Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH

MITARBEIT IM OECD/NEA COMPSIS-PROJEKT

Abschlussbericht

Dr. Jan C. Stiller

Oktober 2011

Auftrags-Nr.: 810410

Anmerkung:

Das diesem Bericht zugrundeliegende Vorhaben ist von der GRS im Auftrag des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit im Rahmen des Vorhabens 3608I01310 „Wissenschaftlicher Beitrag zur COMPSIS-Datenbank und Aufbereitung von Betriebsdaten von rechnergestützter Leittechnik in kerntechnischen Anlagen“ erstellt worden. Die Verantwortung für den Inhalt dieser Veröffentlichung trägt der Auftragnehmer.

Der Bericht gibt die Auffassung und Meinung des Auftragnehmers wieder und muss nicht mit der Meinung des Auftraggebers übereinstimmen.

Einzelne Passagen dieses Berichts wurden mit Rücksicht auf entgegenstehende Rechte Dritter geschwärzt

GRS - A - 3609

Kurzfassung

In deutschen Kernkraftwerken sind in vielen Leittechniksystemen mit sicherheitstechnischer Bedeutung rechnerbasierte oder andere „intelligente“ Einrichtungen wie speicherprogrammierbare Steuerungen (SPS), Field programmable gate arrays (FPGA) oder Application specific intigrated circuits (ASIC) im Einsatz. Zur systematischen Erfassung und Auswertung der internationalen Betriebserfahrungen mit solchen Einrichtungen wurde von der OECD/NEA im Jahr 1996 die Task Group „Computer-Based Systems Important to Safety“ (COMPSIS) initiiert, die seit 2005 als eigenständiges Projekt betrieben wird. Die GRS arbeitet von Anfang an in COMPSIS mit. Seit dem Beginn der zweiten COMPSIS-Projektphase am 1.1.2008 wurde die Mitarbeit im Rahmen des speziell für die COMPSIS-Mitarbeit beauftragten Vorhabens 3608I01310 durchgeführt. Im vorliegenden Bericht wird über dieses Vorhaben berichtet. Zunächst werden die Ziele des COMPSIS-Projektes vorgestellt. Diese umfassen die Bereitstellung eines Formalismus zur Erfassung von Software- und Hardwarefehlern, der Betrieb einer qualitätsgesicherten Datenbank sowie die Ereigniserfassung und Auswertung über einen langen Zeitraum, um die Ereignisursachen und mögliche Gegenmaßnahmen besser zu verstehen. Beim COMPSIS-Projekt sind eindeutig definierte Prozesse zur Erfassung, Verwaltung und Qualitätssicherung der Daten eingerichtet und haben sich bewährt. Im Laufe der zwei Projektperioden wurden kontinuierlich Daten zu COMPSIS-Ereignissen erfasst. Die Datenmenge erhöhte sich von 40 Ereignissen zum Beginn der jetzigen Projektperiode auf 96 Ereignisse zum gegenwärtigen Zeitpunkt. Während des Projektes traten in Deutschland drei COMPSIS-Ereignisse auf, so dass nun insgesamt 8 deutsche Ereignisse in der Datenbank vorhanden sind. Mit den bisherigen Projektergebnissen werden Grundlagen für eine Bewertung sicherheitsrelevanter rechnerbasierter Einrichtungen in Kernkraftwerken geschaffen. Da die Menge der zur Verfügung stehenden Betriebserfahrung noch relativ beschränkt ist, aber rechnerbasierte Leittechnik in zunehmenden Maße eingesetzt wird, sowie da sie kurze Innovationszyklen aufweist, ist es auch in Zukunft erforderlich, am COMPSIS-Projekt mitzuwirken, um den weiteren Zugang zur internationalen Betriebserfahrung solcher Einrichtungen in Kernkraftwerken zu gewährleisten.

Abstract

In German nuclear power plants, software-based or other “intelligent“ devices such as programmable logic controllers (PLS), field programmable gate arrays (FPGA) or application specific integrated circuits (ASIC) are used in many safety-significant instrumentation and control systems. In 1996, the OECD/NEA set up the task group “Computer-Based Systems Important to Safety” (COMPSIS) for the systematic collection and evaluation of international operating experience with such systems. In 2005 COMPSIS became an independent project. GRS has been participating in in COMPSIS from the beginning. Since the start of the second COMPSIS project phase on January 1st 2008 GRS participation has been carried out within the framework of Project 3608I01310. This report gives an account of the work performed in this project. First, the objectives of the COMPSIS project are outlined. These comprise the provision of formal procedures for the collection of events with software errors and hardware failures, the operation of a quality-assured database and the collection and evaluation of events over a long period of time in order to better understand the causes of these events and possible countermeasures. In COMPSIS, clearly defined and proven processes have been established for the collection, administration and quality assurance of the data. During the course of the two project periods, data on COMPSIS events have continuously been collected and added to the data base. The number of events has increased from 40 events at the beginning of the current project period to 96 events at the current stage. During the term of project 3608I01310, three COMPSIS events occurred in Germany, which brings to current total number of German events in the database to eight. The project results obtained so far forms a basis for assessments of safety-relevant computer based I&C systems in nuclear power plants. As the amount of operating experience is as yet relatively limited, but computer-based instrumentation and control systems are increasingly used and also because their innovation cycles are quite short, it is necessary to continue participating in the COMPSIS project in the future to ensure continued access to international operating experience with such systems.

Inhaltsverzeichnis

1 Einleitung und Überblick

In deutschen Kernkraftwerken sind in vielen Leittechniksystemen mit sicherheitstechnischer Bedeutung rechnerbasierte oder andere „intelligente“ Einrichtungen wie speicherprogrammierbare Steuerungen (SPS), Field programmable gate arrays (FPGA) oder Application specific intigrated circuits (ASIC) im Einsatz. Dies betrifft betriebliche Systeme (z. B. die Turbinensteuerung, deren Ausfall zu Transienten führen kann), Begrenzungseinrichtungen auf der Sicherheitsebene 2 und einzelne Betriebsmittel von Komponenten, die auf der Sicherheitsebene 3 eingesetzt sind (z. B. Überstromschutzeinrichtungen von Schaltern, Messumformer, Steuerungen von Notstromdieseln und Kranen, Neutronenflussmessung).

Zur systematischen Erfassung und Auswertung der internationalen Betriebserfahrungen mit solchen Einrichtungen wurde von der OECD/NEA im Jahr 1996 die Task Group „Computer-Based Systems Important to Safety“ (COMPSIS) initiiert. Nach Ablauf der Testphase wurde vom Committee on the Safety of Nuclear Installations (CSNI) im Jahre 2003 beschlossen, diese Initiative in der Form eines eigenständigen Projektes fortzuführen, das in zeitlich begrenzten Phasen abgewickelt wird. Die erste Projektphase hatte die Laufzeit 01.01.2005 bis 31.12.2007. Die Ergebnisse der ersten Projektperiode sind in dem Bericht „Computer-Based Systems Important to Safety (COMPSIS) Project: 3 Years of Operation (2005-2007)“ /1/ dokumentiert. Für die zweite Projektphase des COMPSIS-Projekts war ursprünglich eine Laufzeit vom 01.01.2008 bis 31.12.2010 vorgesehen; sie wurde zwischenzeitlich bis zum 31.12.2011 verlängert. Die GRS arbeitet seit Beginn in COMPSIS mit. Die Mitarbeit fand zunächst im Rahmen des Vorhabens INT 9166 statt. Seit dem Beginn der zweiten Projektphase am 1.1.2008 wurde die Mitarbeit im Rahmen des speziell für die COMPSIS-Mitarbeit beauftragten Vorhabens 3608I01310 durchgeführt. Im COMPSIS-Projekt arbeiten neben Deutschland zurzeit Schweden, Ungarn, Südkorea, China/Taipei, Finnland, die Schweiz und die USA mit. Das Projekt wird von einer Steuerungsgruppe kontrolliert, die so genannte Nationale Koordinatoren und den Obmann des Projekts umfasst. Das Amt des Obmanns wird von Dr. Lindner, ISTec, bekleidet. Seit 27.06.2008 ist das ISTec im Rahmen dieses Vorhabens 3608I01310 im Unterauftrag der GRS tätig.

In diesem Bericht werden in Kapitel 2 zunächst die Ziele des COMPSIS-Projektes vorgestellt. In Kapitel 3 werden die Struktur und die Arbeitsweise des COMPSIS-Projektes sowie das Konzept der COMPSIS-Datenbank erläutert. Außerdem wird der aktuelle Projektstatus an den Projektzielen gespiegelt. In Kapitel 4 wird ein Überblick über die bisher in die COMPSIS-Datenbank eingespeisten Ereignisse gegeben. Kapitel 5 enthält eine kurze Zusammenfassung sowie auf einen Ausblick auf zukünftige Arbeiten im Rahmen des COMPSIS-Projektes.

2 Ziele des COMPSIS-Projektes

Die Projektziele sind in den “Terms and Conditions” für das Projekt beschrieben /3/. Im Detail verfolgt das Projekt die folgenden Ziele:

- Bereitstellung eines Formalismus zur Erfassung von Software- und Hardwarefehlern („COMPSIS-Ereignissen“) in sicherheitsrelevanten rechnerbasierten Systemen in Kernkraftwerken. Der Formalismus ist in einer strukturierten, qualitätsgesicherten und konsistenten Datenbank abzubilden.
- Erfassung und Auswertung von COMPSIS-Ereignissen über einen langen Zeitraum um diese Ereignisse, ihre Ursachen und Gegenmaßnahmen gegen diese Ereignisse besser zu verstehen.
- Einsichten in die primären Ursachen und in beitragende Randbedingungen von COMPSIS-Ereignissen zu gewinnen, mit dem Ziel, Ansätze zur Vermeidung bzw. zur Abschwächung von Auswirkungen abzuleiten.
- Erarbeitung von Verfahren einer effektiven Erfahrungsauswertung der im COMPSIS erfassten Ereignisse einschließlich der Entwicklung von Maßnahmen gegen diese Ereignisse, wie zum Beispiel Diagnosen und Tests.
- Aufzeichnung von Attributen und dominierenden Beiträgen zu den Ereignissen als Basis für nationale Risikoanalysen zu rechnerbasierten Systemen.

Diese Ziele sind auf einen langfristigen Betrieb der Datenbank ausgerichtet. Ein wesentliches Element der “Terms and Conditions” ist der Grundsatz, dass Zugang zu den Daten nur erhält, wer selbst Daten beiträgt.

In den ersten beiden Projektperioden wurden, verglichen mit anderen Datenbankprojekten der OECD, eine relative begrenzte Anzahl von Ereignissen erfasst. Dieser Umstand ist den Tatsachen geschuldet, dass:

- sicherheitsrelevante rechnerbasierte Systeme bisher nur in begrenzten Umfang in Kernkraftwerken implementiert sind,
- aufgrund der redundanten Auslegung sicherheitsrelevanter Systeme Einzelfehler oft nicht als COMPSIS-Ereignisse erfasst werden,
- rechnerbasierte Systeme relativ komplex sind und die Ursachenermittlung von Ereignissen ein schwieriger und langwieriger Prozess ist.

Zusätzlich ist darauf hinzuweisen, dass einige Länder, die eine große Anzahl an Kernkraftwerken betreiben (z. B. Frankreich, Kanada, Japan), nicht im COMPSIS Projekt vertreten sind.

3 OECD/NEA-Projekt

3.1 Übersicht

Das COMPSIS-Projekt ist ein OECD/NEA Datenbankprojekt. Es wird vom Obmann, unterstützt vom Sekretär, geleitet. Alle beteiligten Länder haben einen Nationalen Koordinator benannt. Die Nationalen Koordinatoren (National Coordinator - NC) und der Obmann bilden die Steuerungsgruppe, wobei die Entscheidungen der Steuerungsgruppe nur von den Nationalen Koordinatoren (bzw. deren Vertreter) getroffen werden. Die nationalen Koordinatoren sind für das Einspeisen der Daten in die Datenbank verantwortlich. Sie können zusätzliche „Data Provider“ (DP) benennen, die bezüglich des Datenbankzugriffs die gleichen Rechte zur Dateneingabe besitzen wie die Nationalen Koordinatoren. Die Qualitätssicherung der Daten erfolgt durch den „Operating Agent“ (OA). Im COMPSIS-Projekt ist das das Institutt for Energiteknikk (IFE), Halden /1/. Der Operating Agent betreibt auch die Internetpräsens www.compsis.org und die Datenbank.

3.2 Codierungsrichtlinie

Die Codierungsrichtlinie wurde im Laufe der 1. Projektperiode erarbeitet. Sie ist im Bericht /1/ als Anhang enthalten. Im Laufe der 2. Projektperiode wurden kleinere Änderungen zur Präzisierung von Sachverhalten und zur Fehlerkorrektur vorgenommen, die keine Auswirkungen auf die Datenbank hatten. Um die Codierungsrichtlinie über einen längeren Zeitraum stabil zu halten, wurde ein spezifisches Änderungsverfahren eingeführt. Dieses sieht vor, dass alle Änderungsvorschläge in den Steuerungsgruppensitzungen diskutiert und Annahme oder Ablehnung beschlossen werden. Die Entscheidungen werden in den Sitzungsprotokollen festgehalten und durch den OA umgesetzt.

Die Codierungsrichtlinie liegt aktuell in der Version 3.2 vor /4/.

3.3 Web Page

Die Web Page /3/ stellt das zentrale Nutzerinterface im COMPSIS-Projekt bereit. Über die Web Page werden alle projektrelevanten Dokumente verwaltet und die Datenbank gepflegt. In Bild 2.2 ist der Startbildschirm der Web Page dargestellt. Der Zugriff erfolgt über ein gesichertes Protokoll (https).

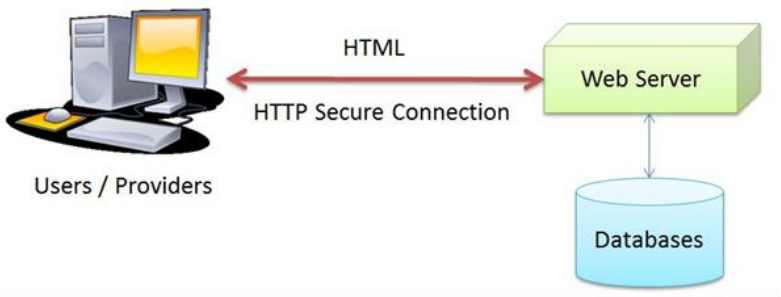

Abb. 2.1: Übersicht über Benutzerschnittstelle, Web Page und Datenbank

Die Web Page besteht aus einem öffentlich zugänglichen Teil und einem durch Passwörter abgesicherten Teil für die Projektbeteiligten. Entsprechend der Rolle im Projekt (z. B. NC, DP) sind unterschiedliche Zugriffsberechtigungen eingerichtet.

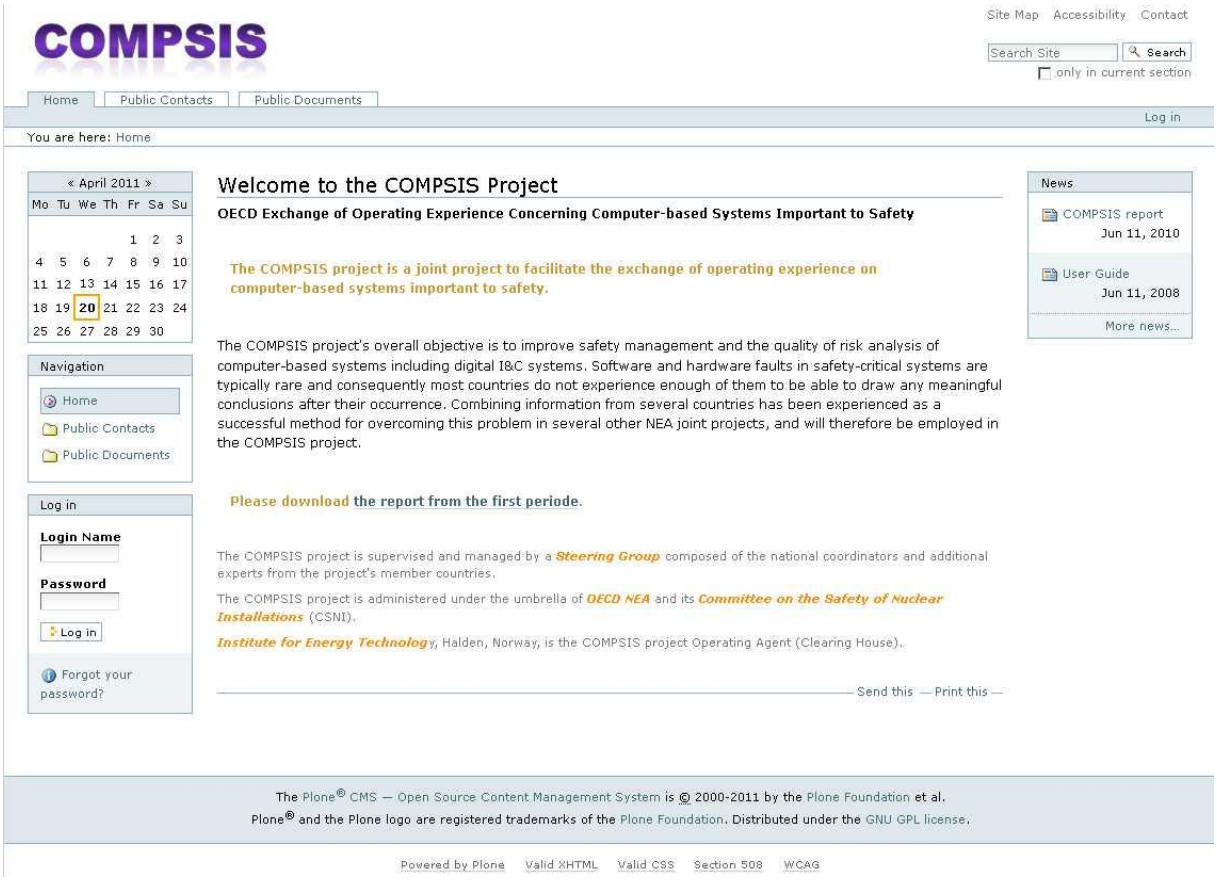

Abb. 2.2: Startbild der Web Page

3.4 Datenbank

Die im COMPSIS-Projekt eingesetzte Software ist Open Source Software. Als Datenbank kommt MySQL zum Einsatz. Das Zusammenspiel der Datenbank mit der Web Page ist in Bild 2.3 dargestellt.

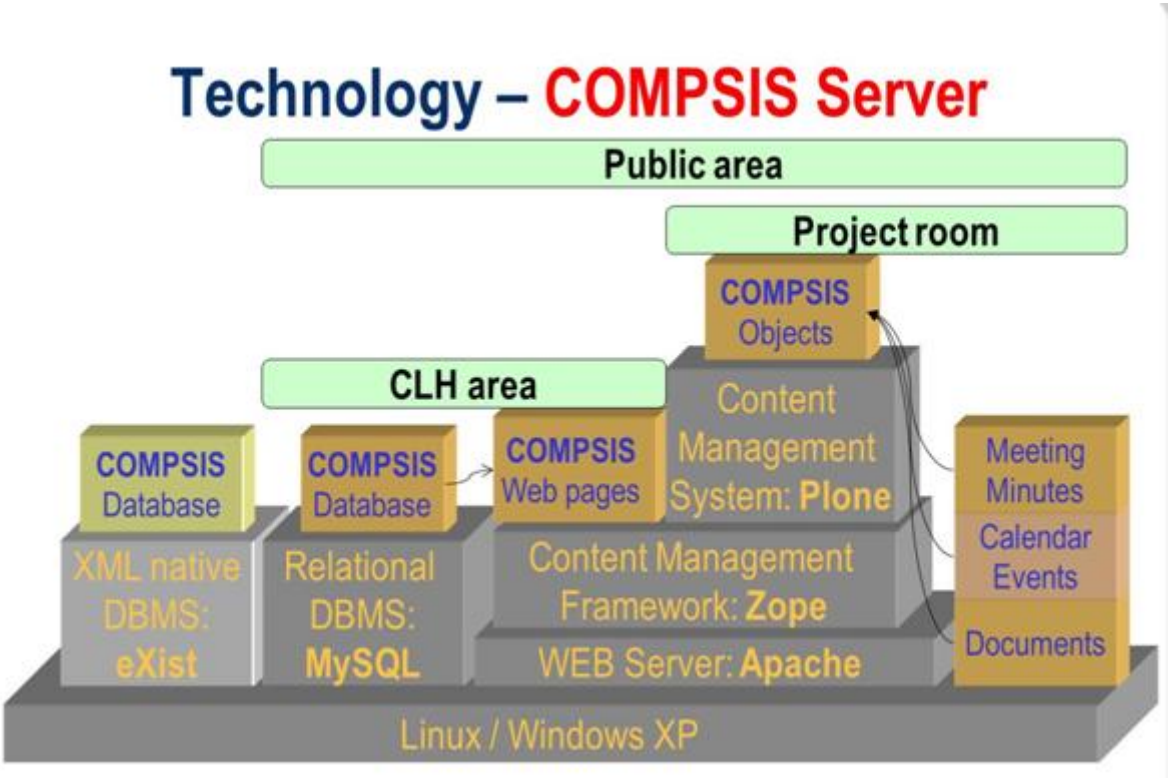

Abb. 2.3: Softwareübersicht

Für die Datenbank wurde eine Nutzeranleitung /6/ erstellt, die die Dateneingabe konsistent zur Codierungsrichtlinie /4/ unterstützt.

Die Projektstruktur ist in /1/ und /2/ detailliert beschrieben.

