Standards of IEC related to safety-critical application of computers

(*International Electrotechnical Commission)

IEC 61508: Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-related Systems (IEC61513 – specific to Nuclear Energy)

IEC 987: Programmed digital computers important to safety in nuclear power plant.

IEC 880: Software for Computers in the Safety Systems of Nuclear Power Stations (IEEE 603-1991)

IEC 61508

- International Standard of rules applied in industry.
- Covers the complete safety life cycle,
- May need interpretation to develop sector specific standards.
- Origin: Process control industry sector.
- Basic functional safety standard applicable to all kinds of industry.
- Defines functional safety as: ***"part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities."***

IEC 61508

- **16 phases**
  - phases 1-5 address **analysis,**
  - phases 6-13 address **realization**
  - phases 14-16 address **operation.**
  - All phases are concerned with the safety function of the system.
- **Seven Parts**
  - Parts 1-3 contain the requirements of the standard (normative),
  - 4-7 are guidelines and examples for development and thus informative.

IEC 61508

- Central to the standard are the concepts **of risk** and **safety** function.
  - **The risk is a function of frequency** (or likelihood) of the hazardous event and the event **consequence severity**.
  - **The risk is reduced to a tolerable level by applying safety functions** which may consist of E/E/PES and/or other technologies.

- IEC 61508 has the following views on risks:
  - **zero risk** can never be reached
  - safety must be considered from the beginning
  - **non-tolerable risks** must be reduced

IEC 61508

Hazard and Risk Analysis

- The standard requires that hazard and risk assessment should be carried out**: 'The EUC (equipment under control) risk shall be evaluated, or estimated, for each determined hazardous event'.**
- The standard advises that **'Either qualitative or quantitative hazard and risk analysis techniques may be used'** and offers guidance on a number of approaches

IEC 61508

- 6 categories of **likelihood of occurrence** and 4 of **consequence.**

Categories of likelihood of occurrence

Category	Definition	Range (Failures per year)
Frequent	Many times in system lifetime	> 10^{-3}
Probable	Several times in system lifetime	10^{-3} to 10^{-4}
Occasional	Once in system lifetime	10^{-4} to 10^{-5}
Remote	Unlikely in system lifetime	10^{-5} to 10^{-6}
Improbable	Very unlikely to occur	10^{-6} to 10^{-7}
Incredible	Cannot believe that it could occur	< 10^{-7}

IEC 61508

Consequence categories

Category	Definition
Catastrophic	Multiple loss of life
Critical	Loss of a single life
Marginal	Major injuries to one or more persons
Negligible	Minor injuries at worst

IEC 61508

- RISK CLASSES
  - Class I: Unacceptable in any circumstance;
  - Class II: Undesirable: tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained;
  - Class III: Tolerable if the cost of risk reduction would exceed the improvement;
  - Class IV: Acceptable as it stands, though it may need to be monitored.

IEC 61508

- typical risk class matrix.

Likelihood	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

IEC 61508

- **Safety Integrity Level (SIL):**
  - Refers to a single method of reducing injury (as determined through risk analysis), not an entire system, nor an individual component.

- Higher level **Safety Integrity Levels (SIL)** require greater compliance in all three areas.
  - 1. Improved reliability.
  - 2. Failure to safety. (“**Fail-Safe**”)
  - 3. Management, Systematic Techniques, Verification and Validation.

IEC 61508

1. Improved Reliability

- For systems that operate…
  - **continuously (continuous mode)** the allowable frequency of failure must be determined.
  - **more than once a year (high demand)** the allowable frequency of failure must be determined.
  - **intermittently (less than once a year / low demand)** the probability of failure is specified as the probability that the system will fail to respond on demand.

IEC 61508

2. Failure to Safety ("Fail-Safe")

- Calculation of safe failure fraction (SFF) determines how Fail-safe the system is.
- Compares the likelihood of **safe failures** with **dangerous failures**.
- Reliability by itself is not sufficient to claim a SIL (Safety Integrity Level) level.

