# Interaktion zwischen funktionaler Sicherheit und Datensicherheit

Francesca Saglietti

Lehrstuhl für Software Engineering
Universität Erlangen-Nürnberg
Martensstraße 3
91058 Erlangen
saglietti@informatik.uni-erlangen.de

**Zusammenfassung:** In der Vergangenheit konzentrierten sich die Verläßlichkeitsanforderungen kritischer Anwendungen entweder auf funktionale Sicherheitsaspekte oder auf Datensicherheitsaspekte - in Abhängigkeit davon, ob der Schutz des Lebens oder der Schutz der Information für die betrachtete Anwendung als dominierendes Interesse betrachtet wurde. Heutzutage, da kritische Infrastrukturen zunehmend von offenen Netzwerken abhängen, nimmt die Interaktion zwischen funktionaler Sicherheit und Datensicherheit stetig an Komplexität zu. Insbesondere können Gutachter und Genehmigungsbehörden nicht mehr - wie früher üblich - auf das klassische Prinzip der Trennung der Belange setzen. Heutzutage werden eher Standards benötigt, die eine vereinheitlichte Bewertung der Vertrauenswürdigkeit einer kritischen IT-Infrastruktur unterstützen. Der Artikel illustriert inhärente Probleme und Fortschritte auf diesem Gebiet, vor allem aus der Perspektive laufender Aktivitäten internationaler Standardisierungsgremien.

## 1 Einführung

In der Vergangenheit konzentrierten sich die Verläßlichkeitsanforderungen kritischer Anwendungen entweder auf funktionale Sicherheitsaspekte oder auf Datensicherheitsaspekte - in Abhängigkeit davon, ob der Schutz des Lebens oder der Schutz der Information für die betrachtete Anwendung als dominierendes Interesse betrachtet wurde.

**Funktionale Sicherheit.** Solange Rechner mit verantwortungsvollen Aufgaben in einer abgeschlossenen Umgebung operierten (typischerweise durch Einbettung softwarebasierter Systeme zur Steuerung eines Fahrzeugs oder einer industriellen Anlage) reichte ein einziger Sicherheitsbegriff aus, um die Vertrauenswürdigkeit der Software hinsichtlich der Abwesenheit von Gefahren infolge eines potentiellen funktionalen Fehlverhaltens zu kennzeichnen.

**Datensicherheit**. Sobald Softwaresysteme zwecks Datenaustausch zunehmend vernetzt wurden, kam zum funktionalen Fehlverhalten der softwarebasierten Steuerung eine neue Bedrohungsquelle hinzu, nämlich die Beeinträchtigung der zu verarbeitenden Information durch (bewußten oder unbewußten) Mißbrauch bzw. infolge höherer Gewalt. Diese Gefahr äußert sich typischerweise durch unerlaubten Zugriff, nichtautorisierte Datenmanipulation oder massiven Nachrichtenversand mit nachfolgender Beeinträchtigung der Privatsphäre bzw. der Diensterbringung.

In diesem Zusammenhang wurde ein neuer Sicherheitsbegriff erforderlich, um die Vertrauenswürdigkeit eines softwarebasierten Systems hinsichtlich der Abwesenheit unerwünschter Folgen für Informationen bzw. Dienstverfügbarkeit deutlich zu kennzeichnen.

**Kritische IT-Infrastrukturen**. Heutzutage tragen bereits große vernetzte Systeme die funktionale Sicherheitsverantwortung für die Steuerung kritischer technischer Prozesse; die Datensicherheit des zugrundeliegenden Kommunikationsnetzes kann ihrerseits ebenfalls Bedrohungen unterworfen sein, der sie standhalten muß. Die Kombination beider Bedrohungsarten erfordert die Betrachtung potentieller Interaktionen zwischen funktionalem und datenbezogenem Fehlverhalten. Typische Beispiele sind:

- Speicherung von Patientendaten, deren unkontrollierte Manipulation zur Anwendung medizinisch oder technisch inadäquater Therapien führen kann, sowie

- mittels Datenübertragung rechnergesteuerte Verkehrssysteme, z. B. funkgesteuerte Zuggeschwindigkeitsanpassung, ferngesteuerte Softwarepflege im Automobil, als autonome Agenten kommunizierende Fahrzeuge.