3.5 Berichte

Im COMPSIS-Projekt wurde im Zeitraum dieses Vorhabens 3608I01310 ein Bericht veröffentlicht /1/. Dieser Bericht enthält eine detaillierte Beschreibung des Projekts und der Datenbank. Datenerhebung, Codierung und Qualitätssicherung werden beschrieben. Außerdem wird ein detaillierter Überblick über die bis zum 31.12.2007 eingespeisten Ereignisse gegeben sowie erste Schlussfolgerungen gezogen. Dieser Bericht ist im Anhang A beigefügt.

Zurzeit befindet sich der Abschlussbericht der aktuellen Periode des COMPSIS-Projektes für die OECD/NEA /2/ in Vorbereitung.

3.6 Projektstatus

In Tabelle 4.1 sind die Projektziele und der erreichte Stand gegenübergestellt.

Table 4.1: Status der COMPSIS Projektziele

Ziel	Status
Bereitstellung eines Formalismus zur Erfassung von Software und Hardware Fehlern („COMPSIS-Ereignissen“) in sicherheitsrelevanten rechnerbasierten Systemen in Kernkraftwerken. Der Formalismus ist in einer strukturierten, qualitätsgesicherten und konsistenten Datenbank abzubilden.	Es wurde eine komplette Arbeitsumgebung bestehend aus Web Page, Datenbank und Dokumenten, die die Prozesse im COMPSIS Projekt festlegen, etabliert /6/, /7/.
Erfassung und Auswertung von COMPSIS-Ereignissen über einen langen Zeitraum um diese Ereignisse, ihre Ursachen und Gegenmaßnahmen gegen diese Ereignisse besser zu verstehen.	Fortlaufender Prozess; Datenauswertungen werden in /2/ veröffentlicht.
Einsichten in die primären Ursachen von COMPSIS-Ereignissen und von beitragenden Randbedingungen zu gewinnen, die geeignet sind, Ansätze zu deren Vermeidung bzw. zur Abschwächung ihrer Auswirkungen abzuleiten.	Erste Analysen wurden durchgeführt und publiziert (siehe /1/). Erweitere Analysen werden in /2/ publiziert.
Erarbeitung von Verfahren einer effektiven Erfahrungsauswertung der in COMPSIS erfassten Ereignisse einschließlich der Entwicklung von Maßnahmen gegen diese Ereignisse, wie zum Beispiel Diagnosen und Tests.	Dieser Prozess bedarf einer weiteren Vertiefung in der geplanten 3. Projektperiode.
Aufzeichnung von Attributen und dominierenden Beiträgen zu den Ereignissen als Basis für nationale Risikoanalysen zu rechnerbasierten Systemen.	Fortlaufender Prozess; Daten stehen den Teilnehmern für Auswertungen zur Verfügung.

Es kann festgehalten werden, dass alle Projektziele bisher erreicht wurden. Die Weiterführung des Projekts sollte sich auf die Ereigniserfassung konzentrieren. Flankierend könnten in Zukunft Auswertemethoden erarbeitet werden.

4 COMPSIS-Ereignisse

Die Anzahl der erfassten Ereignisse ist in der Projektlaufzeit kontinuierlich gestiegen. Zum Zeitpunkt 30.06.2011 wurden 96 Ereignisse erfasst. Davon sind 10 Ereignisse im Zustand „open“ (in Bearbeitung durch den NC), jeweils 4 Ereignisse befinden sich in Bearbeitung bzw. in der Endphase der Qualitätssicherung und 78 Ereignisse wurden abgeschlossen (Status „published“).

In Bild 5.1 ist der Projektfortschritt bezüglich der Ereigniserfassung zwischen der ersten und der zweiten Projektperiode dargestellt.

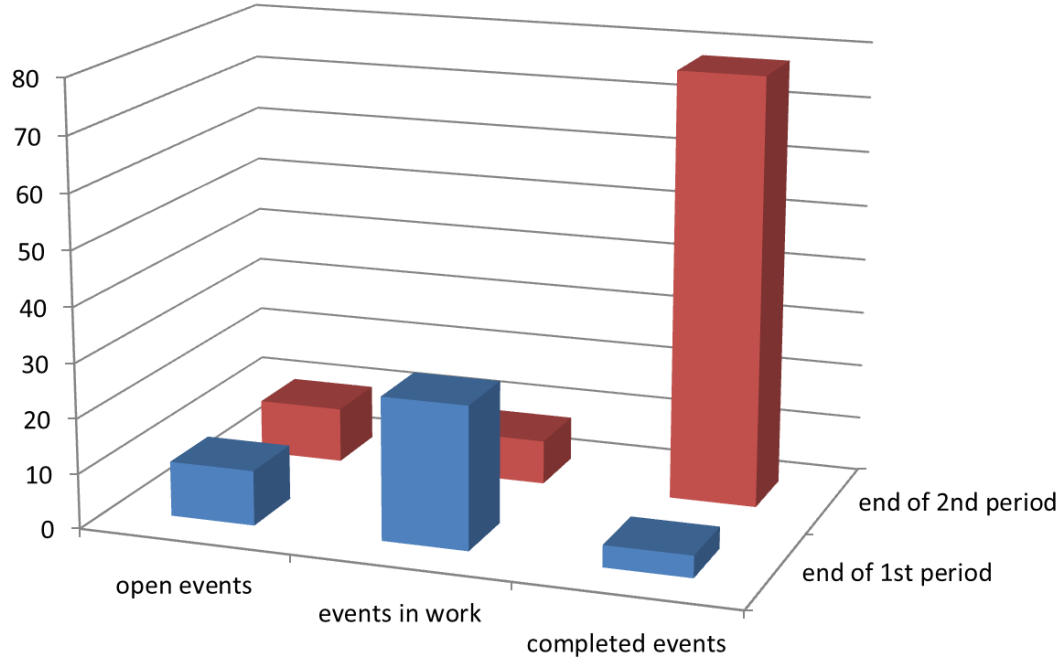

Abb. 5.1: Ereigniserfassung in der 1. und 2. Projektperiode /2/

4.1 Deutsche Ereignisse

In der COMPSIS-Datenbank sind 8 deutsche Ereignisse enthalten. Davon sind 6 Ereignisse im Status „published“, d. h. ihre Bearbeitung und Qualitätssicherung ist abgeschlossen. Zwei Ereignisse sind im Status „open“. Bei einem Ereignis ist die Bearbeitung und Dateneingabe durch die GRS abgeschlossen, aber eine Stellungnahme des Betreibers zu den von der GRS ermittelten Informationen und in der Datenbank vorgenommenen Codierungen steht noch aus. Bei dem anderen Ereignis ist die fachliche Bearbeitung noch nicht abgeschlossen, da die Ursachenklärung durch Hersteller und Betreiber noch nicht beendet ist. Diese beiden Ereignisse sind den anderen COMPSIS-Mitgliedern nicht zugänglich.

Während der Laufzeit des Vorhabens 3608I01310 wurden die deutschen Meldepflichtigen Ereignisse regelmäßig ausgewertet. Dabei wurden folgende Ereignisse als COMPSIS-Ereignisse identifiziert:

- [redacted]

  Dieses Ereignis wurde mit dem Betreiber inhaltlich diskutiert und anschließend als COMPSIS-Ereignis [redacted] in die Datenbank eingegeben. Mittlerweile hat das Ereignis alle im dem Workflow der COMPSIS-Datenbank vorgesehenen Schritte inklusive der Qualitätssicherung durch den Operating Agent durchlaufen, so dass das Ereignis den endgültigen Status „published“ hat.

- [redacted]

  Dieses Ereignis wurde für die Datenbankeingabe entsprechend den COMPSIS Coding Guidelines aufbereitet, übersetzt und als Entwurf in die COMPSIS-Datenbank unter der Nummer [redacted] eingegeben. Dem Betreiber wurde die Bewertung zur Stellungnahme zugesandt. Da noch keine Antwort vorliegt, hat das Ereignis nach wie vor den initialen Status „open“.

- [redacted]

  Dieses Ereignis wurde als COMPSIS-Ereignis identifiziert. Die fachliche Bearbeitung des Ereignisses konnte wegen des Laufzeitendes des Vorhabens nicht abgeschlossen werden, da die Ursachenklärung durch Betreiber bzw. Hersteller noch nicht beendet ist. Die Weiterbearbeitung ist für das angebotene Nachfolgevorhaben (AG 3244) vorgesehen.

Weiterhin wurde das bereits im Jahre 2003 in die damalige, heute nicht mehr gepflegte COMPSIS-Datenbank (MS-Access-2000) eingegebene COMPSIS-Ereignis [redacted] nach den aktuellen Coding-Guidelines /4/ überarbeitet und als [redacted] in die COMPSIS-Datenbank neu eingegeben.

4.2 Auswertung der internationalen Ereignisse

Die nicht-deutschen Ereignisse wurden regelmäßig gesichtet. Dabei wurde insbesondere bewertet, ob eine Übertragbarkeit auf deutsche Anlagen gegeben sein kann. Hierzu wurde ggf. versucht, bei den Betreibern erforderliche technische Informationen zu beschaffen. Dies wurde für alle Ereignisse mit Veröffentlichungsdatum bis 30.05.2011 durchgeführt. Ein Screening der später veröffentlichten Ereignisse ist für das von der GRS angebotene Nachfolgevorhaben (AG 3244) vorgesehen.

Zurzeit werden die COMPSIS-Ereignisse im Rahmen des Lenkungskreises analysiert, um vertiefte Einsichten in primäre Ursachen und beitragende Randbedingungen zu gewinnen. Die Ergebnisse werden im Abschlussbericht des COMPSIS-Projektes für die OECD/NEA /2/, der sich in Bearbeitung befindet, dokumentiert.

Erste systematische Auswertungen, die im Zeitraum dieses Vorhabens 3608I01310 erarbeitet wurden, sind in /1/ enthalten. In ihnen sind Ereignisse berücksichtigt, die bis zum 31.12.2007 in COMPSIS eingespeist wurden. Die Analysen umfassen z. B. die sicherheitstechnische Bedeutung der betroffenen Systeme (Tabellen 3 und 4 auf Seite 23 in Anhang A), der entnommen werden kann, dass bei der Mehrheit der Meldepflichtigen Ereignisse, die als COMPSIS-Ereignis übermittelt wurden, das Sicherheitssystem nicht unmittelbar betroffen war. Nur bei weniger als 20% der Ereignisse waren Einrichtungen betroffen, die Funktionen der höchsten sicherheitstechnischen Kategorie (RPS und ESFAS) ausführen. Weitere quantitative Auswertungen betreffen den Anlagenzustand bei Ereigniseintritt, die Funktion des betroffenen Systems und „lessons learned“, die aus den Ereignissen abgeleitet wurden. In Tabelle 7 bzw. 8 auf Seite 25 in Anhang A sind die aufgetretenen Fehler und die grundlegenden Fehlerursachen dargestellt. Dabei zeigt sich, dass eine große Vielfalt von Fehlern beobachtet wurde (Hardwarefehler, Softwarefehler, fehlerhafte Dokumentation, fehlerhafte Daten usw.), ohne dass sich ein klarer Schwerpunkt abzeichnet. Sowohl systematische Fehler als auch Einzelfehler sind in ähnlicher Größenordnung an COMPSIS-Ereignissen beteiligt. Bei allen diesen

Untersuchungen ist allerdings zu berücksichtigen, dass sie zu einem erheblichen Teil auf noch nicht vollständig bearbeiteten und qualitätsgesicherten COMPSIS-Ereignissen (d.h. Status ist noch nicht „published“) beruhen und somit als vorläufig anzusehen sind. Die weitere Mitarbeit im COMPSIS-Projekt kann zeigen, ob diese Eindrücke bestätigt werden oder im Lichte der deutlich größer werdenden Betriebserfahrung revidiert werden müssen.

Im Folgenden werden beispielhaft drei interessante in COMPSIS-Ereignissen aufgetretene Phänomene angeführt, wobei wegen der Vertraulichkeit der Daten auf die Darstellung von für das Verständnis des Phänomens nicht wesentliche Informationen verzichtet wurde:

Bei dem Austausch einer Baugruppe in einem Leittechnikschrank wurde ein Ausfall einer anderen Baugruppe ausgelöst. Dies verursachte den Ausfall der Erregermaschine des Generators. Die Ursachenerklärung ergab folgende wahrscheinliche Ursache: Eine Stableuchte, die bei den Instandsetzungsarbeiten verwendet wurde, war zufällig so ausgerichtet worden, dass ihr Licht derartig auf das Ende eines Lichtwellenleiters fiel, dass in der an diesen Lichtwellenleiter angeschlossene Baugruppe ausfiel. Als Vorkehrung gegen Wiederholung wurden die entsprechenden Instandhaltungsanweisungen verbessert und Warnhinweise am Leittechnikschrank angebracht.

Bei einem anderen Ereignis wurde eine Reaktorschnellabschaltung dadurch ausgelöst, dass die Speisewasserregelung versagte, nachdem die Klimatisierung der Leittechnischen Einrichtungen ausgefallen war. Als Fehlermechanismus wurde identifiziert, dass sich der Zustand einer von zwei redundanten Stromversorgungen unbemerkt verschlechtert hatte. Während sie bei normalen Bedingungen auslegungsgemäß funktionierte, resultierte die erhöhte Umgebungstemperatur in einer erhöhten Versorgungsspannung. Dies führte zu einer Schutzabschaltung der von dieser Stromversorgung versorgten Einrichtungen. Die Möglichkeit einer fehlerhaften Erhöhung der Ausgangsspannung der Stromversorgungen war bei der Auslegung nicht ausreichend berücksichtigt worden.

Bei einem dritten Ereignis wurde während einer WKP festgestellt, dass ein Temperaturmesssignal plötzlich außerhalb des Messbereichs sprang. Als Ursache wurde die Änderung einer Treibersoftware für eine Baugruppe zum Einlesen von Messwerten identifiziert. In dieser Software wurden bestimmte Variablen als mit einem Vorzeichen behaftete Größen („signed integer“) behandelt, während sie in der alten Version korrekt

als nicht mit einem Vorzeichen behaftete Größen („unsigned integer“) behandelt wurden. Dadurch wurden für einen Teil des Messbereiches falsche Werte übermittelt, während für den anderen Teil, in dem das Messsignal normalerweise liegt, korrekte Werte übermittelt wurden. Deshalb wurde der Fehler im laufenden Betrieb nicht manifest und wurde nicht entdeckt. Derselbe Fehler war bei der zweiter Redundante ebenfalls vorhanden, d. h. es handelt sich um einen gemeinsam verursachten Ausfall (GVA). Der für die Durchführung der Softwareänderung Verantwortliche hatte nicht die möglichen Auswirkungen der Änderung erkannt und deshalb keine vollständige Prüfung veranlasst.

Diese drei Ereignisse zeigen interessante Phänomene, die prinzipiell ähnlich auch in Leittechnikeinrichtungen mit sicherheitstechnischer Bedeutung deutscher Anlagen denkbar sind. Ein vollständiges systematisches Screening der neuen Ereignisse ist für das von der GRS angebotene Nachfolgevorhaben (AG 3244) vorgesehen.

5 Zusammenfassung und Ausblick

In diesem Vorhaben wurde die Mitarbeit der GRS und der ISTec im Unterauftrag der GRS am COMPSIS-Projekt der OECD/NEA durchgeführt.

Beim COMPSIS-Projekt sind eindeutig definierte Prozesse zur Erfassung, Verwaltung und Qualitätssicherung der Daten eingerichtet und haben sich bewährt. Im Laufe der zwei Projektperioden wurden kontinuierlich Daten zu COMPSIS-Ereignissen erfasst. Die Datenmenge erhöhte sich von 40 Ereignissen in der ersten Projektperiode auf 96 Ereignisse zum gegenwärtigen Zeitpunkt.

Mit den bisherigen Projektergebnissen werden Grundlagen für eine Bewertung sicherheitsrelevanter rechnerbasierter oder anderer „intelligenter“ Einrichtungen in Kernkraftwerken geschaffen. Da die Menge der zur Verfügung stehenden Betriebserfahrung noch relativ beschränkt ist, aber rechnerbasierte Einrichtungen in zunehmenden Maße eingesetzt werden, sowie weil rechnerbasierte Leittechnik kurze Innovationszyklen aufweist, ist es aus Sicht der GRS erforderlich, auch in Zukunft am COMPSIS-Projekt mitzuwirken, um den weiteren Zugang zur internationalen Betriebserfahrung mit solchen leittechnischen Einrichtungen in Kernkraftwerken zu gewährleisten.

6 Abkürzungsverzeichnis

COMPSIS	Computer-Based Systems Important To Safety
DP	Data Provider
GVA	Gemeinsam verursachter Ausfall
IFE	Institutt for Energiteknikk
KKW	Kernkraftwerk
NC	National Coordinator
OA	Operating Agent
OECD	Organisation for Economic Co-operation and Development
OECD/NEA	OECD/Nuclear Energy Agency

7 Literatur

/1/ Computer-Based Systems Important to Safety (COMPSIS) Project: 3 Years of Operation, OECD, 2009

/2/ Computer-Based Systems Important to Safety (COMPSIS) Project: Second Period of Operation (2008-2011), 2011 – in Vorbereitung.

/3/ OECD Exchange of operating experience concerning computer-based systems important to safety (COMPSIS) project – Terms and conditions for project operation 2008-2010, 2007 (NEA/SEN/SIN/COMPSIS(2007)1)

/4/ COMPSIS – OECD Exchange of Operating Experience concerning Computer-based Systems Important to Safety at NPPs, Event Coding Guidelines, Version 3.2, OECD, 2008

/5/ http://www.compsis.org

/6/ COMPSIS DataBank (3.2), User Guide (1.0), COMPSIS Clearing House, 2007

/7/ OECD-COMPSIS Quality Assurance Program, OECD, 2009

/8/ OECD-COMPSIS Operating Procedures, OECD, 2009

Anhang A: Computer-Based Systems Important to Safety (COMPSIS) Project: 3 Years of Operation, OECD, 2009

Unclassified **NEA/CSNI/R(2008)13**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **05-Jan-2009**

English - Or. English

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(2008)13
Unclassified

Computer-Based Systems Important to Safety (COMPSIS) Project: 3 Years of Operation (2005-2007)

September 2008

JT03257933

English - Or. English

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

* * *

This work is published on the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full member. NEA membership today consists of 28 OECD member countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made up of senior scientists and engineers, with broad responsibilities for safety technology and research programmes, and representatives from regulatory authorities. It was set up in 1973 to develop and co-ordinate the activities of the NEA concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations.

The committee's purpose is to foster international co-operation in nuclear safety amongst the OECD member countries. The CSNI's main tasks are to exchange technical information and to promote collaboration between research, development, engineering and regulatory organisations; to review operating experience and the state of knowledge on selected topics of nuclear safety technology and safety assessment; to initiate and conduct programmes to overcome discrepancies, develop improvements and research consensus on technical issues; to promote the coordination of work that serve maintaining competence in the nuclear safety matters, including the establishment of joint undertakings.

The committee shall focus primarily on existing power reactors and other nuclear installations; it shall also consider the safety implications of scientific and technical developments of new reactor designs.

In implementing its programme, the CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA) responsible for the program of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also co-operates with NEA's Committee on Radiation Protection and Public Health (CRPPH), NEA's Radioactive Waste Management Committee (RWMC) and NEA's Nuclear Science Committee (NSC) on matters of common interest.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

During the mid 1990s a Task group was formed within the Organisation for Economic Cooperation and Development/Nuclear Energy Agency (OECD/NEA), to exchange information on events involving computer-based systems. In 2005 the OECD/NEA Steering Committee agreed to establish the international Computer-Based Systems Important to Safety (COMPSIS) project to encourage multilateral cooperation in the collection and analysis of data relating to computer-based system events in nuclear facilities. The main objective of the project is to improve the safety of nuclear facilities by utilising operating experience and providing common resources for the analytical framework of qualitative and quantitative assessments.

During the first COMPSIS project period (2005–2007), organisations from Finland, Germany, Hungary, Japan, the Republic of Korea, Slovak Republic, Sweden, Switzerland, the United States and Chinese Taipei agreed to participate.

The lack of computer-based system failure data is one of the major deficiencies in assessments of the risk of computer-based systems in nuclear facilities. To remedy this situation, it was highly important to establish an international computer-based system analysis databank, similar to the one that OECD established for the International Common-Cause Failure Data Exchange/Common-Cause Failure data collection and processing system. The COMPSIS Project is designed to fill the shortage of computer-based system analysis data. This project will enable the identification of the root cause of a computer-based system failure and the effect of the failure and the determination of how the failure could have been prevented. The type of analysis expected from this project is needed to support risk analysis and the regulatory review of computer-based systems.

This report describes the current status of the COMPSIS database after three years of operation and gives some insights into the database structure, coding guidelines, collected computer based system failure events and a first qualitative insight from the data.