Fail-Safe Examples

- Arresting Wires
- Fuses
- Traffic Light Control
- Watch Dog Timer
- Dead Man's Switch

IEC 61508

3. Management, Systematic Techniques, Verification and Validation

- Specific techniques ensure that mistakes and errors are **avoided** across the entire life-cycle.
- **Errors** introduced anywhere from the initial concept, risk analysis, specification, design, installation, maintenance and through to disposal could undermine even the most reliable protection.
- Specifies **techniques that should be used** for each phase of the life-cycle.

IEC 61508

- Industry/Application Specific Variants
  - 1. Automotive Software
  - 2. Rail Software
  - 3. Process Industries
  - 4. Machinery
  - 5. **NUCLEAR POWER PLANTS (IEC 61513)**

Assignment #6

- Details
  - Read the provided article “Designing Safety-Critical Computer Systems” (IEEE Computer, November 2003)
  - Prepare **a presentation file** (PPT or PPTX format) for a 15-minute talk (i.e., about 25 slide length) summarizing the content
  - Grading weight is **twice** the usual assignments
  - Best 3 presentations would get hefty extra points
  - Submission (via email):
    - PPT (or PPTX) file named as “Last_Firstname_6.PPT”
    - Due: M. Nov 7, 2011 (5:00pm)
    - Confirmation Required

IEC 987

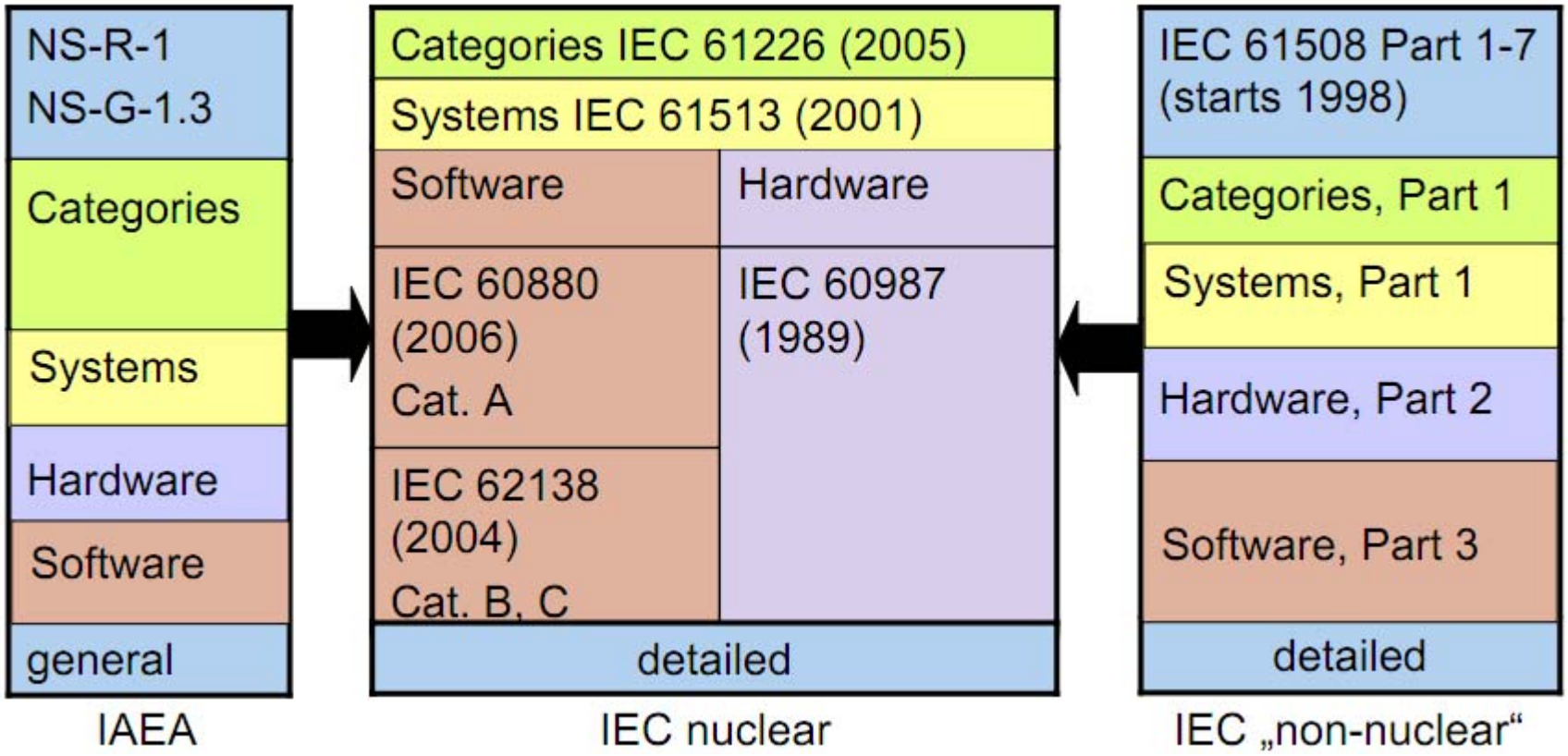
- **IEC 987 - Programmed digital computers important to safety in nuclear power plant.**
- **First edition 1989.**
- **Gives requirements on project structure and the hardware from requirements through design, development to the end of the life of the hardware.**