In Abhängigkeit von der übergeordneten Zielsetzung der zu betrachtenden Anwendung können folgende unterschiedliche kausale Relationen zwischen funktionaler Sicherheit und Datensicherheit von Interesse sein.

**Implikationen der Datensicherheit auf die funktionale Sicherheit.** Datensicherheitslücken können zu technischen Unfallszenarien beitragen, etwa im Falle, daß Angriffe auf die Datenintegrität zu lebensgefährlichen Rechnerversagen führen können.

**Implikationen der funktionalen Sicherheit auf die Datensicherheit.** Schwachstellen im Entwurf können ihrerseits zu Datensicherheitsverletzungen führen, etwa im Falle logischer Fehler mit funktionalem Fehlverhalten in einem komplexen Zugriffskontrollsystem.

## 2 Gemeinsame Terminologie und Modellierung

Um funktionale Sicherheit und Datensicherheit in einem einheitlichen Rahmen analysieren und nachweisen zu können, wird in diesem Artikel folgende beiden Domänen gemeinsame Terminologie eingeführt und durch Bild 1 veranschaulicht.

**Schwachstellen**. Im allgemeinen kann nicht angenommen werden, daß ein komplexes softwarebasiertes System fehlerfrei entworfen bzw. implementiert wurde. Vielmehr wird es Schwachstellen (engl. ***vulnerabilities***) enthalten, die unter bestimmten Bedingungen zu unerwünschten Ereignissen mit kritischen Konsequenzen führen können. Diese Schwachstellen können sowohl durch logische Entwurfsfehler bei der Umsetzung funktionaler Anforderungen als auch durch unbedachte Angriffsflächen bedingt sein.

**Werte**. Unerwünschte Ereignisse mit kritischen Folgen führen zum Verlust von Werten (engl. ***values***). Diese können unterschiedlicher Art sein:

- existentielle Werte (engl. ***existential values***),
  etwa Menschenleben, Gesundheit, ökologisches Gleichgewicht;

- materielle Werte (engl. ***material values***),
  etwa Kapital, materielle Infrastrukturen, sonstige Vermögenswerte;

- geschäftliche Werte (engl. ***business values***),
  etwa Zeit, Diensterbringung, Benutzerkomfort;

- ideelle Werte (engl. ***ideal values***),
  etwa Privatsphäre, Information.

Selbstverständlich induziert jede der oben genannten Verlustarten indirekt auch einen Schaden für Image und Reputation.

**Bedrohungen**. Eine Bedrohung (engl. ***threat***) ist eine Klasse von Ereignissen außerhalb des IT-Systems, die zu kritischen Konsequenzen (im Sinne des Verlustes einer oder mehrerer der oben genannten Wertarten) führen können, falls inhärente Schwachstellen im IT-System die Propagierung derartiger Ereignisse zu unsicherem Systemverhalten ermöglichen. Bedrohungen können unterschiedlicher Natur sein, u. a.

- kriminelle Angriffe,

- organisatorische Mängel,

- menschliche Irrtümer,

- technische Unfälle,

- höhere Gewalt.

**Vorfälle**. Ein Vorfall (engl. ***incident***) ist eine Instanz einer Bedrohung, also ein spezifisches Bedrohungsszenario in Anwesenheit einer Schwachstelle mit kritischen kurz- oder langfristigen Folgen.

**Vertrauenswürdigkeit**. Auf der Basis dieser Begriffsbildung soll im folgenden Vertrauenswürdigkeit (engl. ***trustworthiness***) die Abwesenheit von Vorfällen bezeichnen, selbst unter Annahme bestehender vereinzelter Bedrohungen.