ACRONYMS

CNRA	Committee on Nuclear Regulatory Activities
COMPSIS	Computer-Based Systems Important to Safety
CSNI	Committee on the Safety of Nuclear Installations
DICRel	Digital Instrumentation and Control Reliability Group
EGDIC	Expert Group Digital Instrumentation and Control
FIRE	Fire Incidents Data Exchange project
HLD	High-Level Deficiency
I&C	Instrumentation and control
I/O	Input/Output
IAEA	International Atomic Energy Agency
ICDE	International Common-Cause Failure Data Exchange
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IFE	Institute for Energy Technology
LLD	Low-Level Deficiency
MTO	Man-Technology-Organisation
NEA	Nuclear Energy Agency
NPP	Nuclear Power Plant
NS-G	Nuclear Safety Guide
OA	Operating Agent
OECD	Organisation for Economic Cooperation and Development
OPDE	OECD Piping failure Data Exchange project
PSA	Probabilistic Safety Assessment
SG	Steering Group
UI	User interface
WGRISK	Working Group on Risk Assessment

LIST OF FIGURES AND TABLES

1. INTRODUCTION/BACKGROUND

Computer-based instrumentation and control (I&C) systems and components have been available to the nuclear industry since the 1980s, although many licensees have chosen to retain analog-based systems and components in nuclear facility safety systems. As these analog-based systems aged and replacement parts became more difficult to obtain, licensees began to incorporate computer-based I&C systems as replacements. Software-based systems are currently being used and retrofitted in operating nuclear power plants (NPPs) worldwide. The failure modes of both hardware and software in computer-based I&C systems are, to some extent, different from those of the analogous I&C systems. It is also difficult to perceive the structure of a software-based system in a traditional sense.

Additionally, new advanced reactors use computer-based technology in safety systems, and many countries are announcing plans for these new reactor facilities. The number of computer-based I&C safety system applications in the nuclear industry has continued to increase, thereby requiring an increasingly larger proportion of regulatory resources to address computer-based I&C issues in licensing and inspections of nuclear installations. Other industries (i.e., petrochemical, pharmaceuticals, fossil, and train/rail) have accumulated significant experience with computer-based I&C.

The Committee on Nuclear Regulatory Activities (CNRA) and the Committee on the Safety of Nuclear Installations (CSNI) formed a special task group on Computer-Based Systems Important to Safety (COMPSIS) in 1996. The functions of the task group were to (1) collect, analyse, and gather feedback on lessons learned, issues identified, and corrective actions taken from the operating experience with computer-based systems in NPPs in the various participating countries and (2) follow up on the evolving technology as it applies to NPPs and identify new issues that affect the licensing and operation of computer systems in NPPs. The CSNI Working Group on Operating Experience has provided supervisory support to the group.

The work of the task group resulted in a trial database and in guidelines issued as the CSNI report NEA/CSNI/R(99)14, "Computer-Based Systems Important to Safety (COMPSIS) Reporting Guidelines" [7]. However, the task group concluded at the beginning of 2003 that a more comprehensive data collection and in-depth analysis were worth pursuing internationally as an Organization for Economic Cooperation and Development (OECD) joint project. Consequently, the CSNI approved in June 2003 the start of preparations by the Nuclear Energy Agency (NEA) for a joint project in this area. In December 2004, the CSNI endorsed the initiation of the COMPSIS project. In December 2007, the continuation of the COMPSIS project was announced to the CSNI.

Other CSNI efforts related to computer-based systems include the Working Group on Risk Assessment (WGRISK) technical note on computer-based system reliability [1] and the Expert Group on Digital Instrumentation and Control (EGDIC) work, which recommended future actions in the field of computer-based systems. Both papers underline the importance of COMPSIS. Also, based on those works, the CSNI decided in June 2007 to launch the Digital Instrumentation and Control Reliability (DICRel) task group under WGRISK to make recommendations with regard to the reliability assessment of computer-based systems.

2. SCOPE AND OBJECTIVES

Software and hardware faults in safety critical systems are typically rare events and, consequently, most countries do not experience enough fault events to reach a meaningful synthesis. Combined information from several countries, however, is expected to yield enough data for conclusions to be drawn. This model has been proven to work in several other OECD/NEA joint Projects such as the ICDE, OPDE, and FIRE databases. Consequently, the idea behind the COMPSIS Project is to allow countries to collaborate and exchange operating experience in a structured way that increases available computer-based I&C failure data. The ultimate objective is to use this information to improve safety management and the quality of risk analysis of software-based I&C and other equipment.

The detailed objectives of the COMPSIS Project agreed to by the participants are the following:

- Define a format and collect software and hardware fault experience in computer-based, safety-critical NPP systems (hereafter called "COMPSIS events") in a structured, quality–assured, and consistent database.

- Collect and analyse COMPSIS events over a long term so as to better understand such events, their causes, and their prevention.

- Generate insights into the root causes and contributors of COMPSIS events which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences.

- Establish a mechanism for an efficient feedback of experience gained in connection with COMPSIS events including the development of defenses against their occurrence, such as diagnostics, tests, and inspections.

- Record event attributes and dominant contributors so that a basis for national risk analysis of computerized systems is established.

The COMPSIS Project is envisaged as including COMPSIS events in relevant NPP systems, including both software and hardware-related events. The COMPSIS Coding Guidelines (Appendix A) defines a COMPSIS event as follows:

A COMPSIS event is based on a fault, error, or failure or unexpected behavior involving computer-based systems important to safety. The computer-based system could do one of the following:

- Initiate the event and propagate its effects via outputs to other components or systems.

- Initiate but manage the event with no external effects.

- Receive the event from an external input immediately or eventually causing the system to function improperly.

- Receive the event from an external input, causing the system to initiate an event-treatment mechanism (hence "managing" the event).

The importance to safety of a computer-based system can be stipulated in accordance with Institute of Electrical and Electronic Engineers (IEEE) Standard 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations—Description" [3], International Atomic Energy Agency (IAEA) Safety Requirements NS-R-1, or International Electrotechnical Commission IEC 61226, "Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Classification of Instrumentation and Control Functions" [4].

The project also seeks to take full benefit of the experience gained in national event databanks and licensee event report collection systems. They are among the principal sources of information. The Steering Group for the second COMPSIS agreement period (2008–2010) will investigate possibilities for extending the information exchange to events of interest in other NPP records (e.g., maintenance databases, modification requests, operation logs, and service providers' (vendors, etc.) logs), cause consequence, corrective action, and involved systems, and the coding guidelines will be updated accordingly. These efforts are expected to considerably enlarge the available information base.

The database is expected to support model development validation and similar efforts, to identify all types of events and scenarios for inclusion in models for Probabilistic Safety assessments (PSA) to ensure that all mechanisms are accounted for, and to evaluate computer-based I&C system failure occurrence frequencies, if possible.

3. PROJECT INFRASTRUCTURE

The Project Steering Committee (SG), composed of the national coordinators and additional experts of participating countries, manages the COMPSIS Project. During the first three-year period, the participants were AEC/INER/TPC (Chinese Taipei), STUK (Finland), GRS/ISTec (Germany), HAEA (Hungary), JNES (Japan), Consortium of KINS/KAERI/KHNP/KOPEC (Korea), SKI (Sweden) *now SSM*, VUJE (Slovak Republic), HSK (Switzerland), and NRC (United States).

The SG holds all power to make project decisions. The OECD/NEA Nuclear Safety Division provides the secretariat services to the SG and handles financial matters and other types of administration for the project. Each country provides the funding that is generally used to finance the Operating Agent (OA, often also referred to as clearinghouse) activities. The OA ensures the quality assurance and the operation of the database. It also prepares biannual progress reports to the SG. The Institute for Energy Technology (IFE) sector Man-Technology-Organisation (MTO) Safety, in Halden, Norway, acted as OA in 2005-2007. The SG has agreed to retain the services of IFE for the new three-year period (2008–2010).

In cooperation with the OA, the participants prepare project reports for general CSNI distribution. These reports are intended to contain conclusions on the analysis performed whenever major steps of the project have been completed. The COMPSIS SG approves all reports discussing the project data and/or findings. This document, the first COMPSIS Project report, presents the achievements of the initial 3-year period, 2005–2007.

The COMPSIS Terms and Conditions [2], also found in Appendix B, describes in detail the operation of the COMPSIS Project. In particular, it addresses the responsibilities of the participants, the funding, and the distribution of the database. Furthermore, there is an initiative to write the project operating procedures defining the detailed ways the project works for the second agreement period (2008–2010).

4. DATABASE CONTENT AND STRUCTURE

The COMPSIS Project exchanges computer-based I&C system failure data of NPPs covering all operating modes. The goal is all events that involve the failure of computer-based systems and meet each country's reporting criteria should be reported to the COMPSIS database. The database should give a broad perspective of events/incidents occurring in operations with computer-based systems important to safety. The events to be reported to the COMPSIS database must meet the criteria defined in Chapter 2, "Scope and Objectives."

The structure of a computerized system can be very detailed and complicated. The COMPSIS database is designed to handle a wide range of event reports involving both simple and complex systems.

Figure 1 shows the structure of the information content of an event. The data collected are grouped into the following sections:

- **General Description:** The first set of data fields briefly identifies the event. These include the COMPSIS identifier (a string including the country code and, normally, the national identifier of the event) and a short title to quickly identify the nature of the event. The general description includes the main classification of the event according to the high-level deficiency (HLD) characteristics and a short textual description of the event.

- **Facility Information:** Essential information about the facility where the reported event occurred, including the status of operation before and after the reported event. If the identity of the nuclear facility where the event took place should be concealed, an anonymous plant option is available.

- **Data Provider:** The name of the data provider. This person can be contacted for details not reported in the databank.

- **Cause Analysis:** A structured description of the chain of causes that led to the reported event. Each cause is normally associated with a system (see "Involved Systems" below) and represents what happened at that system. Causes are linked together (propagation path) to show how they contributed to the incident. Associated with the propagation path are comments about possible missing or inadequate barriers that permitted the incident to develop.

- **Consequence Analysis:** A structured description of what has been observed and the possible consequences of the reported event.

- **Corrective Actions:** A description of the corrective actions, planned after the event, to avoid a similar occurrence of the reported event and, in particular, to prevent its causes from recurring. More than one corrective action can be associated with a cause. Interventions on barriers can be associated with the source because the barrier is intended to block.

- **Recovery Actions:** A description of the actions performed at the time of the incident in order to control the consequences.

- **Involved Systems:** The list of systems involved in the event. A system can be involved in one or more events in the chain of causes leading to the reported event, in the reported event itself, or in the consequences. Systems can be organized in a hierarchy, indicating that a system represented at a node is a component or module of the system represented at the parent node. Causes and consequences can be connected to a system, meaning that the event occurred at that system.

- **Severity Level and Effects:** Information about the impact of the reported event on plant operation, the level of damages to the facility, damages to the environment, and injuries to people.

- **Lessons Learned:** Synthesis of the main message of the event relevant to safety measures.

- **Attachments:** Relevant documents useful in understanding the event. There is no rule as to which documents should be included as attachments. The selection of documents is at the discretion of the data provider.

The user interface (UI) of the databank provides the means to submit the information groups listed above. The UI allows the data provider to determine the level of detail of the analysis of an event. Cause and consequence analyses aim at describing the history of the reported event in terms of initiating and resulting events. Thus, the actual report should describe the event in relation to its causes and possible or observed consequences.

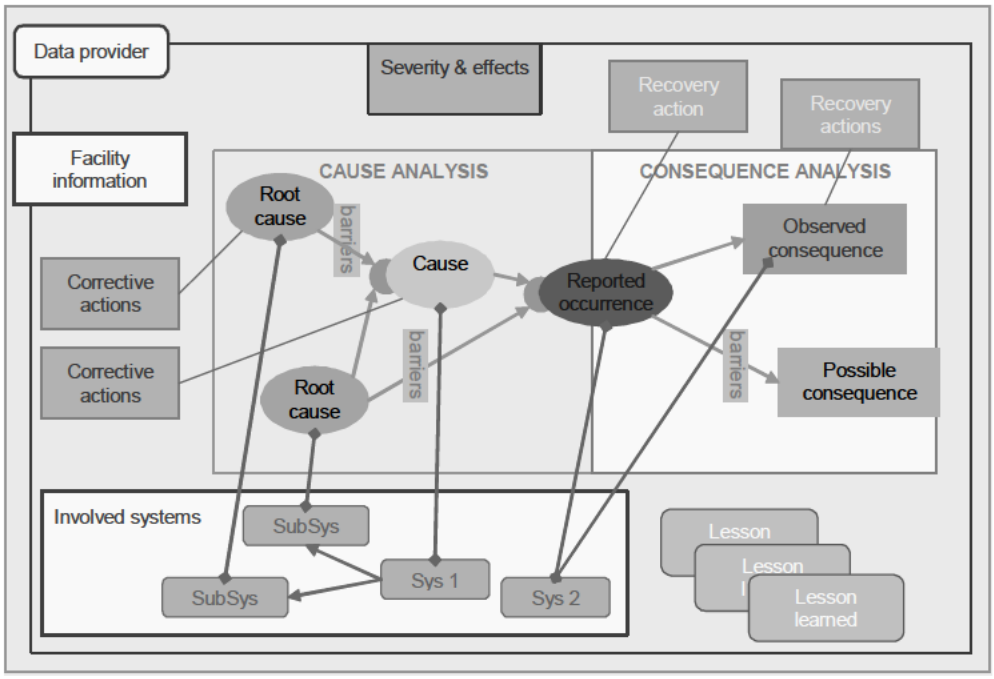

Figure 1: Overview of the structure of information about a COMPSIS event

The coding guidelines describe the content of the database in more detail.

COMPSIS events are stored in a centralised secured database accessible via the Internet (www.compsis.org). Events are input through a Web browser and stored in a relational database (currently MySQL).

5. DATA COLLECTION AND CURRENT STATUS

One challenge in setting up an international database is to ensure a consistent reporting level between countries in order to capture all events meeting the project criteria. Regulatory and utility reporting levels differ between member countries, and the reporting criteria may have changed with time. For events from the past, the database includes for reference the evolution of reporting levels over time. For future events, one objective of the first three-year phase is to define a project reporting level, which will account for the countries' policies while correctly addressing the technical objectives of the project.

With emphasis on data validity and data quality, the COMPSIS coding guidelines have been developed for collecting and classifying computer-based I&C system failure event data to ensure consistent interpretations and applications.

Each national coordinator is responsible for protecting and maintaining the proprietary rights of the information he or she provides to the project, including markings or other indications that such information is confidential. Every country arranges for the protection of proprietary rights. The Operating Agent is also bound to keep the proprietary information secure during the course of the project.

During the period 2005–2007, participating countries have been continuously delivering computer-based I&C system failure data to the COMPSIS Project, beginning with the delivery of the first set of data in August 2005. The first data collection had several objectives:

- To confirm and, if necessary, improve the design and attributes of the COMPSIS database.
- To confirm and, if necessary, improve the coding guidelines against data.
- To test routines for further data collection.

Stable routines for reporting data and data quality assurances are now in place. The Figure 2 below illustrates the COMPSIS events life cycle which is described in Appendix A.

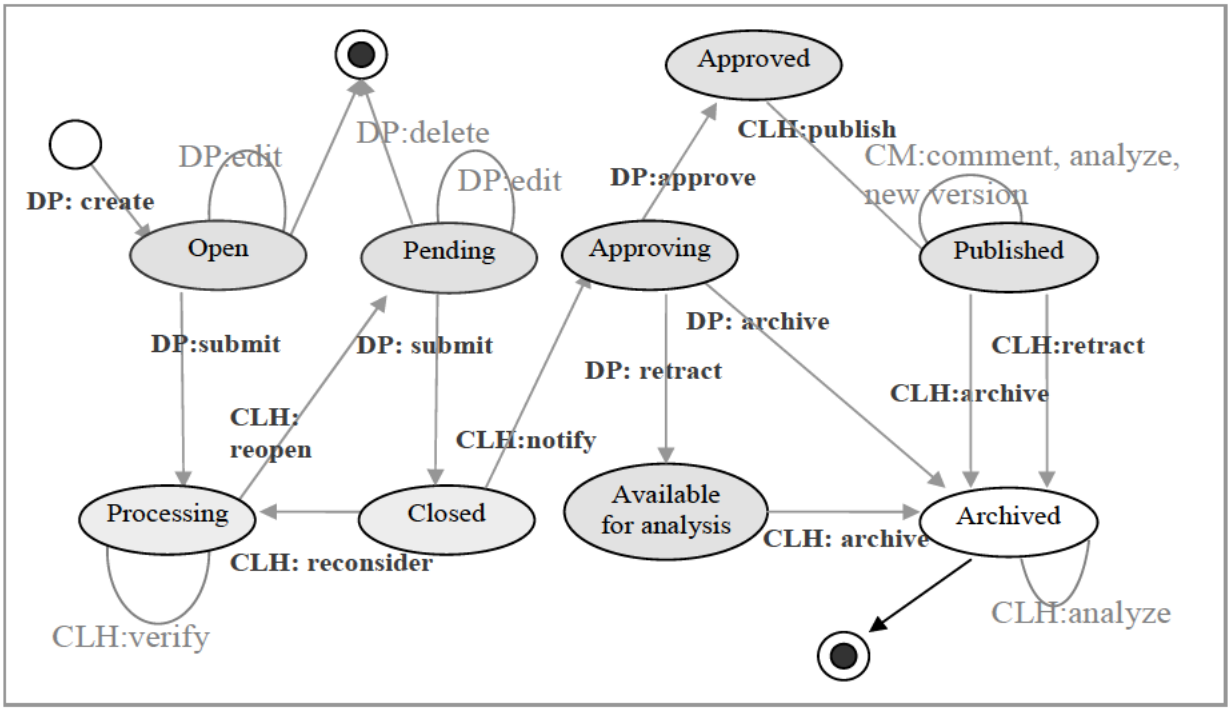

Figure 2: COMPSIS event life cycle
(CLH: Clearinghouse – DP: Data Provider _ CM: COMPSIS Member)

Member countries have delivered additional sets of data to the project. By the end of 2007, the database contained 40 events, 35 of which were being assessed, while five were completed. The quality of all event data is continuously assured as shown by the event life cycle figure. The events are from the period early 2000 to 2005. Although the reporting of events is not exhaustive, the database provides a good platform for starting the analytical phase.

Table 1: Number of events with respect to event life cycle stage

Event life cycle stage	# of events
Open	10
Pending	25
Approving	1
Approved	4

One event in the database serves as an example event (i.e., an anonymous version of real data). The other 39 events include 16 from a boiling-water reactor, 22 from a pressurised-water reactor, and one from a heavy-water-moderated, pressure tube reactor. The status of 35 events as open or pending means that the event data are incomplete and may change before the data are ready to be approved. The data in the following tables should therefore be read with this in mind.

Table 2: Number of events with respect to plant status before the incident

Plant status before incident	Open/ pending	Approved/ approving	All events
Construction			
Refuelling on power			
On power	5	2	7
Full allowable power	14	3	17
Reduced power (including zero power)	1		1
Raising power or starting up	4		4
Reducing power	2		2
Cold shutdown (reactor subcritical and coolant temperature <93°C)	2		2
Refuelling or open vessel (for maintenance)	2		2
Refuelling or open vessel—all or some fuel inside the core	2		2
Start-up test	1		1
No code given	2		2
TOTAL	**35**	**5**	**40**

For each event, *one or more* related systems shall be recorded. These recorded systems shall be classified according to the IAEA and IEC classification. Table 3 and Table 4 show the number of recorded systems versus these classifications. Note that for many of the events in the open or pending category, this information is missing.

Table 3: Number of systems vs. IAEA system safety relevance classes

IAEA safety classes	Open/ pending	Approved/ approving	All systems
Items not important to safety	8	1	9
Safety-related items or systems	11	6	17
Safety systems	2		2
Protection systems	5		5
Safety system support features	1		1
TOTAL	**27**	**7**	**34**

Table 4: Number of systems vs. IEC system safety relevance classes

IEC safety classes	Open/ pending	Approved/ approving	All systems
Not categorised I&C functions	10	1	11
I&C functions of category C	3	1	4
I&C functions of category B	4	5	9
I&C functions of category A	3		3
TOTAL	**20**	**7**	**27**

A system can also be recorded according to a system function; as shown in Table 5.

Table 5: Number of recorded systems per system function

System function		Open/ pending	Approved/ approving	All systems	Recorded lessons-learned reports
--	Control system fuel handling		3	3	1
--	BOP system		1	1	
7.4.1	Protection systems	3		3	2
7.4.1.1	Reactor trip system	1		1	
7.4.3.1	Monitoring	3		3	5
7.4.3.4	Optimisation	1		1	1
7.4.3.5	Control	5		5	
7.4.4	Information systems	2		2	
7.4.5	Limitation system	3	1	4	5
7.4.7.4	Control facilities	2		2	1
TOTAL		**20**	**5**	**25**	**15**

As shown in Table 6, each event is classified according to *one or more* HLDs.

Table 6: Number of recorded HLDs

HLD classification		Open/ pending	Approved/ approving	All HLDs	Recorded lessons-learned reports
--	Not classified	1		1	1
12.1.4	Loss of safety function	1	1	2	
12.1.5	Significant degradation of safety function	2	1	3	6
12.1.6	Failure or significant degradation of the reactivity control	1		1	1
12.1.7	Failure or significant degradation of plant control	4	1	5	
12.1.10	Loss of onsite power	2		2	1
12.1.11	Transient	8		6	
12.1.11.1	Power transient	8	1	9	1
12.1.11.2	Temperature transient	1		1	
12.1.11.3	Pressure transient	2		2	1
12.1.11.4	Flow transient	4		4	2
12.1.14	Fuel-handling incident	3	3	6	2
12.1.16	Security, safeguards, sabotage, or tampering incident	1		1	
TOTAL		**38**	**7**	**45**	**15**

Each event can be classified according to *one or more* causes. Table 7 shows these causes classified according to a list of low-level deficiencies (LLDs).

