruzen.co.jp

Korea, Republic of
KINS Inc., Information Business Dept. Samho Bldg. 2nd Floor, 275-1 Yang Jae-dong SeoCho-G, Seoul 137-130
Telephone: +02 589 1740 • Fax: +02 589 1746
Email: sj8142@kins.co.kr • Web site: http://www.kins.co.kr

Netherlands
Martinus Nijhoff International, Koraalrood 50, P.O. Box 1853, 2700 CZ Zoetermeer
Telephone: +31 793 684 400 • Fax: +31 793 615 698 • Email: info@nijhoff.nl • Web site: http://www.nijhoff.nl

Swets and Zeitlinger b.v., P.O. Box 830, 2160 SZ Lisse
Telephone: +31 252 435 111 • Fax: +31 252 415 888 • Email: infoho@swets.nl • Web site: http://www.swets.nl

New Zealand
DA Information Services, 648 Whitehorse Road, MITCHAM 3132, Australia
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

Slovenia
Cankarjeva Zalozba d.d., Kopitarjeva 2, SI-1512 Ljubljana
Telephone: +386 1 432 31 44 • Fax: +386 1 230 14 35
Email: import.books@cankarjeva-z.si • Web site: http://www.cankarjeva-z.si/uvoz

Spain
Díaz de Santos, S.A., c/ Juan Bravo, 3A, E-28006 Madrid
Telephone: +34 91 781 94 80 • Fax: +34 91 575 55 63 • Email: compras@diazdesantos.es
carmela@diazdesantos.es • barcelona@diazdesantos.es • julio@diazdesantos.es
Web site: http://www.diazdesantos.es

United Kingdom
The Stationery Office Ltd, International Sales Agency, PO Box 29, Norwich, NR3 1 GN
Telephone (orders): +44 870 600 5552 • (enquiries): +44 207 873 8372 • Fax: +44 207 873 8203
Email (orders): book.orders@tso.co.uk • (enquiries): book.enquiries@tso.co.uk • Web site: http://www.tso.co.uk

On-line orders:
DELTA Int. Book Wholesalers Ltd., 39 Alexandra Road, Addlestone, Surrey, KT15 2PQ
Email: info@profbooks.com • Web site: http://www.profbooks.com

Books on the Environment:
Earthprint Ltd., P.O. Box 119, Stevenage SG1 4TP
Telephone: +44 1438748111 • Fax: +44 1438748844
Email: orders@earthprint.com • Web site: http://www.earthprint.com

United Nations (UN)
Dept. I004, Room DC2-0853, First Avenue at 46th Street, New York, N.Y. 10017, USA
Telephone: +800 253-9646 or +212 963-8302 • Fax: +212 963-3489
Email: publications@un.org • Web site: http://www.un.org

United States of America
Bernan Associates, 4611-F Assembly Drive, Lanham, MD 20706-4391
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: order@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669
Telephone: +888 551 7470 (toll-free) • Fax: +888 568 8546 (toll-free)
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

Orders and requests for information may also be addressed directly to:

Sales and Promotion Unit, International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 (or 22530) • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–106309–0
ISSN 1995–7807