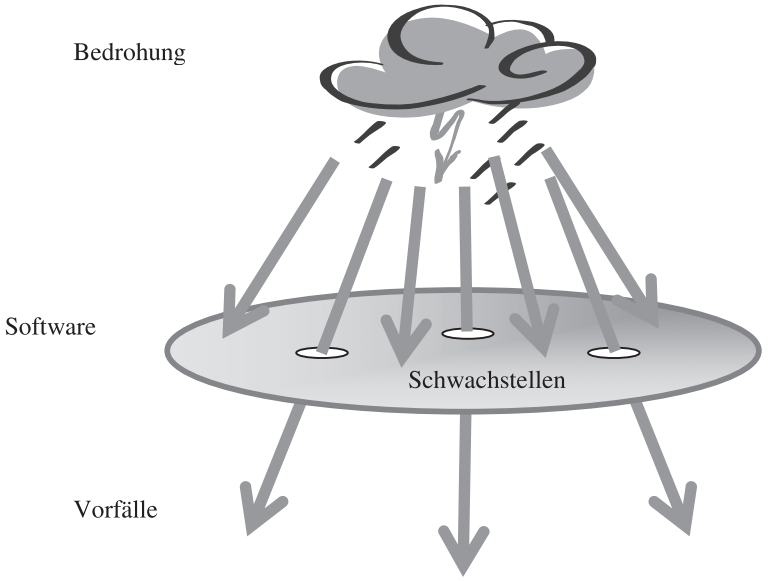


Bild 1: Einheitliche Darstellung zur Beschreibung unsicheren Verhaltens

## 3 Unterschiede zwischen funktionaler Sicherheit und Datensicherheit

### 3.1 Absicht der Bedrohungen

Eine erste klassische Unterscheidung zwischen funktionaler Sicherheit und Datensicherheit betrifft die Absichtlichkeit zu betrachtender Bedrohungen in dem Sinne, daß

- unter **funktionaler Sicherheit** üblicherweise die Abwesenheit zufallsbedingter, unbeabsichtigter Vorfälle verstanden wird, während

- **Datensicherheit** i. A. die Abwesenheit angriffsbedingter Vorfälle bezeichnet.

In diesem Artikel wird diese Sicht nicht vertreten. Die im vorliegenden Rahmen empfohlene Einstellung ist eher, den gesamten ingenieurwissenschaftlichen Ansatz durch wirkungsgeprägte (und nicht etwa ursachengeprägte) Ansätze zu unterstützen. Effiziente Entscheidungen über die im Einzelfall einzusetzenden Fehlerbehandlungsmechanismen sind eher aufgrund der aus bestehenden Bedrohungen und Schwachstellen zu erwartenden Folgen zu treffen, als angesichts des Grads an absichtlichem Fehlverhalten, was meistens weder beobachtbar noch nachweisbar ist.

### 3.2 Zu schützende Werte

Eine weitere Unterscheidung zwischen beiden Sicherheitsarten kann durch Differenzierung der durch Vorfälle gefährdeten Wertarten erzielt werden.

**Datensicherheit** wird durch Abwesenheit von Vorfällen charakterisiert, die **ideelle** und / oder **geschäftliche Werte** gefährden können, also insbesondere von Ereignissen mit unerwünschten Folgen für Informationen, Geschäftsprozesse oder für den Grad der Erbringung eines durch ein IT-System zu realisierenden Dienstes.

**Funktionale Sicherheit** andererseits wird durch Abwesenheit von Vorfällen charakterisiert, die **existentielle** und / oder **materielle Werte** in der Umgebung eines IT-Systems ernsthaft beeinträchtigen können, also insbesondere von Ereignissen mit unerwünschten Folgen für Leben und Gesundheit, Umwelt und materielle Infrastrukturen.