Table 7: Number of recorded LLDs

LLD classification	**Open/ pending**	**Approved/ approving**	**All LLDs**
Hardware failure type	9		9
Systematic failure	8		8
Non systematic failure	5		5
Software failure/fault type	2		2
Primary fault		2	2
Documentation (comments, messages)	4		4
Syntax (spelling, punctuation, typos, instruction formats)		1	1
Interface (procedure calls and references, I/O, user formats)	2		2
Checking (error messages, inadequate checks)		2	2
Data (structure, content)	6	2	8
Function (logic, pointers, loops, recursion, computation, function defects)	8		8
System (configuration, timing, memory)	1	1	2
Secondary fault	1		1
Command fault	4	4	4
TOTAL	**46**	**12**	**58**

In 16 cases, these LLDs are also classified as root causes, as shown in Table 8.

Table 8: Number of recorded root causes

LLD classification	**All LLDs**	**All root causes**
Hardware failure type	9	1
Systematic failure	8	1
Non systematic failure	5	
Software failure/fault type	2	1
Primary fault	2	2
Documentation (comments, messages)	4	1
Syntax (spelling, punctuation, typos, instruction formats)	1	
Interface (procedure calls and references, I/O, user formats)	2	1
Checking (error messages, inadequate checks)	2	1
Data (structure, content)	8	4
Function (logic, pointers, loops, recursion, computation, function defects)	8	2
System (configuration, timing, memory)	2	
Secondary fault	1	
Command fault	4	2
TOTAL	**58**	**16**

Finally, for each event, it is possible to record a lesson learned. By the end of 2007, the project has recorded 17 such lessons-learned reports. In some cases, the lessons-learned report has been linked to an HLD and/or a system function, as shown in Table 9.

Table 9: Number of lessons learned and listing of associated HLDs and system function

System function	**HLD**	**Number of lessons-learned reports**
Control system for a fuel handling device	Fuel-handling incident	1
Protection system	Loss of on-site power	1
Protection system	Power transient	1
Monitoring	Not classified	1
Monitoring	Significant degradation of safety function	4
Optimisation	Failure or significant degradation of the reactivity control	1
Limitation system	Significant degradation of safety function	2
	Failure or significant degradation of plant control	
	Power transient	
Limitation system	Pressure transient	1
Limitation system	Flow transient	2
Control facilities	Fuel-handling incident	1
TOTAL		**15**

6. ANALYSIS OF DATA AND OBSERVATIONS

6.1 Overview

Because of the progress of computer-based technology and obsolescence of analog control equipment, many nuclear systems have been upgraded from analog to computer-based systems. The newer computer-based systems utilise technology with sensors, actuators, and software. These systems apply the advanced human-machine interface design and the software control technology to take the place of analog controls and instruments in conventional control rooms which require operators to watch many indicators, monitor the pump/valve status, and operate hard-wired actuator switches to keep the systems operated within a normal range or deal with abnormal conditions. Replacing these systems with computer-controlled equipment can often reduce the operator's burden and maintenance costs. Although computer-based design offers many advantages, some characteristics inherent in software and hardware integrated systems, human-machine interfaces, and project management may cause failure events during operations. COMPSIS collects data from its member countries on related events that may affect the safety of NPPs. This chapter describes the conceptual model and processes for the pilot analysis of COMPSIS events.

6.2 Preliminary study on root causes and consequences analysis

In a preliminary study performed in June 2007 to identify root causes and simplified consequences analysis, was adopted the simplest form of a single cause for a reported event. After analysing 27 events, it was concluded that there were 7 root causes and 13 causes. The analysis used the low-level deficiency code of the event Coding Guidelines (CG) to categorise those causes. More detailed descriptions of the root causes and consequences analysis appear in the following subsections. Further research will investigate cases where several causes contribute to an event.

6.2.1 Root causes

6.2.1.1 Design defect

Design defect cause is one of the most impact factors for computer-based safety system in these findings. There are two causes in the design defect cause. They are software design defect and hardware design defect. The main reason leading to this cause is negligence concerning system requirements. The undesired result is that many more efforts are needed to make up for the previous mistakes in the requirement analysis phase.

(1) **Software design defect:** In this cause, the authors found that many problems were from designers not taking into account all conditions or operation modes; for example, in the following year 2000 time display, there are out of scope or error parameters:

(2) **Hardware design defect:** The same observation made for software design defect applies here. This cause focuses on hardware design errors or insufficient requirements analysis. For example, the wrong size or length is given in an event:

6.2.1.2 Configuration management

Traditionally, the goal of configuration management (CM) programs is to ensure system consistency throughout the operational life cycle phase, particularly as changes are being made. Software

configuration management (SCM) can be regarded as a subset of general CM in computer-based systems. Similarly, SCM is a process that is involved with identifying configuration items, changes control (including impact analysis), status accounting, and auditing. Its aims are to maintain integrity and traceability of the configuration items throughout the software development life cycle.

However, this study found that impact analysis and safety evaluation were often ignored in the real world. For example, some events are induced by neglecting the comparability with other functions when adding a new function. In addition, the records of change and test reports were missed in the software maintenance environment. More specific descriptions are listed below:

(1) **Impact analysis:** For a complex system, impact analysis should identify all configuration items which will be impacted before any configuration item is changed.

(2) **Status accounting/auditing:** The authors recommend that an SCM team be responsible for managing and controlling the status of a change request in a nuclear power plant. Any updates to change requests and software baselines should be performed under authority of the SCM team. The assessment result, such as reject, accept, or pending, will be recorded as the change request status and returned to the owner of the change request by the SCM team.

6.2.1.3 Communication

Communication is becoming more and more important in computer network environments. There are three causes in this root cause:

(1) **Electromagnetic interference:** In this cause, a firmware (programs store on nonvolatile storage (e.g., ROM or PROM)) of communication module emitting a continuous electromagnetic signal to interrupt communication was found.

(2) **Other interference:** Some false signals or light interruptions in the normal data communication were found.

(3) **Component failure:** Some component failures led to the communication card being disabled.

6.2.1.4 Hardware failure

Hardware failure is one of the most common causes in the study findings, which identified three types of hardware failure—material aging problem, grounded interference, and hardware fault. The two main reasons leading to this cause are the hardware fault and the aging problem. However, there is no effective method to prevent this from happening again.

(1) **Hardware fault:** The study found that most hardware faults come from the controller, circuit, or input/output card. In some cases, this fault is very hard to find because of the intermittent nature of the faults.

(2) **Grounded interference:** The grounded test should be performed before the installation or replacement of new devices or equipment.

6.2.1.5 Routine maintenance

Routine maintenance means periodic testing such as the daily or weekly system test. However, the study found a test data consistency problem in the COMPSIS databank.

(1) **Test validation:** It is recommended to follow standard operation procedure and use software toolkit for routine maintenance work.

6.2.1.6 Quality assurance defect

This cause represents the manufacturing defect from the manufacturer or vendors. The purpose of quality assurance is to help the manufacturer to ensure product quality. Moreover, quality assurance should be performed in parallel with the product manufacture.

(1) **Factory acceptance testing:** Besides the need for a well-defined quality assurance program, factory acceptance testing also should be conducted carefully before shipment to the customer.

6.2.1.7 Human factor

In this human factor cause, the study found that some events stem not only from human factors but also from other causes. However, personnel can avoid this type of event by taking more care.

(1) **Operation error:** In spite of there being defects in system design, personnel can avoid operation error by being more attentive.

(2) **Procedure missing:** In spite of there being deficiencies in software management, personnel can avoid them by establishing a standard procedure.

6.2.2 Consequences analysis

In this consequences analysis, the authors referenced the system description section of the CG and adopted three layers of system structure—application, communication, and process and the system element to represent observed and possible consequences. The results appear in Table 10. In addition, the INER also provided the analysis results of recovery actions, as well as corrective actions, as Table 11 shows. (Recovery actions are intended to control the consequence; corrective actions can avoid the reported event and its consequences.)

Table 10: Observed and possible consequence

Root cause	Structure layer	System element
Design defect	Application	Application software, System software
Configuration management	Application	Application software, System software
Communication	Communication, Process	Interface card
Hardware failure	Process	Actuator, Sensors/Transmitter
Routine maintenance	Process	Actuator, Sensors/Transmitter
Quality assurance defect	Process	Application software, Actuator
Human factor	Application	Human-machine interface

Table 11: Recovery and corrective actions

Root cause	Recovery and actions	Corrective actions
Design defect	Enable diverse protect mechanism	Redefine system requirement
Configuration management	Regression test	Fulfill software engineering concepts and practice
Communication	Repair or replace	Perform environmental test in advance
Hardware failure	Repair or replace	Redundancy design and implementation
Routine maintenance	Reload or redo	Follow procedure or use tool
Quality assurance defect	Retest or validation	Fulfill integrated test
Human factor	Improve alarm design	Enhance training and knowledge management

6.3 Preliminary observations

When this study was performed, the COMPSIS databank included only 27 events. The number is still too small to allow further research such as quantitative analysis. Therefore, instead of attempting to use statistics analysis, a causal learning model is proposed for analysis of COMPSIS data. Figure 3 shows the basic concept of an abduction analysis model.

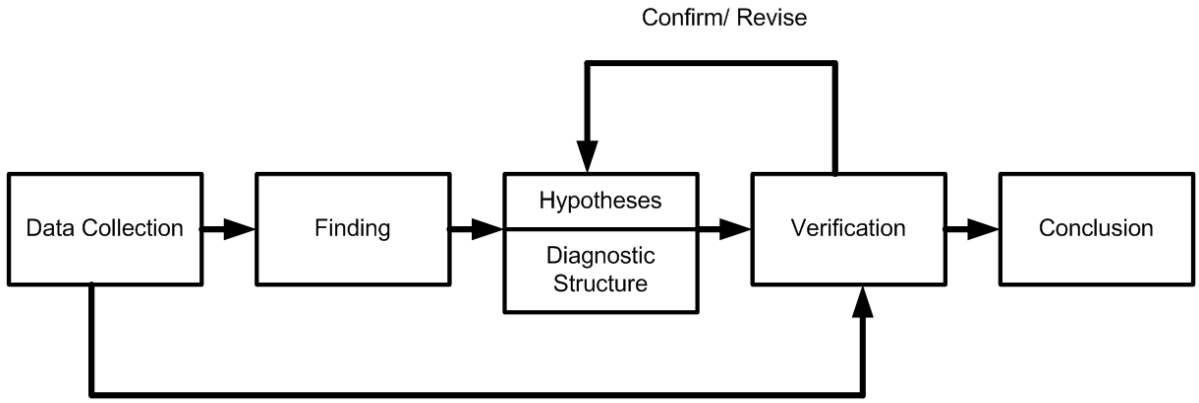

Figure 3: Concept of causal learning model

This model entails five processes, which include data collection, finding, hypotheses/diagnostic structure, verification, and conclusion. The central role of the model is the learning process. This will be described in more detail below.

After the detailed information about events is gathered from the COMPSIS databank (in the first process), a qualitative analysis is used to identify appropriate classifications and causal (cause/effect) relations. Then, the analysts adopt ontology methodology and an ontology tool to express explicitly the complicated event of unambiguous concepts and structured information. Therefore, the output of the second process is a diagnostic-structure graph. In the third process, the analysts will formulate a few hypotheses based on the result of qualitative analysis. Moreover, these hypotheses need to be further verified by the coming evidence. If there is any conflict, hypotheses should be modified or redefined. In other words, a recursive loop exists between hypotheses and new evidence. Finally, the above refined processes allow some conclusions to be made.

Nuclear safety systems depend heavily on computers, networks, and software. Therefore, more and more events are being reported in the COMPSIS databank. The lessons learned so far from these 27 events are listed below:

- Initial findings show that design defect, configuration management, and hardware failure are the three main root causes.
- A well-defined requirement analysis and consistent specification can improve system safety and reliability.
- Safety systems should emphasise simple design, easy maintenance, and procedures for change.
- Improvement of component materials can mitigate the effects of aging hardware.

Qualitative analysis emphasises the identification of root causes and impact analysis. On the other hand, quantitative analysis provides a clear picture by displaying a number. The two types of analysis should be complementary to achieve the best analysis results.

During the initial qualitative analysis, the simplest form of single cause and a reported event were adopted to identify root causes and simplify consequences analysis. With limited time, the analysis addressed only 27 events of the databank (before July 2007). To improve analysis precision, more events are needed for further study.

Further research offers many challenges, such as finding ways to deal with the complicated form that includes combinatorial, temporal, and synchronised relations between root causes and events, and the "many-to-many" relation between systems and events. An ontology-based approach suggests a direction for future research. Ontology is a formal structure to support knowledge sharing and re-use. For this project, it could be used to express explicitly the complicated event of unambiguous concepts and structured information, thus enabling the exploration of causal patterns and event trends in the future.

7. CONCLUSION

The objective of the COMPSIS Project is improving the safety of nuclear facilities by utilising operating experiences and providing common resources for analytical framework of qualitative and quantitative assessments. The first period of the COMPSIS-Project has been concentrating on the development of clear definitions, coding guidelines, data base structure and user interface of the data base. In this period 10 countries took part in the project.

During the first period, the participating members reported 40 events that are collected in the data base. The reporting that have been performed during the first period has to be seen as testing of the user interface and data base structure. The established guidelines and Web-based infrastructure is appropriate to gain further data. A first attempt has been performed for qualitative analysis showing some results obtained from the collected events during the first period Procedures for modifications of guidelines, data base structure and user interface have been proved and further enhancement is expected. Especially rules for and collection of "low-level data" should be taken into account.

During the next period which has started in January 2008 the project shall be focused on reporting of events and starting up the analysis of data. Although, the main objective should be directed to qualitative analysis and results, discussions on possibility for more quantitative analysis should start.

This project will continue to enable the identification of the root cause of a computer-based system failure and the effect of the failure and the determination of how the failure could have been prevented. The type of analysis expected from this project is needed to support risk analysis and the regulatory review of Computer-based systems.

REFERENCES

[1] Nuclear Energy Agency, "Software-Based System Reliability—A Technical Note by the Working Group on Risk Assessment (WGRISK)," NEA/SEN/SIN/WGRISK, 2007.

[2] Nuclear Energy Agency, "COMPSIS Terms and Conditions for 2008–2010," NEA/SEN/SIN/COMPSIS(2007)1.

[3] Institute of Electrical and Electronic Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations—Description," IEEE Standard 603-1991.

[4] International Electrotechnical Commission, "Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Classification of Instrumentation and Control Functions," IEC 61226, 2005.

[5] International Atomic Energy Agency, "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants," IAEA Safety Standards Series, No. NS-G-1.3.

[6] H. Thane, "Safe and Reliable Computer Control Systems—Concepts and Methods," Royal Institute of Technology (KTH), Stockholm, 1996.

[7] Nuclear Energy Agency, "Computer-based system important to Safety (COMPSIS) - Reporting Guidelines" NEA/CSNI/R(99)14, Rev.1.

APPENDIX A

COMPSIS

OECD (Organisation for Economic Cooperation and Development) Exchange of Operating Experience Concerning Computer-Based Systems Important to Safety at Nuclear Power Plants

Event Coding Guidelines

A - FOREWORD

The objective of the present guidelines is to help the user to prepare a Computer-Based Systems Important to Safety (COMPSIS) report on an event so that important lessons learned are efficiently transferred to the COMPSIS database. The principles behind developing the guidelines are to some extent similar to the procedure chosen by the Incident Reporting System. However, the COMPSIS database is designed for computer-based systems and instrumentation and control equipment. The project's ultimate purpose is to collect and disseminate information on significant safety-critical events involving such systems and equipment at nuclear power plants so that such events can lead to conclusions and lessons learned.

June 2008

COMPSIS Steering Group

COMPSIS Operating Agent

A - HISTORY OF CHANGES

Date	Version	Comment
September 2007	3.2	• Introduction of History of Changes. • Implementation of changes required during the 5th Steering Group (SG) meeting in Stockholm, Sweden o Revision of the event life cycle • Minor changes in the text to harmonise graphical user interface and coding guidelines (CG). • Insertion of identification of all event parameters in order to make references from the user guide to the CG. • Removal of country codes and national codes to a separate section, no longer part of Section 5. • Added more comments on the fields of Section 5. • Complete revision of Section 5.1 • Addition of an experimental and incomplete Section 5.2 (to determine if it can be useful). • Revision of definition of basic data structure and basic event. • Section 19 to collect codes previously in Section 5.
October 2007		• Implementation of changes required during the 6th SG meeting in Garching, Germany.
November 2007		• Example added in the appendix
June 08	3.3	• Added missing content to Section 7.3 "Classification of Systems According to Safety Relevance" (according to COMP Action 6-6, 7th SG meeting Paris, France). • Replaced "Clearing House" with "Clearing House/ Operating Agent", and CLH with CLH/OA. • Editorial changes (according to external and SG review)

A - TABLE OF CONTENTS

A - ABBREVIATIONS

BWR	Boiling-Water Reactor
CFR	Code of Federal Regulation
CG	Coding Guidelines
CLH/OA	Clearinghouse / Operating Agent
COSS	Computerised Operation Support Systems
COMPSIS	Computer-Based Systems Important to Safety
CSNI	Committee on the Safety of Nuclear Installations
GUI	Graphical User Interface
HMI	Human-Machine Interface
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
I/O	Input/Output
IRS	Incident Reporting System
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
NPP	Nuclear Power Plant
NS-G	Nuclear Safety Guide
NUREG/CR	Nuclear regulatory Commission/Contractor Report
OO	Object Oriented
PDF	Portable Document Format
PIE	Postulated Initiating Event
ROM	Read Only Memory
PROM	Programmable Read Only Memory
PWR	Pressurised Water Reactor
SG	Steering Group
UI	User Interface

A-1. INTRODUCTION

The objective of the document is to guide the users in reporting events to the Computer-Based Systems Important to Safety (COMPSIS) database. The document consists of a set of coding guidelines for reporting the events to be included in the COMPSIS database with add-on verbal help and examples to aid in the coding effort. In the user interface (UI), this help feature may be called on as hypertext. The coding guidelines are based on standardised descriptions (found in documents of the International Atomic Energy Agency (IAEA) and the International Electrotechnical Commission (IEC), among others) of instrumentation and control (I&C) and computer-based systems important to safety and employed at nuclear facilities for operation, control, monitoring, analysis, optimisation, and maintenance purposes. Among the available standards, some focus not only on the computer-based devices and systems as a product of a process, but also the development process itself (the system life cycle). The rationale is that events initiated by the computer-based system or affecting the computer-based system[1] depend not only on current functional, operational, or structural properties of the systems, but also on different stages of the development process where these properties were defined, specified, implemented, validated and verified, categorised, and possibly later modified. In other words, such descriptions account for evolutionary and thus time aspects closely related to the nature of the events and the way they should be handled.

The events to be reported to the COMPSIS database should be as encompassing as possible and include all data sources available in the participating member countries (e.g., licensee event reports, vendor databases, plant maintenance databases). The aim is that all reports including computer-based systems that meet each country's reporting criteria should be reported. The database should give a broad picture of events and incidents occurring in the operation of computer-based systems.

The guidelines should help to collect and compare data from different countries and different types of nuclear power plants (NPPs). Thus, the guidelines help to classify the attributes of the reported events into predefined classes.

By using the predefined guidelines, participants can transfer important lessons learned to the COMPSIS database in the most efficient and validation- and verification-friendly manner. The guidelines are believed to contribute to better collection and dissemination of information on significant events that are related to the computer-based systems important to safety at NPPs. This will in turn enable more efficient and useful analyses, conclusions, and lessons learned based on the events. Although the guidelines focus on the content of the information to be provided in the report, a sample report format is provided in Appendix A.

[1] In the following, the term "system" also includes single devices.

A-2. TERMS AND DEFINITIONS

The definitions for a COMPSIS event and a basic data structure are unique to the COMPSIS database. All

COMPSIS event

A COMPSIS event is based on a fault, error, or failure or unexpected behaviour involving computer-based systems important to safety. The computer-based system could do one of the following:

- Initiate the event and propagate its effects via outputs to other components or systems.
- Initiate but manage the event with no external effects.
- Receive the event from an external input immediately or eventually causing the system to function improperly.
- Receive the event from an external input, causing the system to initiate an event-treatment mechanism (hence "managing" the event).

Systems important to safety in accordance with different standards

The safety importance of computer-based systems can be characterized in either of three ways[2] in the COMPSIS coding guidelines:

1) According to Institute of Electrical and Electronic Engineers (IEEE) Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations—Description," a safety system is a system that is relied upon to remain functional during and following design basis events to ensure (a) the integrity of the reactor coolant pressure boundary, (b) the capacity to shut down the reactor and maintain it in a safe shutdown condition, or (c) the capability to prevent or mitigate the consequences that could result in potential offsite exposures.

2) According to IAEA Nuclear Safety Guide (NS-G)-1.3, "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants," the systems and items important to safety consist of safety systems and safety related items or systems.

3) A computer-based system important to safety can be a system performing functions of category A, B or C in accordance with IEC 61226, "Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Classification of Instrumentation and Control Functions."

[2] The definition of "safety systems" in IEEE 603-1991 is in accordance with Title 10, Section 50.2, "Definitions," of the U.S. *Code of Federal Regulations* (10 CFR 50.2). Electrical equipment (and thus also computer based systems) is classified as "Class 1E". Therefore in the U.S. *Code of Federal Regulations* and in the IEEE standards, safety-related electrical equipment is synonymous with class 1E equipment. The definition of safety related systems in IAEA NS-R-G-1 and in IEC standards is different, in that safety related systems are of lower importance than safety systems but still important to safety.

Accident

An accident is an undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss.

Availability

Availability is the probability that the system will be functioning correctly at any given time. Note that availability is usually quantified by "1- MTTR/MTTF", where MTTR is the "mean time to repair" the system and MTTF is the "mean time to failure."

Basic data structure

A basic data structure consists of a set of attributes commonly used to describe causes, consequences and reported events.

