Implementierung von
IEC 61508
Ziele

• Verständnis für eine mögliche Vorgehensweise mit IEC 61508 schaffen
• Bewusstes Erkennen und Behandeln bon Opportunitäten
• unmittelbaren Aktionsplanung festlegen
◆ IEC 61508
- The new main standard for software safety
- Strategy is to tailor for different domains (e.g., chemical process)
- Comprehensive standard – would be no surprise if MISRA shifts to this for next generation (but, that is speculation on my part)
- Includes SILs & table of recommended techniques

• E/E/PES = electrical/electronic/programmable electronic safety-related systems

◆ Also, a few new ideas that are useful
- E.g., concept of a “proof test”
IEC 61508

Overall safety lifecycle

Phase

Safety requirements allocation

Decommission & disposal

Overall scope definition

Hazard & risk analysis

Overall safety requirements

Overall operations & maintenance plan

Other technologies

Verification

Concept

Realisation

E/E/PES

External risk reduction

Overall safety & validation plan

Overall installation & commission plan

Overall modifications and retrofit

Overall safety validation

Overall operations maintenance & repair
NOTE 1 Activities relating to verification, management of functional safety and functional safety assessment are not shown for reasons of clarity but are relevant to all overall, E/E/PES and software safety lifecycle phases.

NOTE 2 The phases represented by boxes 10 and 11 are outside the scope of this standard.

NOTE 3 Parts 2 and 3 deal with box 9 (realisation) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.
THE SAFETY LIFECYCLE

- The model is an overview and omits activities which are common to many lifecycle phases, for example:
  - management
  - documentation
  - verification
  - quality assurance

- Forms the spine of the guideline, on which all activities hang and to which all methods, techniques and tools apply

- To be used as the basis for demonstrating compliance to the standard

  (“But a different overall safety lifecycle can be used ... Providing the objectives and requirements of each clause of this standard are met” [1: 7.1.1.1])
3 Hazard and risk analysis

To identify the hazards of the EUC in all modes of operation, the event sequences leading to the hazards, and the EUC risks associated with the hazards

- What hazards does the system pose?
- What are their possible causes and consequences?
- What is the likelihood of their occurrence?
- What are the risks associated with each of the hazards?
- By how much do we need to reduce the risks

Hazard identification

↓

Hazard analysis

↓

Risk analysis
HAZARD AND RISK ANALYSIS

- **Hazard identification**
  - Define hazards and hazardous of EUC and EUC control system for all reasonably foreseeable circumstances
    - Fault conditions
    - Reasonably foreseeable misuse
    - Human factors (not sufficient to confirm that normal operation is safe)

- **Hazard analysis**
  - Determine the event sequences leading to each hazardous event
  - Identify the causes of hazards and assess the consequences of hazardous event

- **Risk analysis**
  - Determine the risks associated with the hazardous events
APPLICATION OF IEC 61508

There is equipment under control (EUC) which, with its control system, poses a threat to its surroundings.

- Safety functions are performed by E/E/PE systems.
- Steps need to be taken to understand the risks involved and reduce them to a tolerable level.
Proposed IT – Overall Security Life Cycle
(equivalent to the Safety Reference Model, IEC 61508, Part 1)

System Requirements

Security
| Security Analysis
| (Environment, Risks, Threats, Countermeasures, ...)
| Security Requirements
| Security Design
| (Secure components, Interaction, Procedures)

Safety
| Risk/Hazard Analysis
| (System Boundary, Probabilities, Effects, Mitigation)
| Safety Requirements
| Safety Design
| (Safe Components, Interaction, Procedures)
Activities may differ very much between Safety and Security depending on requirements, e.g. during Decommissioning and Disposal:

Security: Secure management of data (unretrievalable destroyed or secure archivation of preserved integrity);

Safety: Safe management of shut down or continued (degraded) operation
Life Cycle considerations for IT – Security Management (ref, national IT Security Handbooks)

Has to take into account the complete system life cycle equivalent to safety life cycle of IEC 61508

3.1. IT – Security Management is a continuous process of:

- Development of IT – Security Policy
- Implementation of IT – Security Policy
- IT – Security during Operation

Implement results of work documented in Bibliography!
3.2. IT – Security includes the following processes (related to stages [xx] of the Life Cycle Model)

- Definition and Implementation of Security Policy ([1] – [5], from „Concept“ to „Security Requirements Allocation“)
- Maintaining Security Level during Operations [14] (includes Maintenance, Change Management and Incident Handling), Disaster Recovery ([14],[15]) and Business Continuity Planning ([15], [16])
Organisation: Wechselwirkung Produkt - Prozess

Wechselwirkung zwischen Produkt und Prozess ...

... auf allen Systemebenen

Ebene Fahrzeug

Ebene System (Steuergerät)

Ebene Software, Hardware
Organisation: Automotive-Systems-Engineering (ASE)
Organisation: Automotive-Systems-Engineering (ASE)

Engineering-Prozess

Management-Prozess

Prozess-Management

Engineering-Prozess: „Ausführen“

Management-Prozess: „Planen, Steuern und Verfolgen des Engineering“

Prozess-Management: „Definition, Implementierung, Überwachung, Verbesserung der Prozesse“
Anforderungen der IEC 61508

Anforderungen an die funktionale Sicherheit und Dokumentenmanagement

Anforderungen an Verfahren und Techniken

Anforderungen an den Sicherheitslebenszyklus
Anforderungen der IEC 61508
Mindestanforderungen an den Entwicklungsprozess
Anforderungen aus juristischer Sicht
Zusammenfassung der Anforderungen

Management-Prozess

Juristische Sicht
- Vertrags- und Projektmanagement
- Anforderungs-, Änderungsmanagement
- Spezifikation, Test- und Abnahmekriterien
- Qualitätssicherungsmaßnahmen

Reifegradmodell CMMI
- Anforderungsmanagement
- Projektmanagement
- Konfigurationsmanagement
- Qualitätsmanagement

IEC 61508
- Sicherheitsanforderungen
- Sicherheitsplanung
- SW-Konfigurationsmanagement
- SW-Qualitätsmanagement
- SicherheitsAssessments
Schritte zum sicherheitsgerechten Entwicklungsprozess
Grundmodell des Wandels

Zentrale Frage:
Kosten des Status Quo > Kosten der Änderung?
Diamant-Modell

Diagnose und Führung der Veränderung

**Auftrag**
Zweck, Ziele und Vision der Zukunft

**Energie**
Management-Verpflichtung, die Entscheidungen veranlasst und über die Zeit stabil hält

**Kultur, Werte und Verhalten der Organisation**

**Ressourcen**
Alles was es benötigt, um den Auftrag zu vervollständigen

**Struktur**
Vorgehen, Plan Projektorganisation

Dr. Prentner & Dr. Wallmüller
Zusammenfassung

• Suche und Finde aktiven (Top Management) Sponsor

• Ausgangspunkt sind Geschäftsziele

• Diagnose muss vorliegen / Assessment als Treiber

• Wichtigste Verbesserungen (kurzfristig, langfristig) festlegen

• Detaillierter Plan für 1 Jahr

• Verfolgung und messen der Verbesserungsinitiativen
... noch Fragen?