Zwar können im Einzelfall unterschiedliche Wertarten einen gewissen Grad an Überschneidung zulassen. Zwecks Klassifikation der aktuell vorliegenden Sicherheitsanforderungen ist es dennoch von Bedeutung, die unterschiedlichen, bei unbeherrschbaren Vorfällen zu erwartenden Verlustarten qualitativ und quantitativ zu charakterisieren.

### 3.3 Lokalisierung zu beherrschender Schwachstellen und Bedrohungen

Um im Einzelfall die Entwicklungs- und Genehmigungsprozesse zu präzisieren, die für die mit der zu planenden Anwendung eingehenden funktions- und datenbezogenene Sicherheitsrisiken adäquat sind, muß eine sorgfältige Systemanalyse - über den Schweregrad potentieller Verluste hinaus - vor allem die räumliche Befindlichkeit von Schwachstellen und Bedrohungen berücksichtigen und dabei zwischen beiden folgenden Möglichkeiten unterscheiden.

- Hauptziel der **funktionalen Sicherheitsmechanismen** ist der *Schutz der Umgebung eines IT-Systems* (einschließlich der Benutzer, sowie aller im Einflußbereich sich aufhaltenden Menschen und Umweltelemente) *vor Fehlverhalten des IT-Systems* (typischerweise infolge logischer Fehler oder physikalischer Vorgänge, wie Alterung, Verschleiß, Verstrahlung, etc.).

- Hauptziel der **Datensicherheitsmechanismen** ist dagegen der *Schutz des IT-Systems* (einschließlich Informationen und Diensterbringung) *vor unerwünschtem Verhalten seiner Umgebung* (sei dieses Verhalten durch Benutzerunerfahrenheit, höhere Gewalt oder kriminelle Angriffe bedingt).

# 4 Standardisierte Ansätze

## 4.1 Risiko-Analyse

Um entsprechend dem Schweregrad einer rechnerbasierten Anwendung die Anforderungen an die Rigorosität ihres Entwicklungs- und ihres Genehmigungsprozesses skalieren zu können, ist es erforderlich, das zugrundeliegende Risiko durch Betrachtung folgender Aspekte zu bewerten:

- für alle Elemente (Objekte, Funktionen, Daten, menschliche Wesen) die Bedrohungsart, die diese beeinträchtigen kann,

- für jede identifizierte Bedrohungsart Schätzwerte für die Eintrittswahrscheinlichkeit zugehöriger Vorfälle, sowie zu erwartender verlustbedingter Kosten.

Genauer ist für jede identifizierte potentielle Bedrohung ihr Schweregrad im Sinne des damit verbundenen Risikos quantitativ zu erfassen, nämlich als Produkt der Vorfallswahrscheinlichkeit und des vorfallsbedingt zu erwartenden Schadensausmaß:

**Risiko (Bedrohung)**
**=**
**Eintrittswahrscheinlichkeit (Vorfall) ∗ Schadensausmaß (Vorfall)**

## 4.2 Standards zur funktionalen Sicherheit

In diesem Zusammenhang betrifft eine wesentliche Frage, nach welchen Kriterien die Qualitätsanforderungen an den Entwicklungsprozeß und an das zu entwickelnde Produkt systematisch zu ermitteln sind. Im folgenden wird eine Reihe existierender bzw. sich in Vorbereitung befindlicher Standards vorgestellt, die ihre Empfehlungen auf einer vordefinierten Anforderungshierarchie basieren.

Während die meisten bisherigen Standards entweder funktionale Sicherheit oder Datensicherheit adressieren, ist eine einheitliche Vorgehensweise zur Genehmigung der übergeordneten Vertrauenswürdigkeit noch Gegenstand laufender Normierungsbestrebungen.

Allen standardisierten Ansätzen gemeinsam, obgleich auf unterschiedlichen Detaillierungsebenen, ist eine vorausgehende Risiko-Analyse mit dem Ziel, den Schweregrad potentiellen inkorrekten Softwareverhaltens zu erfassen und zu klassifizieren. Auf der Basis einer sich so ergebenden Sicherheitsklassifikation werden von den meisten heutigen Standards entsprechende Qualitätsgrade identifiziert, die zum Zweck der Genehmigung nachzuweisen sind.