Basic event

To show the causal evolution of the COMPSIS event causes, consequences, and reported event can be described and connected in a causal graph. Basic event is a collective name to indicate a cause or a consequence or the reported event. In Figure 3, each of the coloured ovals represents a basic event (i.e. something that has happened or been observed such as a reported event, cause, root cause observed consequence, or something that may happen, such as a possible consequence).

Computer-based system

A system whose functions are mostly dependent on, or completely performed by, microprocessors, programmed electronic equipment, or computers.

Dependability

Trustworthiness of the delivered service (e.g. a safety function) such that reliance can justifiably be placed on this service. *Reliability, availability, safety,* are attributes of dependability.

Error

The difference between a computed, observed, or measured value (or condition) and the specified, intended, expected or theoretically correct value (or condition). As an example, a difference of 30 meters between a measured result and the expected result (correct result) can be regarded as an error.

Failure

Failure is the inability of a system or component to perform its required functions within specified performance requirements.

Fault

A fault can be defined as the following:

- A defect in a hardware device or component; for example, a short circuit or broken wire
- An incorrect step, process, or data definition in a computer program.

The temporal behaviour of faults can be categorised into three groups:

- **Transient faults:** occur once and subsequently disappear. These faults can appear because of to electromagnetic interference, which may lead to bit-flips.
- **Intermittent faults:** occur and disappear repeatedly. These faults can happen when a component is on the verge of breaking down or, for example, because of to a glitch in a switch.
- **Permanent faults:** occur and stay until removed (repaired). Such a fault can be a damaged sensor or a systematic fault, as in the case of a programming fault.

Hazard

A hazard is a state or a set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident (loss event). A hazard is defined with respect to a system's or a component's environment.

A hazard has two properties:

- Severity (the worst accident that can happen).
- Likelihood of occurrence.

The two properties combined are called the hazard level.

Human failure

This refers to a human behaviour (or action) that could lead to other failures, faults, or errors for a given system.

Reliability

Reliability is the probability that a piece of equipment or component will perform its intended function satisfactorily for a prescribed time and under stipulated environmental conditions.

Note that reliability is often quantified by MTTF.

Risk

Risk is the hazard level combined with (1) the likelihood of the hazard leading to an accident (sometimes called danger) and (2) the hazard exposure or duration (sometimes called latency).

Safety

Safety is the freedom from accidents or losses. Safety is here meant to be absolute. Although nothing can be totally safe it is more constructive to aim for total safety. Note that the fault tolerance discipline distinguishes between the human action (a mistake), its manifestation (a hardware or software fault), the result of the fault (a failure), and the amount by which the result is incorrect (the error).

A-3. EVENT SELECTION FOR REPORTING

The events to be reported to the COMPSIS database should be based on the national reporting criteria in the participating member countries. The aim is that all reports including computer-based systems that meet each country's reporting criteria should be reported. The database should give a broad picture of events/incidents occurring in the operation of computer-based systems important to safety in NPPs.

A-4. FORMALIZATION OF THE COLLECTED INFORMATION

COMPSIS events could have been stored in the databank as textual reports (for example in portable document format (PDF) and shared as simple documents. The coding guidelines could have been formed sufficient to guide the data providers to fill in the content of the document describing the event. Instead, a more structured and formal approach has been chosen for defining the COMPSIS events, specifying the coding guidelines, and developing the databank. The main reasons for this approach are to encourage and guide the event reporters to collect as much information about the events as possible, and to improve further analysis of the reported events, so that more efficient and feasible means can be suggested to prevent or handle the events. Although requiring fully formalized event reports would have eased not only manual but also automated analysis of the events, a trade-off solution has been chosen, as it is believed to be more feasible and user friendly, and thus more likely to result in actual use of the databank. Therefore, the solution contains many free text fields and optional fields, so that the event reporter (data provider) can select case by case the most suitable level of formalization.

The advantages of having a more formal description of the event can be observed through three different activities:

1) **Submitting an event:** A UI can be provided to support the user in entering all the required information and to offer the possibility of adding optional information. The completeness of the report can be automatically checked. Also, the validation process will have the advantage of relying on the structured data.
2) **Searching for events:** While textual search today is quite advanced, it still has several limitations. Structured data are still fundamental for more effective retrieval, and for the possibility of searching by different categories (for example, looking for events involving a certain type of system).
3) **Subsequent analysis:** Automatic analysis can be applied to structured data. The observations mentioned for searching are even more important for analysis, where the queries to retrieve data to look for correlations must be generated by an "intelligent" engine, much less flexible than a human being, and the result must be precise, essential and unambiguous.

COMPSIS events concern digital I&C and computer-based systems. In the following, a description of the systems in focus is given. Next, the COMPSIS event is analysed and its main components presented. Finally, the data structure used to describe these components is explained. In the graphical user interface (GUI) database overview, the headline for each COMPSIS event is displayed.

4.1 System description

Since computer-based systems can be designed in many different ways, only two examples of system decomposition are given. Figure 1 illustrates a complex computer-based system assumed to consist of an application layer that includes (among others things) the control, alarm, and monitoring subsystems; a communication layer that includes the network functionality; and a process layer that provides input/output (I/O) access to the process hardware. Figure 2 illustrates a different way to depict the structure of a less complex computer-based system.

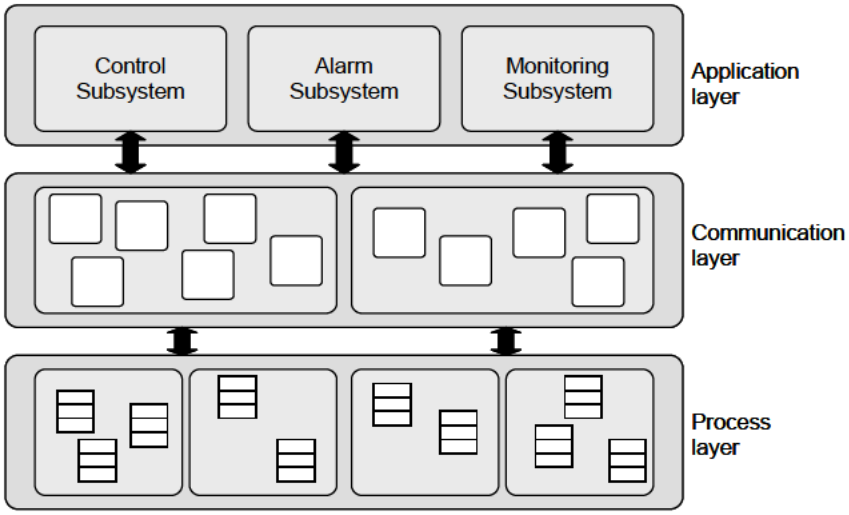

Figure 1: An example of a complex computer-based system

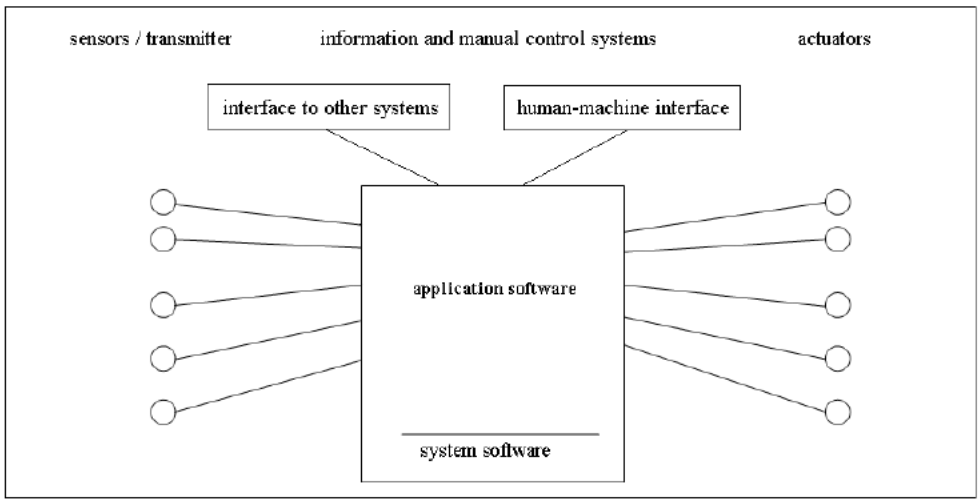

Figure 2: An example of a less complex computer-based system

4.2 COMPSIS events

A COMPSIS report about a COMPSIS event consists of the following groups of information:

- **Basic description**: it includes the title, a classification according to the high-level deficiency characteristics, and a detailed description of the event.
- **Facility information**: essential information about the facility at which the reported event occurred, including the status of operation before and after the reported event.
- **Involved systems**: the list of systems involved in the event (The systems can be involved in one or more events in the chain of causes leading to the reported event, in the reported event itself, or in the consequences.).
- **Cause analysis**: a description of what caused the reported event or the chain of causes leading to the event.

- **Consequence analysis**: a description of the observed and possible consequences of the reported event.
- **Corrective actions**: a description of the corrective actions planned after the event to avoid a similar occurrence of the reported event and, in particular, to prevent its causes.
- **Recovery actions**: a description of the action performed in order to control the consequences.
- **Severity level and effects**: information about the impact of the reported event on plant operation, people, the surrounding environment, and facilities.
- **Lessons learned**: a summary of the main lessons learned from the event.
- **Attachments**: a list of relevant documents useful in better understanding the case.

The User Interface (UI) of the databank provides a means to submit the information groups listed above. Chapter 5 describes each group of information in detail and in terms of classes and their attributes.

The next section explains the activities related to the analysis of reported events and thus the principles applied to define a format for event reporting. Following that is a discussion dealing with the life cycle of the event from the time it is created (reported) for the first time until it is subject to publishing or archiving.

4.2.1 Analysis of the COMPSIS event

A COMPSIS event is analysed in four steps. Cause and consequence analyses aim at describing the history of the reported event in terms of initiating and resulting events. Thus, the actual report should describe the event in relation to its causes and possible or observed consequences. The following figure exemplifies this principle.

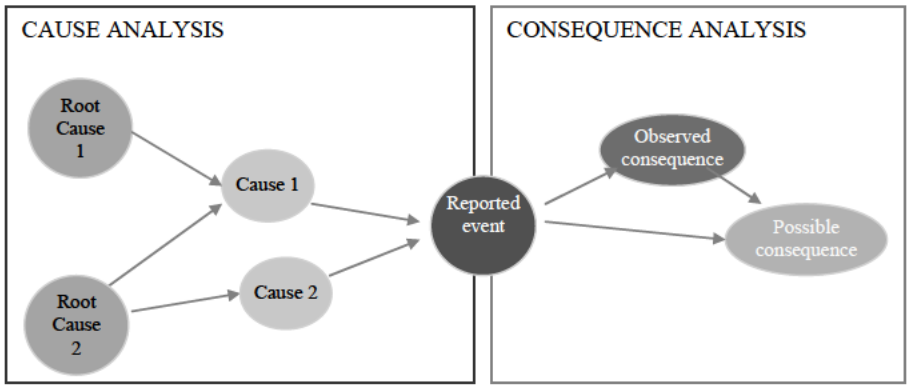

Figure 3: An abstract example of the chain of events behind the COMPSIS event. On the left, the initiating events are identified during a cause analysis, and on the right, the resulting events are identified during a consequence analysis

In the simplest case, a cause analysis can result in the following figure:

Figure 4: A simple example of a reported event and its single cause

When neither the cause analysis (no causes have been identified) nor the consequence analysis (no consequences have been identified) are not performed the description of the reported event is still present. The COMPSIS event consists of the reported event.

Several causes can contribute to an event, giving rise to at least three types of relationships between the causes, referred to as "cause condition" in the UI:

1) The combinatorial relationship (for example "Root Cause 1 **and** Root Cause 2 give rise to Cause 1").
2) The temporal relationship (for example "Root Cause 1 happens before Root Cause 2 in order for Cause 1 to occur").
3) The synchronised relationship (for example "Root Cause 1 lasts for at least 2 hours after Root Cause 2 has occurred in order for Cause 1 to occur").

While each event (cause, root cause, reported event, consequence) is often associated with a system, its subsystems, modules, or components, the general term "system" is used in this set of coding guidelines and the COMPSIS databank so that the event reporters (data providers) can themselves decide, based on the system in focus, the most suitable level of details. Also, a "many-to-many" relationship can exist between systems and events. Furthermore, the propagation of events from one system to another can normally be ascribed to broken barriers or missing barriers. Therefore, the UI allows the submittal of information about broken or missing barriers, when such information is available.

Figure 5 illustrates the link between the events (causes of the reported event) and additional information about systems and barriers, clarified through a cause analysis.

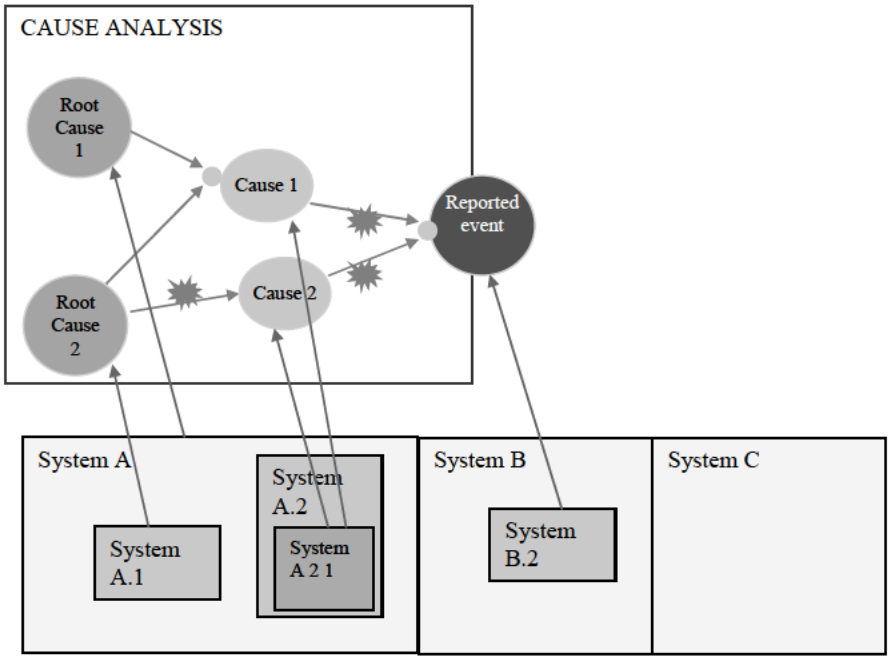

Figure 5: The link between the events, systems, and barriers, clarified through a cause analysis

Similar information can be extracted during a consequence analysis. In addition to the identification of the possible and observed consequences, the analysis includes specification of recovery actions (to control the consequences), as well as corrective actions (to avoid the reported event and thus its consequences). Corrective actions can be associated with causes of the reported event.

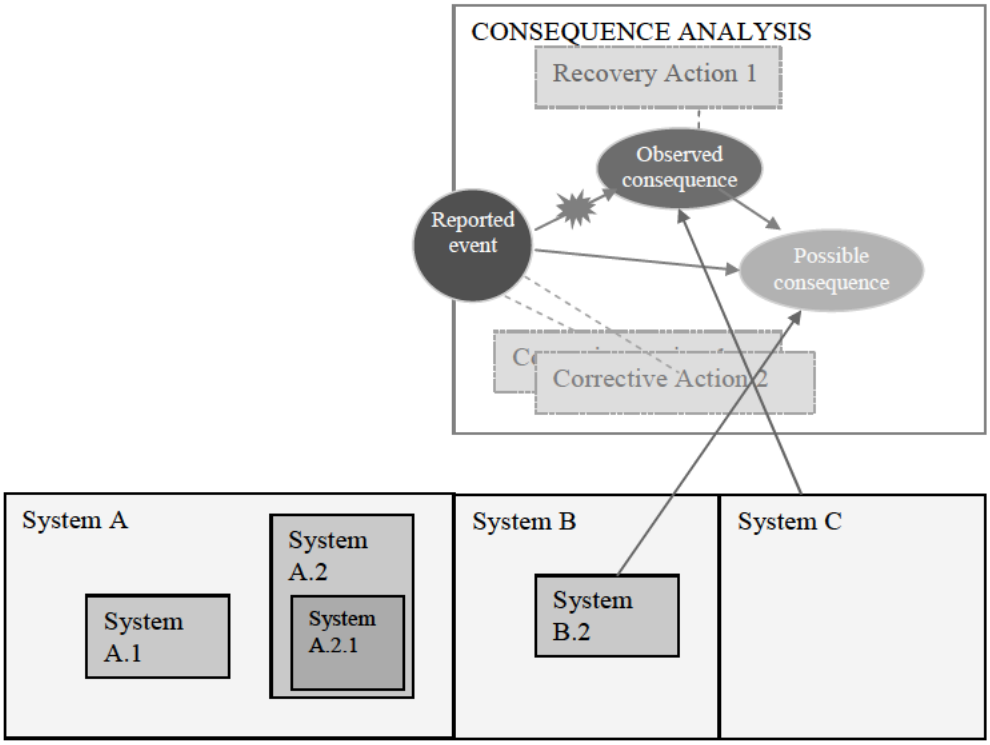

Figure 6: Exemplifying information collected through a consequence analysis

Safety as a dependability factor is a central issue for this set of guidelines and the COMPSIS databank. Therefore, the UI facilitates a description of the impact(s) and their severity levels on the plant operation, people, surrounding environment, and facilities. Safety analysis can be carried out in parallel with a cause and consequence analysis. In practice, a consequence analysis includes a safety analysis as an integrated part.

4.2.2 COMPSIS event life cycle

A COMPSIS event starts its life when an event reporter/data provider creates the event (Figure 7). The event then enters the state Open. The data provider can edit the event information how many times as he/she wishes to, with no time limit. Only the data provider sees the event, and only he/she can modify it. The data provider is also free to create several *drafts* of the event report subject to submission.

At a certain point the data provider submits the event to the Clearinghouse/Operating Agent (CLH/OA) for verification of the reporting according to the COMPSIS coding guidelines (this document), and the event enters the state Processing. The event is from now on visible to the other COMPSIS members. At this stage, the CLH/OA checks the information for quality assurance, and only the CLH/OA can edit the event. However, such editing should take place only after confirmation from the data provider. Whenever the information is unclear or incomplete, mandatory parts are missing, or a part has been modified, the CLH/OA should inform the data provider. Note also that any notification emails between the CLH/OA and the data provider should not contain data because of security reasons.

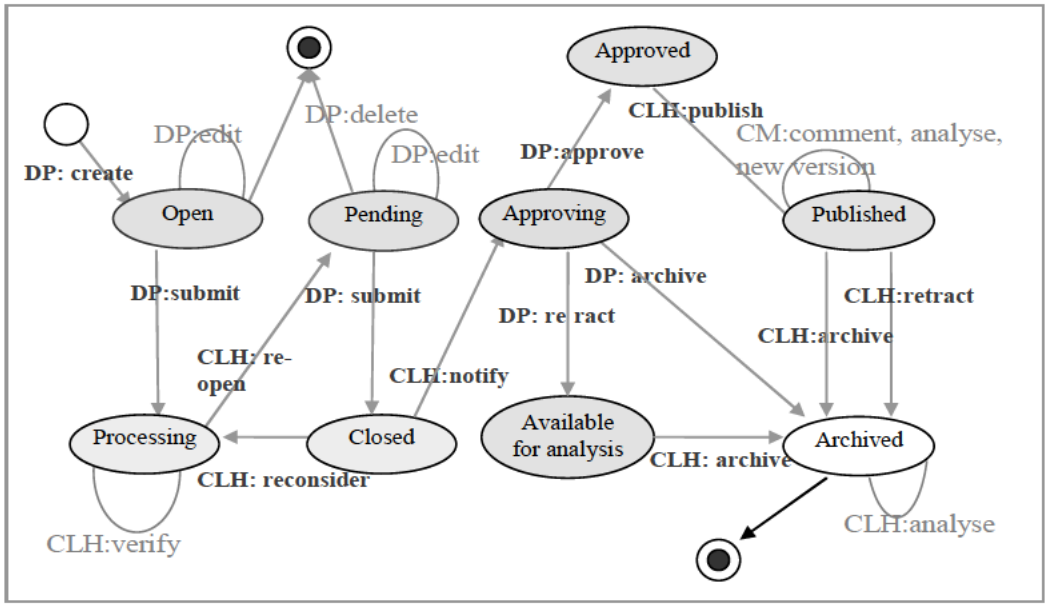

Figure 7: COMPSIS event life cycle in terms of a state diagram

After the CLH/OA has checked the information, the event is reopened (re-open in the figure) so that the data provider can edit it. The event then enters the state Pending where it is subject to edit. The data provider is again free to create several drafts of the event report subject to submission. In this state, the data provider can also delete the event (the history of the event takes into account any form in which the event existed). The main difference between the Open and Pending states, is that in the Pending state, the event is visible to the COMPSIS members.

Once the data provider submits the event from Pending, the event will enter the state Closed. In this state, the CLH/OA reconsiders the event. If there are problems (e.g., mandatory parts are missing), the event re-enters the state of Processing.

Otherwise, if the verification process is successful, the CLH/OA notifies the data provider and the event enters the state Approving. The event cannot be modified in this state, as the CLH/OA is only waiting for the final authorisation to publish the event. When the event is in the state Approving, the data provider can still retract the publication of the event. The event remains then in the databank as Available for Analysis. In this state, the event cannot be viewed by anyone else, and only the CLH/OA can perform analysis on the event, unless the data provider wishes the event to be archived. Being in the state Archived, the event is no longer visible or available for analysis. Explicit requests to see archived events can be made following a specific procedure, but the explanation of this procedure is outside the scope of this set of coding guidelines. In any stage during the life cycle of the event, the event can be viewed by its provider.