IEC 987

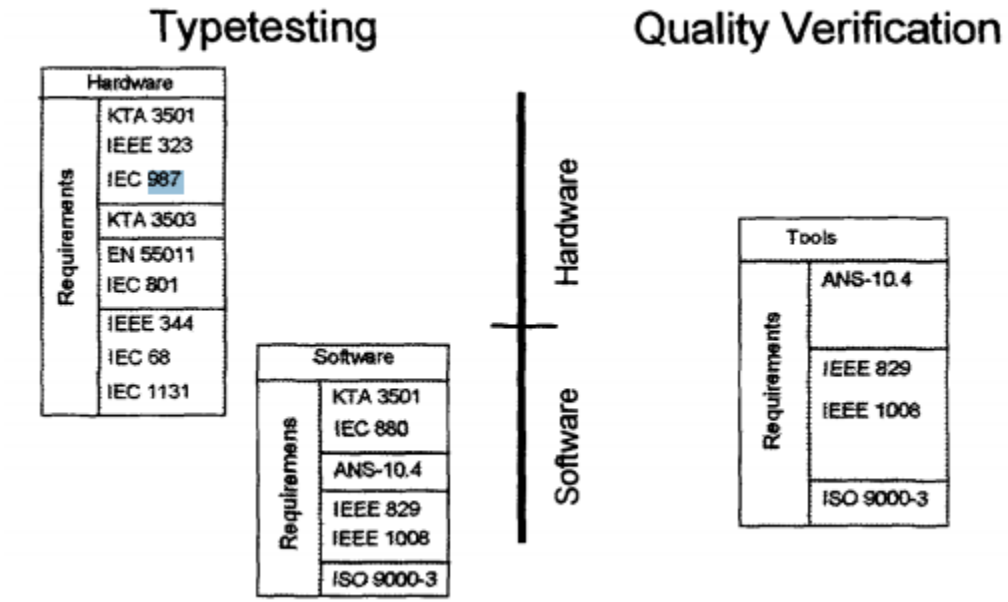
- **The quality and reliability considerations for computerized C&I systems are decided based on their safety functions**

- For the hardware and overall system aspects of these systems, well established practices are followed conforming to IEC-987