**Generischer Standard IEC 61508.** Die dem Standard IEC 61508 zugrundeliegende Sicherheitsklassifikation beruht auf der probabilistischen Quantifizierung minimaler Softwarezuverlässigkeitsanforderungen aufgrund eines Vergleichs der durch die softwarebasierte Automatisierung induzierten Risiken mit den der technischen Anwendung inhärenten Risiken. Eine derartige Risikoanalyse resultiert in einem von vier möglichen sogenannten Safety Integrity Levels (SILs), wie in Tabelle 1 dargestellt, die darüber hinaus zwischen diskreten und stetigen Betriebsmodi unterscheidet.

| Safety Integrity Level | average probability of failure on demand | probability of failure per hour |
|---|---|---|
| **4** | $10^{-5} \leq x < 10^{-4}$ | $10^{-9} \leq x < 10^{-8}$ |
| **3** | $10^{-4} \leq x < 10^{-3}$ | $10^{-8} \leq x < 10^{-7}$ |
| **2** | $10^{-3} \leq x < 10^{-2}$ | $10^{-7} \leq x < 10^{-6}$ |
| **1** | $10^{-2} \leq x < 10^{-1}$ | $10^{-6} \leq x < 10^{-5}$ |

Tabelle 1: Sicherheitsklassifikation nach IEC 61508

Auf der Basis der im Einzelfall identifizierten SIL definiert der Standard gestaffelte Anforderungen an den Entwicklungsprozeß und an das zu entwickelnde Produkt. Damit wurde erstmals ein generischer Ansatz entwickelt, der sich an die speziellen Eigenarten einer Reihe von Anwendungsbereichen anpassen läßt.

**Software für medizinische Geräte.** Um die zum Teil problematische Bestimmung probabilistischer Kenngrößen zu vermeiden, empfehlen alternative standardisierte Vorgehensweisen eine deterministische Skalierung der Sicherheitsanforderungen in Abhängigkeit von den schlimmstenfalls zu erwartenden (***worst-case***) Szenarien. Dies trifft zum Beispiel für die Genehmigung von Software für medizinische Geräte zu (s. IEC 62304), wie in Tabelle 2 illustriert.

| | |
|---|---|
| **Class A** | ***No injury*** *may occur to the patient or to the operator resulting from a hazard to which the software item may be a contributing factor* |
| **Class B** | ***Non-serious injury*** *may occur to the patient or to the operator resulting from a hazard to which the software item may be a contributing factor* |
| **Class C** | ***Death or serious injury*** *may occur to the patient or to the operator resulting from a hazard to which the software item may be a contributing factor* |

Tabelle 2: Sicherheitsklassifikation nach IEC 62304

**Software für die Automobilindustrie.** Eine weitere Sicherheitsklassifikation deterministischer Natur wurde von der britischen Automobilindustrie erarbeitet (s. [MISRA 94]). In Anbetracht der menschlichen Präsenz und Mitwirkung beim Fahren eines Autos berücksichtigt dieser Ansatz die Chancen des Fahrers, unerwartetem Softwareversagen während des Betriebs durch menschliche Reaktion entgegenzusteuern.