When the data provider approves the event, it enters the state Approved, ready to be published. Once in the state Published, the event is visible to all individuals with access permission to the COMPSIS databank. The event can from here be subject to further analysis. At this stage, any such individual can comment on the event, or a new version of the event can be created. Once published, the event can still be archived or retracted, on request of the data provider, the CLH/OA performs the action

Should new information about a COMPSIS event arrive after the event has been published, a new COMPSIS event as a new *version* of the previous description needs to be created. The new version, as a separate COMPSIS event, will have its own life cycle. Only the original data provider or whoever is now filling his/her role can create a new version of an event.

When a COMPSIS event goes through the COMPSIS event life cycle (Figure 7), the traceability of the changes should be recorded. In order to give immediate information about the state of an event, the event listing on the portal marks an event with a background of the same colour as the life cycle state (Figure 8). The transactions from state to state (i.e., the history of any event updates) is visible to all COMPSIS members (Figure 9).

Event List

Click on the *Compsis Event identifier* to see a dynamic summary; on the *Title* to get a printable report; on *Status* to see the history

Events currently under editing cannot be viewed (On the S-DB events in status: open, pending). The same apply to events that have been deleted.
On the V-DB the content of events accessible only to analysis or archived is not visible

Event Identifier	Date	Event Title	Plant name	Reactor type	Status
BWR					
DE/DE-28/2004/129	2004/10/04 occurrence	Damaged fuel element handle	Gundremmingen-C	BWR	pending
DE/DE-13/2005/078	2005/11/14 occurrence	Unexpected motion of the refuelling platform	Brunsbuettel	BWR	pending
DE/DE-16/2005/008	2005/01/26 occurrence	Temporary disturbance of Symphony modules in the operational control system (balance-of-plant (BOP) system)	ISAR-1	BWR	pending
PWR					
DE/DE-27/2004/019	2004/02/12 occurrence	Finding revealed by an in-service inspection relating to the adjustment of the emergency travel limit switch of the refuelling machine	GROHNDE	PWR	open

<< Beginning of the list Previous Page Next Page

Figure 8: Event list showing each event in a colour corresponding to the colour of the state

Log of transition on the COMPSIS event:

Event ID: *DE/DE-28/2004/129*

Date	From	To	Comment
2007/05/01	open	open	default creation data
2007/05/05	open	processing	before the 5th meeting
2007/07/04	processing	pending	Observations: --- In Details: Dependency is given as "systematic fault". In Root Cause: Dependency is given as "systematic fault". Evaluation: --- "systematic fault" is not in the CG 3.0. Should be added in next update.

Figure 9: Traceability of the history of a COMPSIS event

A-5. CONCEPTUAL DESCRIPTION OF THE DATA STRUCTURE

A COMPSIS event is represented in the databank as a structured collection of information. The conceptual description of the data structures and their relations is provided in the following objects or entities, each of which consists of a set of attributes. As described previously, the entity basic data structure illustrates a collection of attributes inherited by several other entities.

In the UI, mandatory attributes are marked with a red square. In this coding guideline, mandatory attributes are marked with an "M" in the far-left column, or to the left of the field name (entity). Where one or more, but not all, attributes are mandatory, this is indicated with an "M*." If the attribute is optional, this is indicated with an "O." Where the mandatory attribute is to be picked from a pre-defined list of field values, it is indicated where this list is restricted, or if free text is optional. In some cases, an attribute can be optional, but once the attribute is created, other attributes become mandatory. This situation is indicated with an "M+" and explanatory text.

Chapters 6-12 include the codes used in the COMPSIS databank. For the codes in Chapters 6-12, it is mandatory to also record the confidence level of the information provided. For a specified value, the field values available are "confirmed", "expert judgement," and "reported." When a value cannot be specified, the available field values are "unknown" or "not relevant." In addition to the confidence level, a note can help to explain why that value has been assigned. If none of the predefined values is suitable, a new one can be suggested. As far as possible, it is better to define a new value than simply use the category "other". In the UI, the set of value/new value/note/confidence level is indicated as "CG Assessment."

For an overview of parameter organisation, please refer to 5.2.

5.1 Describing a COMPSIS event

In this section, all the parameters used for describing a COMPSIS event are organised in Tables. In the next section, the same information is summarised in diagrams.

5.1.1 COMPSIS event

The general information about the COMPSIS event is given in the table below.

Table 1: COMPSIS event main information

No.	Optional/ Mandatory	Attribute	Type/Example/Comments
1	M	COMPSIS Event Identifier	String (*Country*/*Plant code*/*National Event Identifier*) (e.g. "US/US-336/95-013-00/") *Country* (see Section 19.1). *Plant code* is to be selected from a list of plants for that country. *National Event Identifier* is to be given as a unique value.
2	M	Title	Title of the event. A simple, short text that indicates what the COMPSIS event is about.

No.	Optional/ Mandatory	Attribute	Type/Example/Comments
3	M	High-Level Deficiency Characteristics	For possible values, see Section 12.1. It can have more than one value.
3a	M	Reported event	A link to an entity described in Table 2. It is the 'reported event' in the cause graph (Figure 3) presented in the previous Section "4.2.1 Analysis of the COMPSIS event". This link represents the possibility to add detailed information about the COMPSIS event (see Section 5.1.2)
3b	M	Normal/Low level Event	An event can be classified as a normal reported event, or a low-level event. A low-level event should be marked by a flag. Default value is "normal"
4	O	Additional Information	Free text.
5	M	Computer-Based Systems	List of [Entity Reference] System (see below) of relevance in the COMPSIS event description.
6	M*	Cause Analysis	[Entity Reference] Cause Analysis (see Section 5.1.5).
7	O	Consequence Analysis	[Entity Reference] Consequence Analysis (see Section 5.1.9).
8	O	Corrective Actions	[Entity Reference] Corrective Actions (see Section 5.1.8).
9	O	Recovery Actions	[Entity Reference] Recovery Actions (see Section 5.1.11).
Severity and Effects:			
10	M	Summary	A text describing briefly the impact of the COMPSIS event.
11	M	Severity Level	Severity level (Section 13) has three attributes impact on people, impact on facility, and impact on environment.
12	M	Effect on Operation	Effect on plant operation (see Section 11).
Plant Information:			
13	M	NPP	[Entity Reference] NPP (see below).
14	M	NPP OpertStat	Operational status of NPP when event occurred (see Section 19.3).
15	M	Plant Condition	[Entity Reference] Plant Condition (see Section 5.1.4).
Other:			
16	O	Attachments	List of [Entity Reference] Attachments (see Section 5.1.16).
17	O	Lessons Learned	List of [Entity Reference] Lesson Learned (see section 5.1.15).

5.1.2 Basic data structure

The following table summarises the set of parameters that can be used to describe the basic events (causes, consequences, reported event: the circles) in the cause graph (Figure 3) presented in the previous section "4.2.1 Analysis of the COMPSIS event". A COMPSIS event has always at least the "reported event".

This entity is the basis for other entities (cause and consequence entities), meaning that these entities inherit all attributes from the basic data structure and add new attributes specific to each entity (see definition of basic data structure and basic event in Chapter 2).

Only the name and description are mandatory for all the basic events. The other attributes here marked as "M" are optional for causes and consequences, and mandatory only for the "reported event." In the GUI, the set of information associated with the reported event is also indicated as "event detailed description."

Table 2: Basic data structure for basic events

No.	Optional/ Mandatory	Attribute	Description
1	M	Name	String. Few words to indicate what the event is about. It is given, and cannot be changed for, "reported event."
2	M	Description	Text. For the "reported event," this is the description of the COMPSIS event as a whole.
3			
Dates: At least one of the following must be supplied for the "reported occurrence," preferably Occurred, then Discovered, then Reported. "Occurred" means the time when the failure mechanism was introduced to the system (or became safety relevant if several stages and contributors exist). In addition, the time for the event detection can be recorded.			
4	M*	Occurred	Format: YYYY/MM/DD
5		Discovered	Format: YYYY/MM/DD
6		Reported	Format: YYYY/MM/DD
7	M	Low-Level Deficiency Characteristics	For possible values, see Sections 12.2.1–12.2.5. It is possible to specify more than one value.
8A	M	Event Detection	For possible values see Section 16.
8B	O	Symptoms	Free text to describe the symptoms of the event.
Failure description: The behaviour of the failure is described with three different attributes.			
9	M	Temporal Behaviour	For possible values, see Section 12.2.6.
10	M	Dependency	For possible values, see Section 12.2.7.
11	O	Further Comments	Free text to add information about the failure. For example, other classification criteria, not generally accepted, like "Digital to Digital" or

No.	Optional/ Mandatory	Attribute	Description
			"Analogue to Digital."
Involved system: Associating a system with an event is not mandatory, but once it has been introduced, the related features are mandatory. Remember that it is always possible to specify the "unknown" and "not relevant" values.			
11	O	Involved Computer-Based System	[Entity Reference] System (see Table 13) This is a link to the system associated with the basic event. It is one of the systems listed in Table 1 No. 5.
12	M	Comp.System Prior Status	For possible values, see Section 10.2.
13	M	Comp.System Posterior Status	For possible values, see Section 10.2.
14	M	Failed Safety Functions	List of safety functions that failed (see Section 8). This is a subset of the list defined in Table 2 No. 6.
15	M	Life Cycle Stage	Life cycle stage in which fault mechanism was introduced (Section 6.1).
16	M	Life Cycle Supporting Activities	Life cycle supporting activities in which the cause was introduced (Section 6.2).
Causal relationship contribution: This section aims to describe how the input basic events contributed to the basic event in term of timing, synchronisation, and logical (AND, OR) combination. This information is meaningful in the context of a causal graph (see 5.1.5) or consequence graph (see 5.1.9)			
17	O	Logic	Text in the form of a logic formula describing how the causes to this event combine. For example, if A, B and C contribute to this cause, "A and B and C happened, if only one of them occurred the failure would not be propagated."
18	O	Synchronisation	Text describing the sequence of the input causes. For example, if A, B and C contribute to this cause, "A and B happened before C started."
19	O	Timing	Text describing the timing in more in detail. For example, if A, B and C contribute to this cause, "C started 3 hour after A terminated."

5.1.3 Nuclear power plant

Note that the information about existing NPPs or other nuclear facilities of interest is not inserted in the databank by the data provider, but by the CLH/OA.

Table 3: Nuclear power plant

No.	Optional/ Mandatory	Attribute	Description	Example
1	M	Country	String (Country Code, see Section 19)	US
2	M	Plant Code	String (Identifier)	US-336
3	M	Name	String (Name of NPP)	Millstone-2

No.	Optional/ Mandatory	Attribute	Description	Example
4	M	Facility Type	String (Acronym, see below)	PWR
5	O	Operator	String (Acronym)	NNEC
6	O	Vendor	String (Acronym)	GE
7	O	CapNET	Integer	878
8	O	CapGROSS	Integer	903
9	M	OpertStat	Operation state of the facility at the present time. For possible values, see Section 19.3.	In operation
10	M	StartOper	Date format: YYYY/MM/DD	1975/01/12
11	M	ShutDown	Date format: YYYY/MM/DD	

5.1.4 Plant[3] condition

The goal is to state the general condition of the facility at the moment of the COMPSIS event.

Table 4: Plant Condition

No.	Optional/ Mandatory	Attribute	Type
1	O	Additional Features	Free text. It is possible to give other information here about the plant that are relevant to a better understand the event.
2	M	Prior Plant Status	Plant status before the event or the incident (see Section 10.1).
3	M	Posterior Plant Status	Plant status as a result of the event/after the incident (see Section 10.1).

5.1.5 Cause analysis

The goal of this section is to provide a way to report the analysis of the causes behind the event. The cause analysis can be reported simply as text, or a causal graph can be exploited to organise the description of causes and identification of root causes.

Table 5: Cause analysis

No.	Optional/ Mandatory	Attribute	Description
1	M	Summary	Free text. A summary of the cause analysis. The cause analysis can be performed in detail, creating the causal graph. In this case, this field contains a summary of what the causal graph describes. Otherwise, when the detailed analysis is not available this field is used to give a general indication of the causes behind the event. In the worse cases, the field can indicate that no cause analysis is available. For example, it surely exists but, for

[3] In the UI, the terms "plant" and "facility" are used as synonyms.

No.	Optional/ Mandatory	Attribute	Description
			some reason, it should not be in the COMPSIS database.
2	O	Cause Graph	List of [Entity Reference] Causes (see Section 5.1.6). List of [Entity Reference] Barriers (see Section 5.1.14) among two causes. All together define the causal graph, describing in detail what happened and the cause of the event. One cause can have many (root) causes contributing to it, as it can contribute to many other intermediate causes and to the "reported event."

5.1.6 Cause

A cause (an element of the causal graph) is described by the attributes of Table 2 plus the one in the next table. **Note that it is not mandatory to create a cause, but once a cause is created, the attributes indicated with "M+" are required**. This means that when a cause is created, at least one link to another cause (or reported event) must exist.

Table 6: Cause

No.	Optional/ Mandatory	Attribute	Description
1	M+	Root cause	(Boolean) true if the cause is a root cause, false otherwise (an intermediate cause)
2	M+	Cause links	List of [Entity Reference] Cause a list of links to the other causes (if not root cause) that directly provoked it a list of links to events that are directly provoked by it Furthermore: For each link, it is possible to describe the barriers adding a [Entity Reference] Barriers (see Section 5.1.14).

5.1.7 Corrective actions overview

The goal is to give an opportunity to describe the actions that were taken after the COMPSIS event to mitigate the causes or to avoid similar events in the future. The data provider can choose to describe the corrective action in a free way or in a more structured way.

Table 7: Corrective actions overview

No.	Optional/ Mandatory	Attribute	Description
1	M	Summary	Free text. When the data provider opts for a general description, it should be placed here. In the case of a more detailed description, which exploits the next field, a short summary is advisable in this field.
2	O	Corrective Action Links	List of [Entity Reference] Corrective Action (see Section 5.1.8).

5.1.8 Corrective action

Defining a corrective action is not mandatory, **but when an entity of this type is created, but once a corrective action is created, the attributes indicated with "M+" are required**.

Table 8: Corrective actions

No.	Optional/ Mandatory	Attribute	Description
1	M+	Name	String. A mnemonic name, giving an immediately idea about the kind of action.
2	M+	Correction Type	For possible values, see Section 14.
3	M+	Description	Free text to describe the action.
4	O	To Prevent	List of [Entity Reference] cause/COMPSIS event (see above) that this corrective action should prevent.

5.1.9 Consequence analysis

Once the cause analysis is performed and corresponding corrective actions found, the consequences can also be described. Like the cause analysis, the consequence analysis can be performed in a simple way by giving a description or in a more structured way by listing and linking the consequences, both observed and potential.

Table 9: Consequence analysis

No.	Optional/ Mandatory	Attribute	Description
1	M	Summary	Free text. When the data provider opts for a general description, it should be placed here. In the case of a more detailed description, which exploits the next field, a short summary is advisable in this field.
2	O	Consequence Graph	• List of [Entity Reference] observed and possible Consequences (see Section 5.1.10). • List of [Entity Reference] Barriers (see Section 5.1.14) among two consequences. Together, these define the consequence graph, describing in detail what happened after the "reported event," how the failure could have been propagated, or other consequences observed. One consequence can have many basic events contributing to it, as it can contribute to many other basic events.

5.1.10 Consequence

A consequence (an element of the consequence graph) is described by the attributes of Table 2 plus the ones in the next table. **Note that it is not mandatory to create a consequence, but once a consequence is created, the attributes indicated with "M+" are required.** This means that when a consequence is created, at least one link to another basic event (or reported event) must exist.

Table 10: Consequence

No.	Optional/ Mandatory	Attribute	Description
1	M+	Observed	(Boolean) True if observed, false if possible.
2	M+	Consequence Links	List of [Entity Reference] Consequence • a list of links to the other basic events that directly are consequences of it • a list of links to basic events that are directly provoked by it Furthermore: • For each link, it is possible to describe the barriers adding a [Entity Reference] Barriers (see Section 5.1.14)

5.1.11 Recovery action overview

The goal is to give an opportunity to describe the actions that were taken immediately to mitigate the consequences and to return to a normal situation during the COMPSIS event. The data provider can choose to describe the recovery action in a freer way (filling in just the first field below) or in a more structured way, defining a list of recovery actions and associating them with a consequence.

Table 11: Recovery action overview

No.	Optional/ Mandatory	Attribute	Description
1	M	Summary	Free text summarising the action(s) performed to recover to a normal situation.
2	O	Recovery Action Links	List of [Entity Reference] Recovery Action (see below)

5.1.12 Recovery action

Defining a recovery action is not mandatory, but once a recovery action is created, the attributes indicated with "M+" are required.

Table 12: Recovery action

No.	Optional/ Mandatory	Attribute	Description
1	M+	Name	(text)
2	M+	Recovery Type	(see Section 15)
3	M+	Description	(text)
4	M+	To Limit Impact of	[Entity Reference] Consequence/COMPSIS event (see above) for which this recovery action should limit impact

5.1.13 Computer-based system

Defining a system is not mandatory. **Once a data provider decides that defining a system is useful for the event description (and hence create an entity), the attributes indicated with "M+" are required.** It is possible to define more systems, and for each system, the data in the following Table can be supplied.

Table 13: Basic data about computer-based systems involved in the event

No.	Optional/ Mandatory	Attribute	Description
1	M+	Name	String. It could be the actual name of the system or another name, more intuitive name that could help to explain the event.
2	M+	Description	Free text with information on for example, platform, manufacturer, series model.
3	M*	Safety Relevance according to IAEA	(see Section 7.1)
4		Safety Relevance according to IEC	(see Section 7.2)
5		Safety Relevance according to IEEE 603	(see Section 7.3)
6	O	National classification	A free text to indicate the classification of the system according to the system used in the nation where the event occurred.
7	M+	Functions	(see Section 7.4)
8	M+	Safety Functions	(see Section 8)
9	M+	Layers	(see Section 9.1)
10	M+	Elements	(see Section 9.2)

5.1.14 Barriers

Barriers are defined between two basic events (Table 2). They aim to describe the problem in barriers preventing the propagation of the failure. The plant barriers described in one instance (Nos. 1 and 2) are the plant barriers that allowed the propagation of failure between the two indicated basic events. Similarly, when the basic events are associated with a system, the system barriers between computer-based systems (Nos. 3 and 4) should be associated with those systems.

For example assume that a root cause (root cause 1) has been defined and it is linked directly to the "reported event." Root cause 1 involves System A, while the reported event happened in System B. The system barrier description (Fields 3 and 4) indicated at the top of Figure 10 should describe a problem in possible (real) barrier(s) between System A and B.

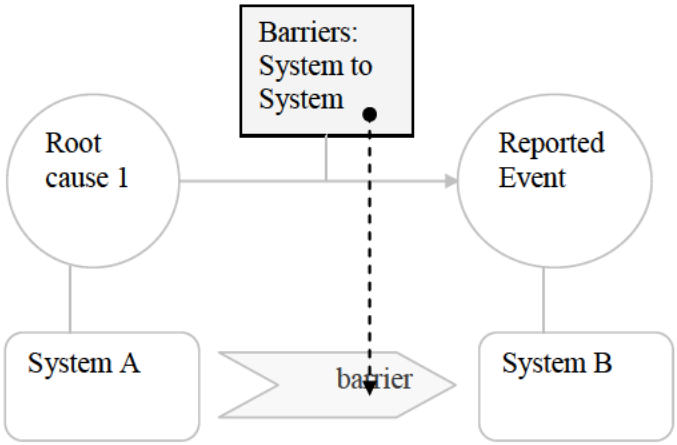

Figure 10: Description of problem of system barrier between two basic events

Table 14: Information about the barriers that allowed causes to propagate

No.	Optional/ Mandatory	Attribute	Description
1	O	Broken Barriers in the Plant DiD	Text. The barriers (tests, inspections, checkups, software/hardware measures (redundancy, lockouts, lockins, interlocks, etc.)) which should have captured/contained the fault.
2	O	Missing Barriers in the Plant	Text. Barriers that should have been in place in the plant to capture/contain the fault.
3	O	Broken Barriers in the Computer-Based DiD system	Text. The barriers (tests, inspections, checkups, software/hardware measures (redundancy, lockouts, lockins, interlocks, etc.)) which should have captured/contained the fault).
4	O	Missing Barriers in the Computer-Based System	Text. Barriers that should have been in place in the computer-based system to capture/contain the fault.

5.1.15 Lesson learned

One or many lessons learned can be found to help in understanding the case and planning for prevention. Instead of giving one text field in which to write freely about the lesson learned, the guidelines organise the lesson learned into a list of simpler lessons.

Lessons learned are optional, **but once a lesson learned is created, the attributes indicated with "M+" are required.**

Table 15: Lesson learned

No.	Optional/ Mandatory	Attribute	Description
1	M+	Name	A meaningful name for the lesson learned.
2	M+	Content	A description of what has been learned.

5.1.16 Attachment

Any document that helps in understanding the case is welcome. There is no limit on the number of attached documents, nor constraints on the format or content: the selection is within the discretion of the data provider. **Attachments are optional, but once an attachment is created, the attributes indicated with "M+" are required**. The attributes in Table 16 are required.

Table 16: Attachment

No.	Optional/ Mandatory	Attribute	Description
1	M+	Title	A meaningful name for the attachment.
2	M+	Description	Short description of the content of the file.
3	M+	File	The attached file (bitmap images, video, audio).