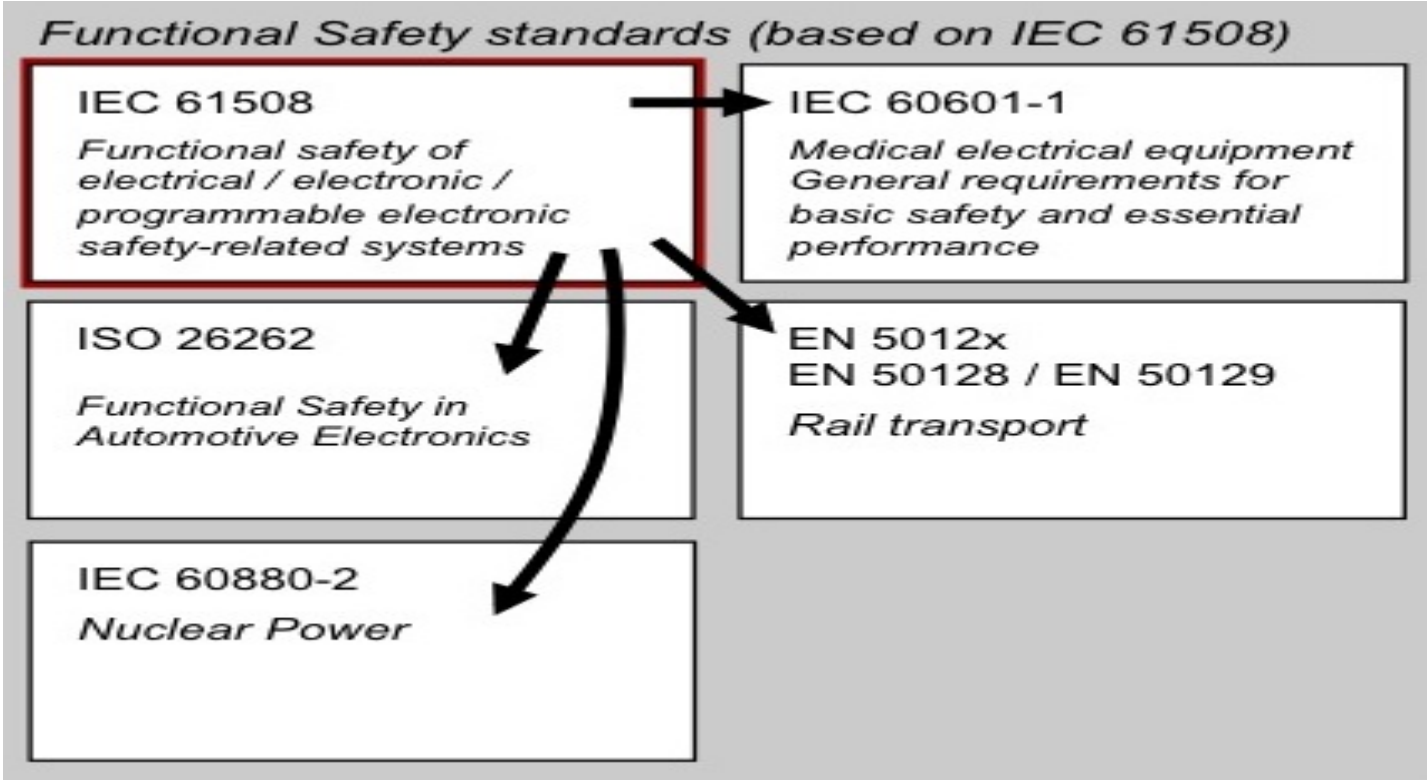
IEC 987


NS-R-1
NS-G-1.3
Categories
Systems
Hardware
Software
general
IAEA
Categories IEC 61226 (2005)
Systems IEC 61513 (2001)
Software
Hardware
IEC 60880 (2006) Cat. A
IEC 62138 (2004) Cat. B, C
IEC 60987 (1989)
detailed
IEC nuclear
IEC 61508 Part 1-7 (starts 1998)
Categories, Part 1
Systems, Part 1
Hardware, Part 2
Software, Part 3
detailed
IEC „non-nuclear“