Diese Klassifikation von unter extremen Randbedingungen noch möglicher Mensch-Maschine-Interaktion führt zu den in Tabelle 3 dargelegten Sicherheitskategorien mit zugehörigen gestaffelten Anforderungen an die Softwarequalität.

| Categories | Definition | SIL |
|---|---|---|
| **Uncontrollable** | *This relates to failures whose effects are **not controllable** by the vehicle occupants, and which are most likely to lead to extremely severe outcomes. The outcome cannot be influenced by a human response.* | **4** |
| **Difficult to control** | *This relates to failures whose effects are **not normally controllable** by the vehicle occupants but could, under favourable circumstances, be influenced by a mature human response. They are likely to lead to very severe outcomes.* | **3** |
| **Debilitating** | *This relates to failures whose effects are **usually controllable** by a sensible human response and, whilst there is a reduction in the safety margin, can usually be expected to lead to outcomes which are at worst severe.* | **2** |
| **Distracting** | *This relates to failures which produce **operational limitations**, but a normal human response will limit the outcome to no worse than minor.* | **1** |
| **Nuisance only** | *This relates to failures where **safety is not normally considered to be affected,** and where customer satisfaction is the main consideration.* | **0** |

Tabelle 3: Sicherheitsklassifikation nach MISRA

**Weitere Anwendungsgebiete.** Bis auf anwendungsspezifische Unterschiede analoge Vorgehensweisen werden auch für softwarebasierte Steuerungen in folgenden industriellen Bereichen eingesetzt:

- Verfahrenstechnik (s. IEC 61511),
- Kerntechnik (s. IEC 61226 und IEC6 2138),
- Maschinenbau (s. IEC 62061),
- Bahntechnik (s. EN 50128).

### 4.3 Standards zur Datensicherheit

**Common Criteria for Information Technology Security Evaluation.** Die folgenden 7 als Evaluation Assurance Levels (EALs) gekennzeichneten Stufen, die in den wohlbekannten Common Criteria (s. [CC 99]) vorgeschlagen werden, bieten eine steigende Skala zum Abgleich der zu erzielenden Qualität mit dem einzusetzenden Aufwand und der zu erwartenden Realisierbarkeit der angestrebten Qualitätssicherung:

- EAL1: funktionaler Test,
- EAL2: struktureller Test,
- EAL3: methodischer Test und Überprüfung,
- EAL4: methodischer Entwurf, Test und Überprüfung,
- EAL5: semiformaler Entwurf und Test,
- EAL6: semiformal verifizierter Entwurf und Test,
- EAL7: formal verifizierter Entwurf und Test.

Ein Vergleich mit den oben genannten, auf funktionaler Sicherheit basierenden Standards zeigt, daß die den EALs zugrundeliegende Hierarchie im Wesentlichen durch zunehmende Anforderungen an Funktionalität, Entwurf, Verifikation und Test charakterisiert wird. In diesem Sinne ist die EAL-Klassifikation eher prozeß- als wirkungsorientiert. Offen bleibt hier die Frage nach einer systematischen, reproduzierbaren Ermittlung der jeweils in Frage kommenden EAL-Stufen, deren Identifizierung in einfacheren Fällen noch auf intuitiver Basis erfolgen kann.

### 4.4 Einheitliche Standardisierungsansätze

**IEC Entwurf.** Genau die Frage nach der Bestimmung adäquater Datensicherheitsanforderungen für Systeme mit funktionaler Sicherheitsrelevanz wird in einem neuen Entwurf der IEC unter dem Titel "Security for Industrial Process Measurement and Control" behandelt. Dieser Entwurf schlägt derzeit vor, zu diesem Zweck eine qualitative Analyse der Einflußfaktoren

- auf die Eintrittswahrscheinlichkeit eines Angriffs, sowie
- auf den Schweregrad der Angriffsfolgen

durchzuführen, um für jeden Faktor einen angemessenen Datensicherheitsgrad (engl. ***security level***) zu ermitteln. Der maximale Grad unter allen Faktoren soll dann den übergeordneten Datensicherheitsgrad der Anwendung (sog. ***Security Requirement Level***, SRL) bestimmen.

Die hier vorgeschlagene Vorgehensweise zur Schweregradermittlung stellt also insgesamt eine Vergröberung der in Abschnitt 4.1 eingeführten Risiko-Analyse dar; die dadurch zu erwartende Genauigkeit darf deshalb in Frage gestellt werden. Andererseits hat dieser Ansatz den Verdienst, erstmals eine systematische Analyse der Datensicherheit im Rahmen industrieller Steuerungen zu betrachten.