5.2 Summary

The following presents an overview of the data structure used to describe a COMPSIS event. This is only a different representation of the same information described in Section 5.1. The goal here is to give an overview, close to the data structure defined in the Relational Database behind the DataBank.

The overview is based on a series of Unified Modelling Language class diagrams. This notation is quite common in the modelling community. The type of diagrams reported here are intuitive. Boxes (classes of objects) organize the attribute described in the tables above, and lines indicate relationships among the "classes of objects." Those relationships are indicated in the tables as [Entity reference]. The structuring of the classes, relations and names have been maintained as much as possible closed to the tables and fields used in the definition of the underlining Relational Database.

Figure 11 describes the top level, the COMPSIS event. To support editing of different versions of the same event the dynamic information described in Table 2 is split into "COMPSIS Event" information that does not change; and "COMPSIS Event_draft" data that can be modified after the event is created with editing. Basic information is related to the COMPSIS Event. Yellow (lighter) boxes indicate information that is modified only by the Operating Agent (on request from COMPSIS members). Violet boxes (darker) represent the information modified by data providers during editing. The content of EventLCTrace is generated automatically when operation like *submission* (see 4.2.2 COMPSIS event life cycle) are performed.

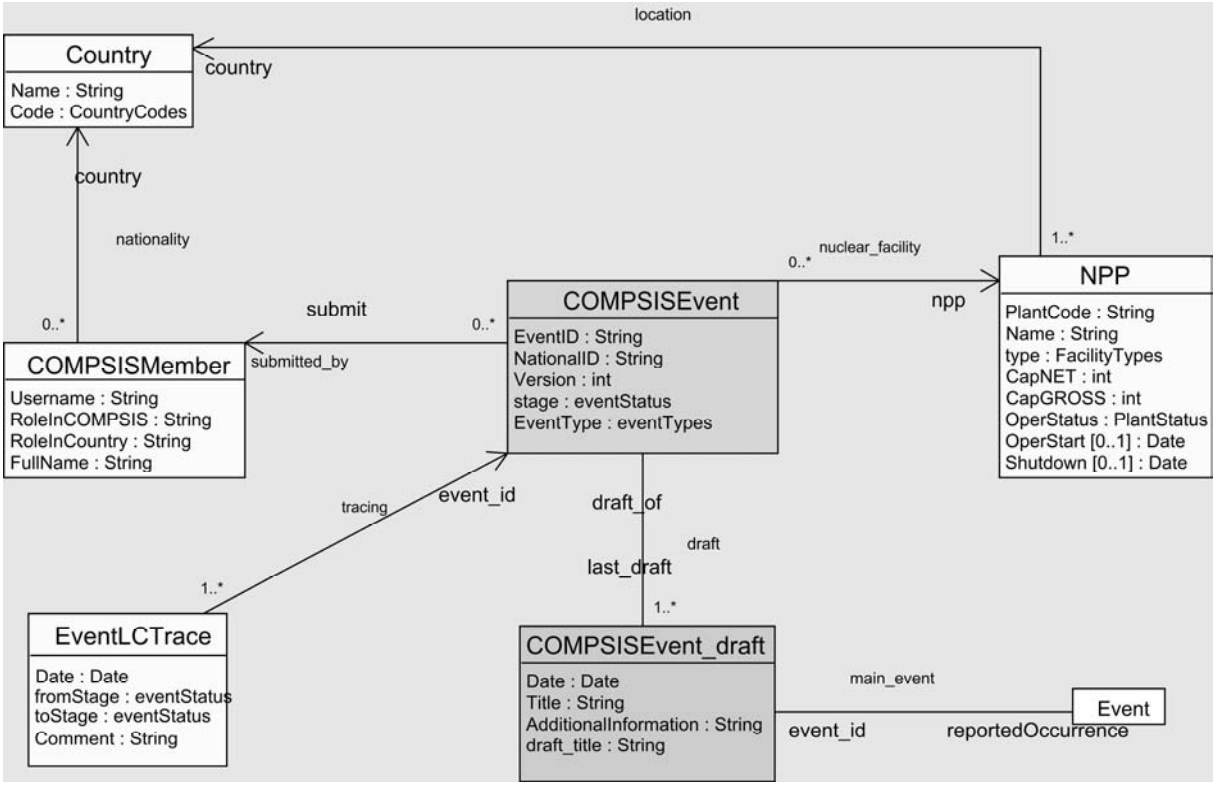

Figure 11: Top level: the COMPSIS event

Figure 12: Presents the general information contained in a draft description of the COMPSIS event.

White boxes are detailed in following diagrams.

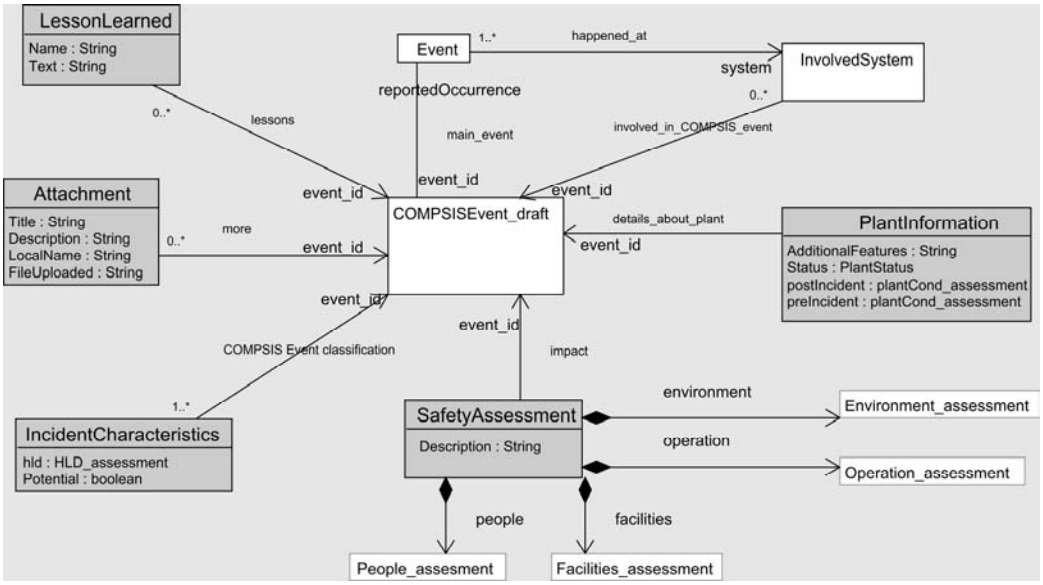

Figure 12: General information in a draft of a COMPSIS event

Boxes with a green border represent assessments of a feature which values are defined in the Coding Guidelines. For more details about the assessments see Figure 16.

Figure 13 summarises the information specifying the Cause/Consequence analysis and the recovery and corrective actions relevant to the COMPSIS event.

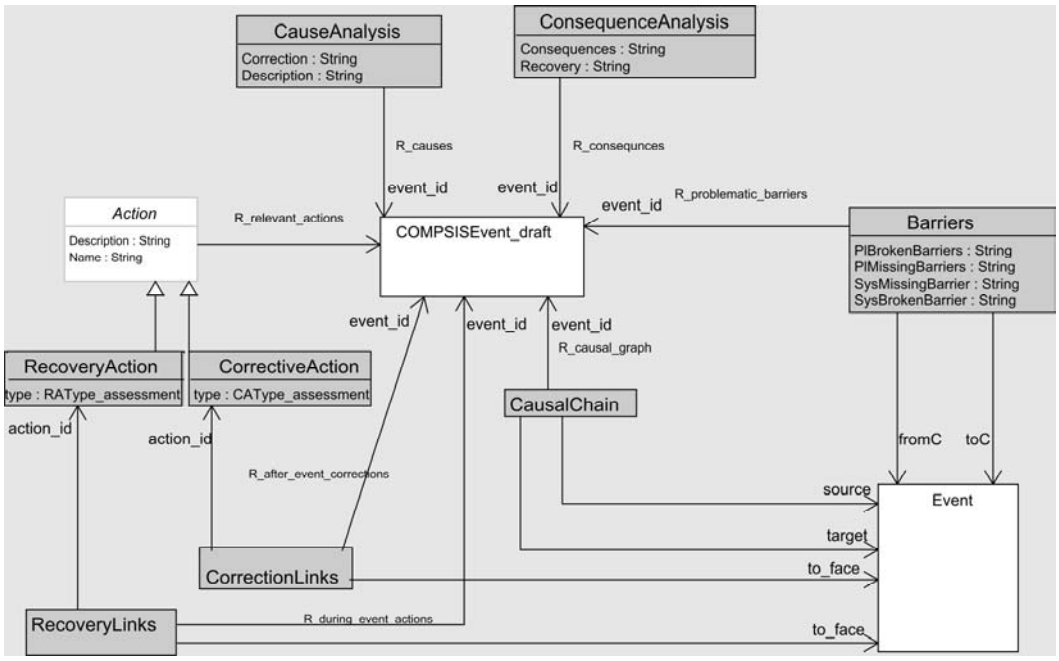

Figure 13: Information related to cause/consequence analysis

The central concept in the description of the Causes/Consequences chain is the Basic Event (See Section 2), here simple Event. Figure 14 shows the information related to the basic events.

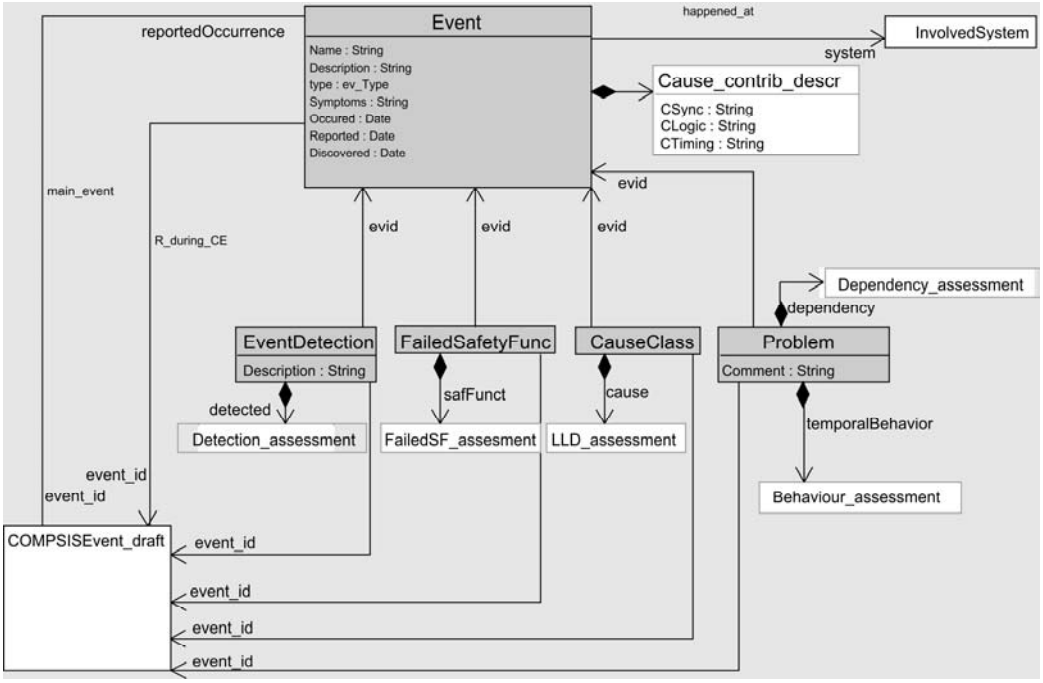

Figure 14: Information about events identified in the cause/consequence analysis

In particular an Event can be associate to a System, general information can be supplied to a system (left-bottom of Figure 15), and in particular specific information about the status of the system as involved in the specific Event.

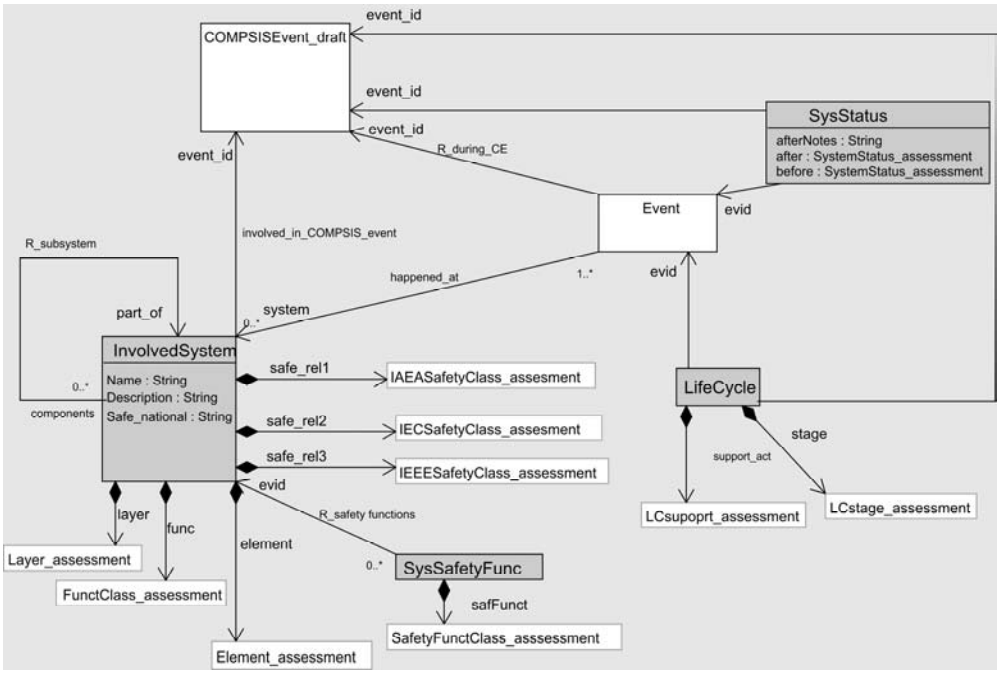

Figure 15: Information related to involved systems

The following figure collects all the assessments currently defined in the CG and implemented in the DataBank.

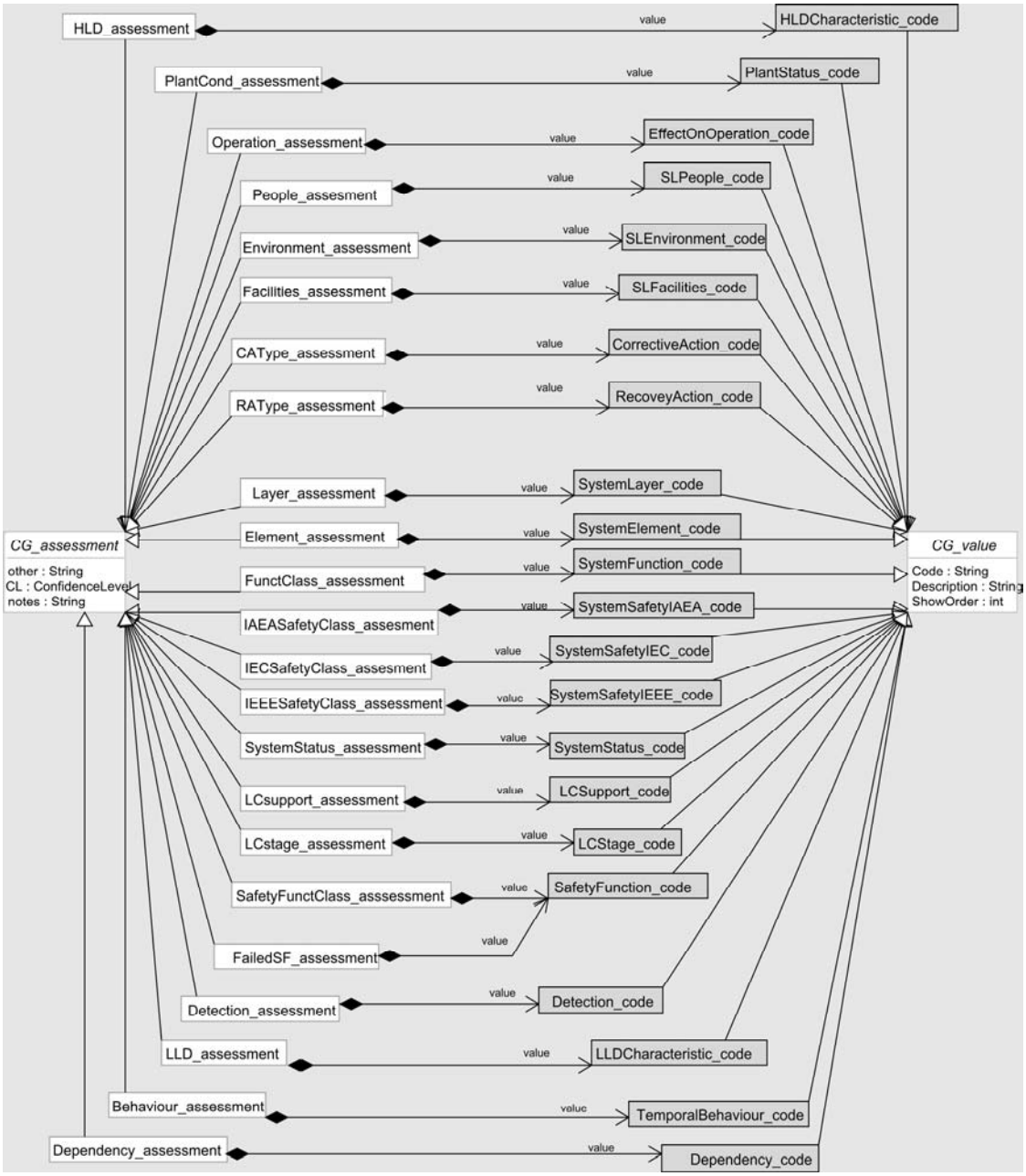

Figure 16: Feature assessments currently defined

The arrows with triangular head mean inheritance, for example "LLD_assessment" has attributes other, CL, and notes, inherited from the parent class CG_assessment. The same hold for *_code classes. Those classes have the names of the tables in the database. The content of the Tables is defined by the Coding Guidelines, and can be changed only by the Operating Agent.

A-6. LIFE CYCLE

GUI Navigation

The life cycle stages and Lifecycle supporting activities are parameters of the *basic data structure* "Entity", and are accessible on the *Edit Basic Event* page which applies to the COMPSIS Event (reported event) and all Causes and Consequences.

For the COMPSIS Event (reported event), the navigation path is:
Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit Details** button

For a Cause or Consequence, the navigation path is:
Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit [Cause/Consequence] Analysis** button
Cause/Consequence Analysis: click hyperlink to a Cause/Consequence

6.1 Life cycle stages

Since different life cycles are applied to develop computer-based systems important to safety, a very general approach should be used. It includes only the phase independent from a specific lifecycle model but necessary in each life cycle. The life cycle phase(s) shall be recorded in which the fault(s) is (are) introduced into the computer-based system. The field values in Table 17 can be applied.

Table 17: Field values for the life cycle stages

Value no.	Field values for the field life cycle stages
6.1.1	Requirement specification phase
6.1.2	Design and implementation phase
6.1.3	Selection of pre-developed component (off-the-shelf components)
6.1.4	Manufacturing phase
6.1.5	Installation and commissioning phase (including system integration)
6.1.6	Operation phase
6.1.7	Maintenance (without modifications)
6.1.8	Modification
6.1.8.1	Change requirements specification (including analysis of the impact of the modification)
6.1.8.2	Implementation phase of modification
6.1.8.3	Installation and commissioning of modification

6.2 Life cycle supporting activities

There are also supporting activities that should be recorded if they contribute to the fault introduced to the computer system. The field values in Table 18 can be applied. As an option, a new code can be defined by free text.

Table 18: Field values for life cycle supporting activities

Value no.	Field values for the field life cycle supporting activities
6.2.1	Documentation
6.2.2	Project planning
6.2.3	Change and configuration management
6.2.4	Integration of human factors

A-7. CLASSIFICATION OF THE COMPUTER-BASED SYSTEMS AND FUNCTIONS

GUI Navigation

The classification of the computer-based systems and functions are parameters of the system entity, and are accessible on the Edit System page.

The navigation path is:

Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit Systems** button
Edit Systems: click hyperlink to a system

Any system associated to a basic event (COMPSIS event, cause or consequence) is also available through the *Edit Basic Event* page.

The safety relevance of the failed system shall be recorded as far as applicable in classes of the IAEA Safety Guide NS-G-1.3, in the categories of IEC 61226 or in the categories of IEEE 603. One of the three (IAEA, IEC, or IEEE) safety relevance classes is mandatory. National classifications may be recorded in addition in a free text format.