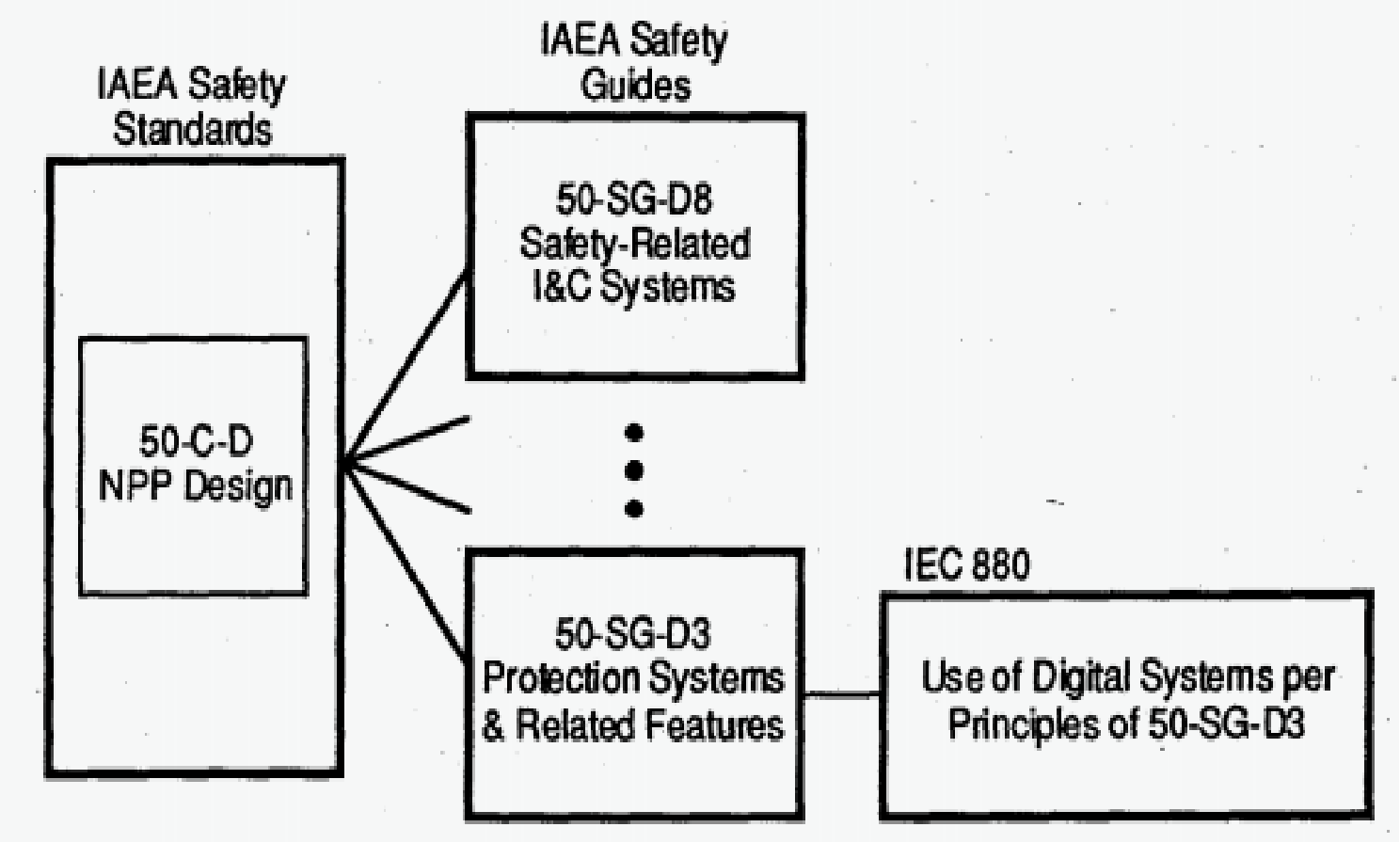
IEC 987


Typetesting
Quality Verification
Hardware
Requirements
KTA 3501
IEEE 323
IEC 987
KTA 3503
EN 55011
IEC 801
IEEE 344
IEC 68
IEC 1131
Software
Requirements
KTA 3501
IEC 880
ANS-10.4
IEEE 829
IEEE 1008
ISO 9000-3
Hardware
Software
Tools
Requirements
ANS-10.4
IEEE 829
IEEE 1008
ISO 9000-3

IEC 880: Software for Computers in the Safety Systems of Nuclear Power Stations



IEC 880


IAEA Safety Standards
50-C-D NPP Design
IAEA Safety Guides
50-SG-D8 Safety-Related I&C Systems
50-SG-D3 Protection Systems & Related Features
IEC 880
Use of Digital Systems per Principles of 50-SG-D3

IEC 880

- A standard on Software for Computers in the Safety Systems of Nuclear Power Stations.
- Applicable to the highly reliable software required for computers used in the safety systems of nuclear power plants for safety functions.