**Fehlerbaumanalyse.** Eine genauere, wenn auch ungleich aufwendigere Analysetechnik würde klassische Fehlerbäume folgendermaßen einsetzen und erweitern:

- für jedes identifizierte Bedrohungsereignis (***top event***) mit Bezug auf die *funktionale Sicherheit* werden top-down diejenigen Unterereignisse hergeleitet, die für deren Instanziierung als Vorfall verantwortlich sein können; derartige Unterereignisse können nach Kapitel 1 auch *Datensicherheitsverletzungen* einschließen;

- anschließend werden die minimalen Schnittmengen des sich ergebenden Fehlerbaums bestimmt;

- schließlich werden, in Abhängigkeit von dem Schweregrad des anfänglich betrachteten Bedrohungsereignisses, sowie vom Verantwortungsgrad der identifizierten Unterereignisse Anforderungen an Schutzmechanismen zu deren Vermeidung bzw. Beherrschung systematisch hergeleitet.

## 5 Zusammenfassung

Dieser Beitrag hat sich mit klassischen Unterschieden und Gemeinsamkeiten bei der Ermittlung adäquater Anforderungen an funktionale Sicherheit und an Datensicherheit befaßt. Eine Reihe normativer Ansätze wurde vorgestellt, die auf unterschiedlichen Arten die im Einzelfall adäquaten Sicherheitsanforderungen bestimmen. In Anbetracht der heute zunehmenden Verbreitung kritischer IT-Infrastrukturen wird eine einheitliche Vorgehensweise als dringend notwendig erachtet. Zu diesem Zeck wird hier der Einsatz einer erweiterten Fehlerbaumanalyse empfohlen, die Datensicherheitsverletzungen als Unterereignisse zu übergeordneten Verletzungen funktionaler Sicherheit zu integrieren erlaubt.

## Literatur

[CC 99] Bundesamt für Sicherheit in der Informationstechnik (BSI). 1999. Common Criteria for Information Technology Security Evaluation, CC 2.1, aligned with International Standard ISO / IEC 15408

[EN 50128] European Committee for Electro-technical Standardization (CENELEC). 2001. Railway Applications: Software for Railway Control and Protection Systems, European Norm EN 50128

[IEC 61226] International Electro-technical Commission (IEC). 1993. Nuclear Power Plants - Instrumentation and Control Systems Important for Safety - Classification. International Standard IEC 61226

[IEC 61508] International Electro-technical Commission (IEC). 1998. Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems, Part 3: Software Requirements. International Standard IEC 61508-3

[IEC 61511] International Electro-technical Commission (IEC). 2003 / 2004. Functional Safety: Instrumented Systems for the Process Industry Sectors. International Standard IEC 61511

[IEC 62061] International Electro-technical Commission (IEC). 2004. Safety of Machinery – Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems. Final Draft International Standard IEC 62061 FDIS

[IEC 62138] International Electro-technical Commission (IEC). 2004. Nuclear Power Plants - Instrumentation and Control important for Safety - Software aspects for computer-based systems performing category B or C functions. International Standards IEC 62138

[IEC 62304] International Electro-technical Commission (IEC). 2004. Medical Device Software - Software Life-cycle Processes. Committee Draft IEC 62304 CD

[IEC 2005] International Electro-technical Commission (IEC). 2005. Security for Industrial Process Measurement and Control - Network and System Security. New Work Item Proposal

[IEV 01] Internationales Elektrotechnisches Wörterbuch. 2001. Beuth Verlag

[LAP 92] J.-C. Laprie. 1992. Dependability: Basic Concepts and Terminology in English, French, German, Italian and Japanese. Springer-Verlag

[MISRA 94] Motor Industry Software Reliability Association (MISRA). 1994. Development Guidelines for Vehicle-Based Software