7.1 Classification of the systems according to the safety relevance (IAEA NS-G-1.3)

The field values in Table 19 can be applied:

Table 19: Field values for the safety classification according IAEA NS-G-1.3

Value no.	Field values for the safety classification according to IAEA NS-G-1.3
7.1.1	Items not important to safety
7.1.2	Items important to safety
7.1.2.1	Safety related items or systems
7.1.2.2	Safety systems
7.1.2.2.1	Protection systems
7.1.2.2.2	Safety actuation system
7.1.2.2.3	Safety system support features

7.2 Classification of the functions according to the safety relevance (IEC 61226)

The field values in Table 20 can be applied:

Table 20: Field values for the classification according to IEC 61226

Value no.	Field values for the safety classification according to IEC 61226
7.2.1	Not categorised I&C functions
7.2.2	I&C functions of category C
7.2.3	I&C functions of category B
7.2.4	I&C functions of category A

7.3 Classification of the functions according to the safety relevance (IEEE 603)

The field values in Table 21 can be applied:

Table 21: Field values for the classification according to IEEE 603

Value no.	Field values for the safety classification according to IEEE 603
7.3.1	Items not Important to Safety
7.3.2	Items Important to Safety
7.3.3	Safety-Related Systems
7.3.3.1	Protection Systems
7.3.3.2	Safety Actuation System
7.3.3.3	Safety System Support Features

7.4 Classification of the computer-based systems according to their functions

This is a mandatory field for each system identified. The field values in Table 22 can be applied:

Table 22: Field values for the classification of the computer-based systems according to their functions

Value no.	Field values for the classification of computer-based systems according to their functions
7.4.1	Protection systems
7.4.1.1	Reactor trip system
7.4.1.2	Engineered safety features actuation system
7.4.2	Interlock systems
7.4.3	Computerised operation support systems (COSS)
7.4.3.1	Monitoring
7.4.3.2	Alarm
7.4.3.3	Diagnosis
7.4.3.4	Optimisation
7.4.3.5	Control
7.4.4	Information systems
7.4.5	Limitation systems
7.4.6	Risk reduction systems
7.4.7	Human-machine interface systems
7.4.7.1	Main control room
7.4.7.2	Supplementary control room
7.4.7.3	Emergency response facilities
7.4.7.4	Control facilities
7.4.7.5	Displays
7.4.7.6	Monitoring accident conditions
7.4.7.7	Systems for alarm annunciation
7.4.7.8	Recording system for historical data

A-8. DETAILED SAFETY FUNCTIONS OF COMPUTER-BASED SYSTEMS

GUI Navigation

The *detailed safety functions of computer-based systems* are parameters of the *system* entity, and are accessible on the *Edit System* page. Each system may implement several safety functions.

The navigation path for specifying the safety functions of a system is:

Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit Systems** button
Edit Systems: click hyperlink to a system

Any system associated to a *basic event* (COMPSIS event, cause, or consequence) is also available through the *Edit Basic Event* page.

Note also that on the *System* page the safety functions of a given system are specified. In addition, the *failed* safety function of a system is set on the *Edit Basic Event* page for the relevant Event/Cause/Consequence.

The navigation path for specifying the failed safety functions of a COMPSIS Event is:

Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit Details** button

The navigation path for specifying the failed safety functions of a Cause/Consequence is:

Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit [Cause/Consequence] Analysis** button
Cause/Consequence Analysis: click hyperlink to a Cause/Consequence

If possible, more detailed safety functions in addition to those in Chapter 7 may be addressed. The field values in Table 23 can be applied. As an option, a new code can be defined by free text.

Table 23: Field values for detailed safety functions of computer-based systems

Value no.	Field values for detailed safety functions of computer-based systems
8.1	Safety functions directly related to plant functions
8.1.1	Control of reactivity
8.1.1.1	Provide for normal reactivity control within safe limits
8.1.1.2	Prevent unacceptable reactivity transients
8.1.1.3	Shut down the reactor as necessary to prevent anticipated operational occurrences from leading to design-basis accident conditions
8.1.1.4	Shut down the reactor to mitigate the consequences of accident conditions
8.1.1.5	Maintain the reactor in a safe shutdown condition after all shutdown actions
8.1.2	Heat removal/mass-balance
8.1.2.1	Remove heat from the core during power operations
8.1.2.2	Remove residual heat in appropriate operational states and design-basis accident conditions with the reactor coolant boundary intact

Value no.	Field values for detailed safety functions of computer-based systems
8.1.2.3	Maintain sufficient coolant inventory for core cooling in normal operational states and following any postulated initiating events (to achieve mass-balance)
8.1.2.4	Remove heat from the core after a failure of the reactor coolant pressure boundary in order to limit fuel damage
8.1.2.5	Transfer heat to the ultimate heat sink from intermediate heat sinks used in removing heat from the core
8.1.3	Confinement/physical barrier integrity
8.1.3.1	Maintain the integrity of the cladding for the fuel in the reactor core
8.1.3.2	Maintain the integrity of the reactor coolant pressure boundary
8.1.3.3	Limit the release of radioactive materials and minimize the exposure of the public and personnel to radiation
8.2	Other safety functions
8.2.1	Primary functions
8.2.1.1	Protection functions
8.2.1.2	Control functions
8.2.1.3	Monitoring and display functions
8.2.1.4	Testing functions
8.2.2	Service functions
8.2.2.1	Supply of electric functions
8.2.2.2	Supply of pneumatic or hydraulic functions
8.2.2.3	Supply of data communication functions
8.2.2.4	Supply of monitoring and testing functions

A-9. STRUCTURE OF THE COMPUTER-BASED SYSTEMS

GUI Navigation

The *structure of the computer-based systems* are parameters of the *System* entity, and are accessible on the *Edit System* page.

The navigation path is:

Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit Systems** button
Edit Systems: click hyperlink to a system

Any system associated to a *basic event* (COMPSIS event, cause or consequence) is also available through the *Edit Basic Event* page.

9.1 Layers of the computer-based system

The failed layer of the complex systems shall be recorded (see Figure 1). This is a mandatory field for each system identified. The field values in Table 24 can be applied. As an option, a new code can be defined by free text.

Table 24: Field values for the layers of the computer-based system

Value no.	Field values for the layers of the computer-based system
9.1.1	Application layer
9.1.2	Communication layer
9.1.3	Process layer

9.2 Elements of the computer-based system

The failed element of the computer-based systems shall be recorded (see Figure 1). This is a mandatory field for each system identified. The field values in Table 25 can be applied. As an option, a new code can be defined by free text.

Table 25: Field values for the elements of the computer-based system

Value no.	Field values for the elements of the computer-based system
9.2.1	Computer hardware
9.2.1.1	Electronic parts
9.2.1.2	Electromechanical parts
9.2.2	Computer software
9.2.2.1	Offline software
9.2.2.1.1	System software (development tools, utility programs, etc.)
9.2.2.1.2	Application software
9.2.2.2	Online software
9.2.2.2.1	System software (operating system, communication software, etc.)
9.2.2.2.2	Application software (real-time software, embedded software, information software, etc.)
9.2.3	Firmware (programs stored on non-volatile storage, such as ROM or PROM)
9.2.4	Data
9.2.5	Documentation

A-10. STATUS

GUI Navigation

The *status* parameters include both the status (before and after an event) of the plant (facility) and the status (before and after) of one or more computer-based systems associated with a COMPSIS event/cause/consequence.

The navigation path to the Plant Status is:

Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit Facility Information** button

The navigation path to the computer-based status of a COMPSIS Event is:

Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit Details** button

The navigation path to the computer-based status of a Cause/Consequence is:

Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit [Cause/Consequence] Analysis** button
Cause/Consequence Analysis: click hyperlink to a Cause/Consequence

10.1 Plant status

The field values in Table 26 can be applied. As an option, a new code can be defined by free text.

Table 26: Field values for the plant status

Value no.	Field values for the plant status
10.1.1	On power
10.1.1.1	Full allowable power
10.1.1.2	Reduced power (including zero power)
10.1.1.3	Raising power or starting up
10.1.1.4	Reducing power
10.1.1.5	Refueling on power
10.1.2	Hot shutdown (reactor subcritical)
10.1.2.1	Hot standby (coolant at normal operating temperature)
10.1.2.2	Hot shutdown (coolant below normal operating temperature)
10.1.3	Cold shutdown (reactor subcritical and coolant temperature < 93°C)
10.1.3.1	Cold shutdown with closed reactor vessel
10.1.3.2	Refueling or open vessel (for maintenance)
10.1.3.2.1	Refueling or open vessel – all or some fuel inside the core
10.1.3.2.2	Refueling or open vessel – all fuel out of the core
10.1.3.3	Mid-loop operation (PWR)
10.1.4	Construction
10.1.4.1	Preoperational
10.1.4.2	Startup test
10.1.4.3	Commissioning
10.1.5	Testing or maintenance being performed
10.1.6	Decommissioning

10.2 Computer-based system status

The field values in Table 27 can be applied. As an option a new code can be defined by free text.

Table 27: Field values for the computer-based system status

Value no.	Field values for the computer-based system status
10.2.1	Operation
10.2.2	Standby
10.2.3	Maintenance/modification
10.2.4	Periodic test
10.2.5	Commissioning (e.g. after upgrade of the computerized system)

A-11. EFFECTS ON PLANT OPERATION

GUI Navigation

The *effects on Plant Operation* parameter applies to the COMPSIS event.

The navigation path to the Effect of Plant Operation for a COMPSIS Event is:

Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit Severity and Effects** button

The navigation path to the Effect of Plant Operation for a Cause/Consequence is:

Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit [Cause/Consequence] Analysis** button
Cause/Consequence Analysis: click hyperlink to a Cause/Consequence
Edit Basic data structure: click **Edit Severity and Effects** button

For effects on plant operation the field values in Table 28 can be applied:

Table 28: Field values for the effects on plant operation

Value no.	Field values for the effects on plant operation
11.1	Unidentified or no significant effect on operation or not relevant
11.2	Reactor scram
11.2.1	Automatic reactor scram
11.2.2	Manual reactor scram
11.3	Controlled shutdown
11.4	Load reduction
11.4.1	Automatic load reduction
11.4.2	Manual load reduction
11.5	Activation of engineered safety features
11.6	Challenge to safety or relief valve
11.6.1	Challenge to safety or relief valve in the primary circuit
11.6.2	Challenge to safety or relief valve in the steam or condensate cycle
11.7	Unanticipated or significant release of radioactive materials
11.7.1	Unanticipated or significant release of radioactive materials outside the plant
11.7.2	Unanticipated or significant release of radioactive materials inside the plant
11.8	Unplanned or significant radiation exposure of personnel or public
11.9	Personnel or public injuries
11.10	Outage extension
11.11	Exceeding technical specification limits

A-12. DEFICIENCY CHARACTERISTICS

GUI Navigation

The *high-level deficiency characteristics* apply only to the COMPSIS Event.

The navigation path to the HLFC for a COMPSIS Event is:
Event Submission: select event and click the **Edit Event** button

The *low-level deficiency characteristics* are parameters of the *basic data structure* entity, and are accessible on the *Edit Basic Event* page which applies to the COMPSIS event (reported event) and all causes and consequences.

The navigation path to the LLFC for a COMPSIS Event is:
Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit Details** button

The navigation path to the LLDC for a Cause/Consequence is:
Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit [Cause/Consequence] Analysis** button
Cause/Consequence Analysis: click hyperlink to a Cause/Consequence

12.1 High-level deficiency characteristics

For each COMPSIS event, the high-level deficiency characteristics should be recorded. Each high-level deficiency characteristic should be recorded if the high-level deficiency is either an actual high-level deficiency or a potential high-level deficiency. The value actual is applied as the default value.

For both the actual and the potential high-level deficiencies the field values in Table 29 can be applied. As an option, a new code can be defined by free text.

Table 29: Field values for the high-level deficiency characteristics

Value no.	Field values for the high-level deficiency characteristics
12.1.1	Degraded fuel
12.1.2	Degraded reactor coolant boundary
12.1.3	Degraded reactor containment
12.1.4	Loss-of-safety function
12.1.5	Significant degradation of safety function
12.1.6	Failure or significant degradation of the reactivity control
12.1.7	Failure or significant degradation of plant control
12.1.8	Failure or significant degradation of heat removal capability
12.1.9	Loss of offsite power
12.1.10	Loss of onsite power
12.1.11	Transient
12.1.11.1	Power transient
12.1.11.2	Temperature transient
12.1.11.3	Pressure transient
12.1.11.4	Flow transient
12.1.11.5	Other transient
12.1.12	Physical hazards (internal or external to the plant)

Value no.	Field values for the high-level deficiency characteristics
12.1.13	Discovery of major condition not previously considered or analysed
12.1.14	Fuel-handling incident
12.1.15	Radiation waste incident
12.1.16	Security, safeguards, sabotage or tampering incident

12.2 Low-level deficiency characteristics

For each COMPSIS event, the low-level deficiency characteristics could be recorded. Each low-level deficiency characteristic should be recorded if the high-level deficiency is either an actual high-level deficiency or a potential high-level deficiency. The value actual is applied as default value.

For both the actual and the potential high-level deficiencies the field values in Table 30 can be applied. As an option, a new code can be defined by free text. The failure should be described in terms of equipment behaviour (Section 12.2.6) and dependency (Section 12.2.7).

Table 30: Field values for the low-level deficiency characteristics

Value no.	Field values for the low-level deficiency characteristics
12.2.1	Hardware failure type
12.2.1.1	Systematic failure
12.2.1.2	Nonsystematic failure
12.2.2	Software failure/fault type
12.2.2.1	Primary fault
12.2.2.1.1	Documentation (comments, messages)
12.2.2.1.2	Syntax (spelling, punctuation, typos, instruction formats)
12.2.2.1.3	Build, Package (change management, library, version control)
12.2.2.1.4	Assignment (declaration, duplicate names, scope, limits)
12.2.2.1.5	Interface (procedure calls and references, I/O, user formats)
12.2.2.1.6	Checking (error messages, inadequate checks)
12.2.2.1.7	Data (structure, content)
12.2.2.1.8	Function (logic, pointers, loops, recursion, computation, function defects)
12.2.2.1.9	System (configuration, timing, memory)
12.2.2.1.10	Environment (design, compile, test, other support system problems)
12.2.3	Secondary fault
12.2.4	Command fault
12.2.5	Middleware failure/fault type

The field values for equipment behaviour are given in Table 31. As an option, a new code can be defined by free text.

Table 31: Field values for equipment behaviour

Value no.	Field values for equipment behaviour
12.2.6.1	Transient failure/fault
12.2.6.2	Intermittent failure/fault
12.2.6.3	Permanent failure/fault

The field values for dependency are given in Table 32. As an option, a new code can be defined by free text.

Table 32: Field values for dependency

Value no.	Field values for dependency
12.2.7.1	Single fault/error/failure
12.2.7.2	Multiple fault/error/failure
12.2.7.2.1	Independent
12.2.7.2.2	Dependent
12.2.7.3	Common-cause failure
12.2.7.4	Systematic

For common-cause failures, the definition NUREG/CR-6268, "Common-Cause Failure Data Collection and Analysis System," Revision 1, issued September 2007 can be used ("A dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause").

Items can be faults/errors/failures in systems (digital and/or analogue) that interact in a significant or unforeseen manner. They can for example, be classified according to "source" and "target" systems or other characteristics as in the following

- digital to digital
- digital to analogue
- analogue to digital
- analogue to analogue

These additional comments on the failure can be recorded through free text.

A-13. SEVERITY LEVEL

GUI Navigation

The *severity level* parameters apply to the COMPSIS event (same as for *effects on plant operations*).

The navigation path to the Severity Level for a COMPSIS Event is:

Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit Severity and Effects** button

The navigation path to the Severity Level for a Cause/Consequence is:

Event Submission: select event and click the **Edit Event** button
Edit Event: click **Edit [Cause/Consequence] Analysis** button
Cause/Consequence Analysis: click hyperlink to a Cause/Consequence
Edit Basic data structure: click **Edit Severity and Effects** button

The severity level has three attributes: impact on people, impact on facility, and impact on environment.

For impact on people the field values in Table 33 **can be applied**. As an option, a new code can be defined by free text.

Table 33: Field values for impact on people

Value no.	Field values for impact on people
13.1.1	*Catastrophic* – Death
13.1.2	*Critical* – Severe injury/illness, requires medical care (lengthy convalescence and/or permanent impairment)
13.1.3	*Marginal* – Minor injury/illness, requires medical care but no permanent impairment
13.1.4	*Negligible* – Superficial injury/illness, little or no first aid treatment
13.1.5	*None*

For impact on facility the field values in Table 34 **can be applied.** As an option, a new code can be defined by free text.

Table 34: Field values for impact on facility

Value no.	Field values for impact on facility
13.2.1	*Catastrophic* - System loss, cannot be repaired, requires salvage or replacement
13.2.2	*Critical* - Major system damage, loss of mission
13.2.3	*Marginal* – Loss of non-primary mission
13.2.4	*Negligible* - Less than minor system damage, disabled less than one day
13.2.5	*None*

For impact on environment the field values in Table 35 can be applied. As an option, a new code can be defined by free text.

Table 35: Field values for impact on environment

Value no.	Field values for impact on environment
13.3.1	*Catastrophic* - Severe environmental damage
13.3.2	*Critical* - Major environmental damage
13.3.3	*Marginal* - Minor environmental damage
13.3.4	*Negligible* - Less than minor environmental damage
13.3.5	*None*

A-14. CORRECTIVE ACTIONS

GUI Navigation

The *corrective actions* parameter applies to each cause.

The navigation path is:

Event Submission: select event and click the **Edit Event** button

Edit Event: click **Edit Corrective Actions** button

If a corrective action has been performed, the type of action should be recorded. The field values in Table 36 can be applied. As an option, a new code can be defined by free text.

Table 36: Field values for corrective actions

Value no.	Field values for corrective actions
14.1	No correction
14.2	Correction by human action
14.2.1	Shutdown
14.2.2	Repair
14.2.3	Replacement
14.2.4	Reset
14.3	Correction by automatic plant action or by design
14.3.1	Shutdown
14.3.2	Reset
14.4	Long-term corrective action
14.5	Short-term corrective action

A-15. RECOVERY ACTIONS

GUI Navigation

The *recovery actions* parameter applies to each consequence.

The navigation path is:

Event Submission: select event and click the **Edit Event** button

Edit Event: click **Edit Recovery Actions** button

If a recovery action has been reported, the type of action should be recorded. The field values in Table 37 can be applied. As an option, a new code can be defined by free text.

Table 37: Field values for recovery actions

Value no.	Field values for recovery actions
15.1	No recovery
15.2	Recovery by human action
15.2.1	Shutdown
15.2.2	Repair
15.2.3	Replacement
15.2.4	Reset
15.3	Recovery by automatic plant action or by design
15.3.1	Shutdown
15.3.2	Reset
15.4	Long-term recovery action
15.5	Short-term recovery action

A-16. DETECTION

If detection has been reported, the type of detection should be recorded. The field values in Table 38 can be applied. As an option, a new code can be defined by free text.

Table 38: Field values for detection

Code no.	Field values for detection
DE	Demand event
MA	Maintenance/test
MC	Monitoring in control room
MW	Monitoring on walkdown
TA	Test during annual overhaul
TI	Test during operation
TL	Test in laboratory
TU	Unscheduled test

A-17. CLASSIFICATION OF MANIFEST EVENTS

These are events that already have resulted in system operation deficiencies. They can be classified with regard to the particular stage of the development process, particular functional or operational requirement(s) at a certain stage, particular structure (subsystem or component) at a certain stage, and finally, particular system activity/analysis.

A-18. CLASSIFICATION OF LATENT EVENTS

These are events that have resulted in system condition deficiencies, but not yet in system operation deficiencies. They can be classified with regard to the particular stage of the development process, particular functional or operational requirement(s) at a certain stage, particular structure (subsystem or component) at a certain stage, and finally, particular system activity/analysis.

A-19. OTHER CODES

19.1 Country codes

Each country has a two-letters code[4]. Codes used in COMPSIS are defined in ISO 3166 (see, for example http://www.unemed.net/edocs/countryv2.jsp). A starting list is the field values in Table 39 (other countries will be added as they join COMPSIS):

Table 39: Field values for country codes

Code no.	Field values for country codes
CH	Switzerland
DE	Germany
FI	Finland
HU	Hungary
JP	Japan
KR	Republic of Korea
SE	Sweden
SK	Slovakia
TW	Chinese Taipeh
US	United States of America

19.2 Facility types

The facility type has the values in Table 40

Table 40: Field values for facility types

Code no.	Field values for country codes
BWR	Boiling-Water Reactor
FBR	Fast Breeder Reactor
FCF	Fuel Cycle Facility
GCR	Gas-Cooled Reactor
GCR_GR	Gas-Cooled Reactor (graphite)
GCR_AGR	Gas-Cooled Reactor (heavy-water moderated)
GCR_HTGR	Gas-Cooled Reactor (heavy-water moderated)
GCR_HWGCR	Gas-Cooled Reactor (heavy-water moderated)
GEN	Generic Report (reactor type is irrelevant)
HWLWR	Heavy-Water Moderated, Boiling Light-Water-Cooled Reactor
LWGR	Light-Water-Cooled, Graphite-Moderated Reactor (e.g. RBMK)
PBMR	Pebble Bed Modular Reactor

[4] Information needed in the NPP table can be made available by obtaining them from other databases (e.g., the one established by IAEA). Thus, the data can be entered automatically once the plant code is entered by the user.

PHWR	Heavy-Water-Moderated, Pressure Tube Reactor
PWR	Pressurised-Water Reactor (no further specifics)
PWR_WWER	Pressurised-Water Reactor
RES	Research Reactor
SGHWR	Steam Generating Heavy-Water Reactor

19.3 NPP operation states

An NPP can have one of the operation states given in Table 41.

Table 41: Field values for NPP operation states

Code no.	Field values for NPP operation states
InOp	Under Construction
UndCon	In Operation
ShDown	Shut Down
UndDec	Under Decommissioning
'Dec	Decommissioned

A - REFERENCES

[IEEE 603] Institute of Electrical and Electronic Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations – Description," IEEE Standard 603-1991

[IEC 61226] International Electrotechnical Commission, "Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - Classification of Instrumentation and Control Functions," IEC 61226, 2005.

[NSG13] International Atomic Energy Agency, "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants", IAEA Safety Standards Series, No. NS-G-1.3.

[Tha96] H. Thane, "Safe and Reliable Computer Control Systems – Concepts and Methods", Royal Institute of Technology (KTH), Stockholm, 1996.

[14Rev2] Nuclear Energy Agency/Committee on the Safety of Nuclear Installations, "Coding Guideline—Early Version 2003," NEA/CSNI/R(99), 14Rev2.