IEC 880

- Although no specific language is recommended, guidance is given for the selection of a suitable language based on some common basic rules for safety-system programming languages

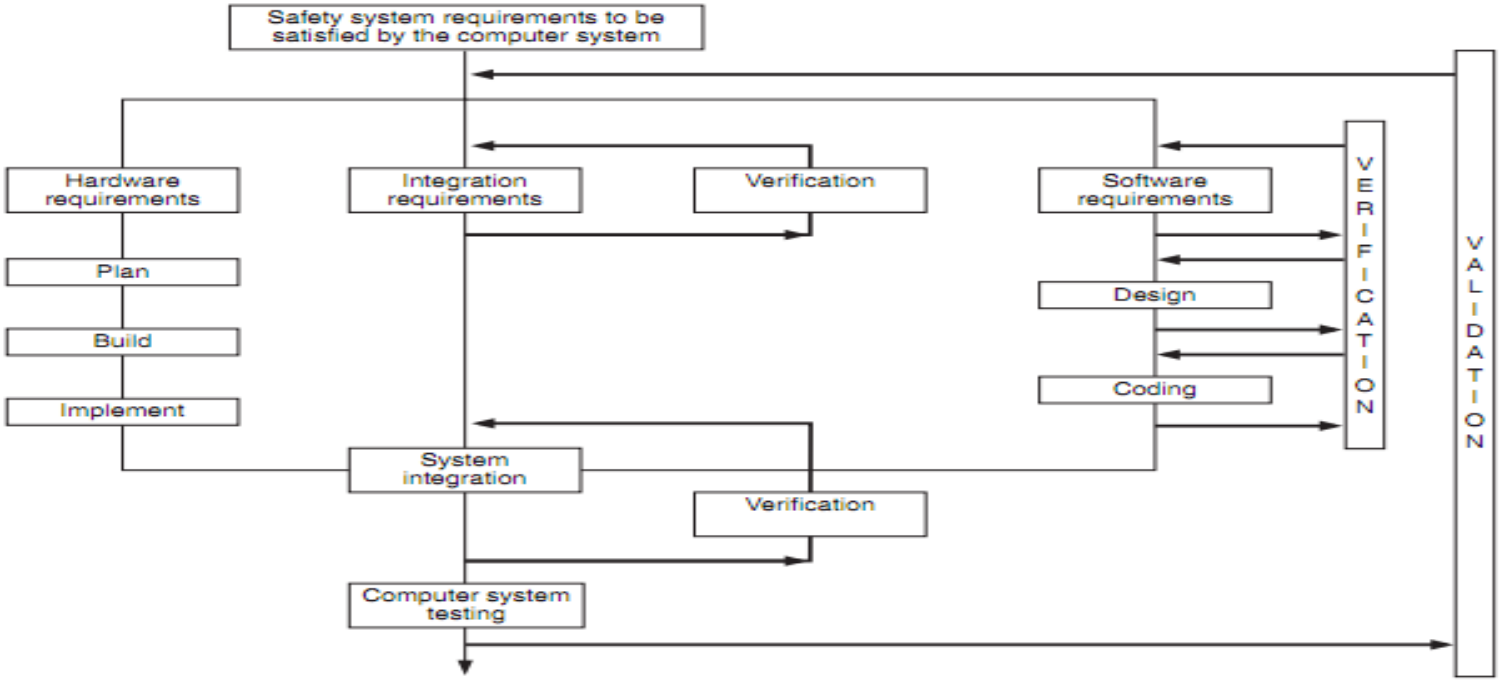
IEC 880

For example:

- Languages with a thoroughly tested translator
- The language must be completely and unambiguously defined
- Problem-oriented languages are strongly preferred
- The language should not prohibit:
- Error-limiting constructs
- Translation-time type checking
- Run-time type and array-bound check, and parameter checking

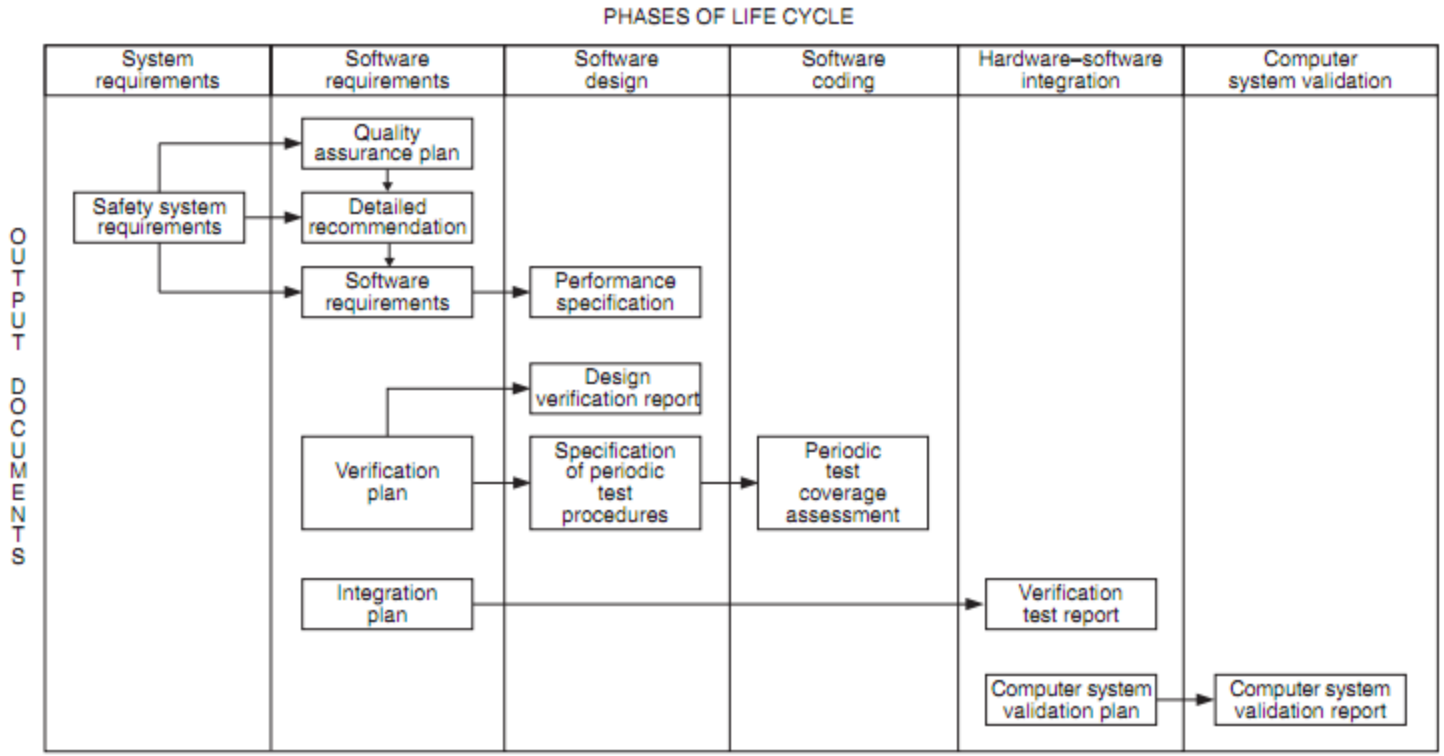
IEC 880

IEC 880 development life cycle



IEC 880

Software development life cycle documentation based on IEC 880



IEC 880

- *IEC 60880-2 Nuclear Power*
- This standard serves as a reference for IEC 61513, which deals with the system aspects of high integrity computer-based I&C used in safety systems of nuclear power plants together.

- IEC 60880 is the second level SC45A document tackling the issue of software aspects for I&C systems performing category A functions. Software for category B and C functions is dealt with in IEC 62138.

IEC 880

- IEC 60880 and IEC 62138 together cover the domain of the software aspects of computer-based systems used in Nuclear Power Plants to perform functions important to safety