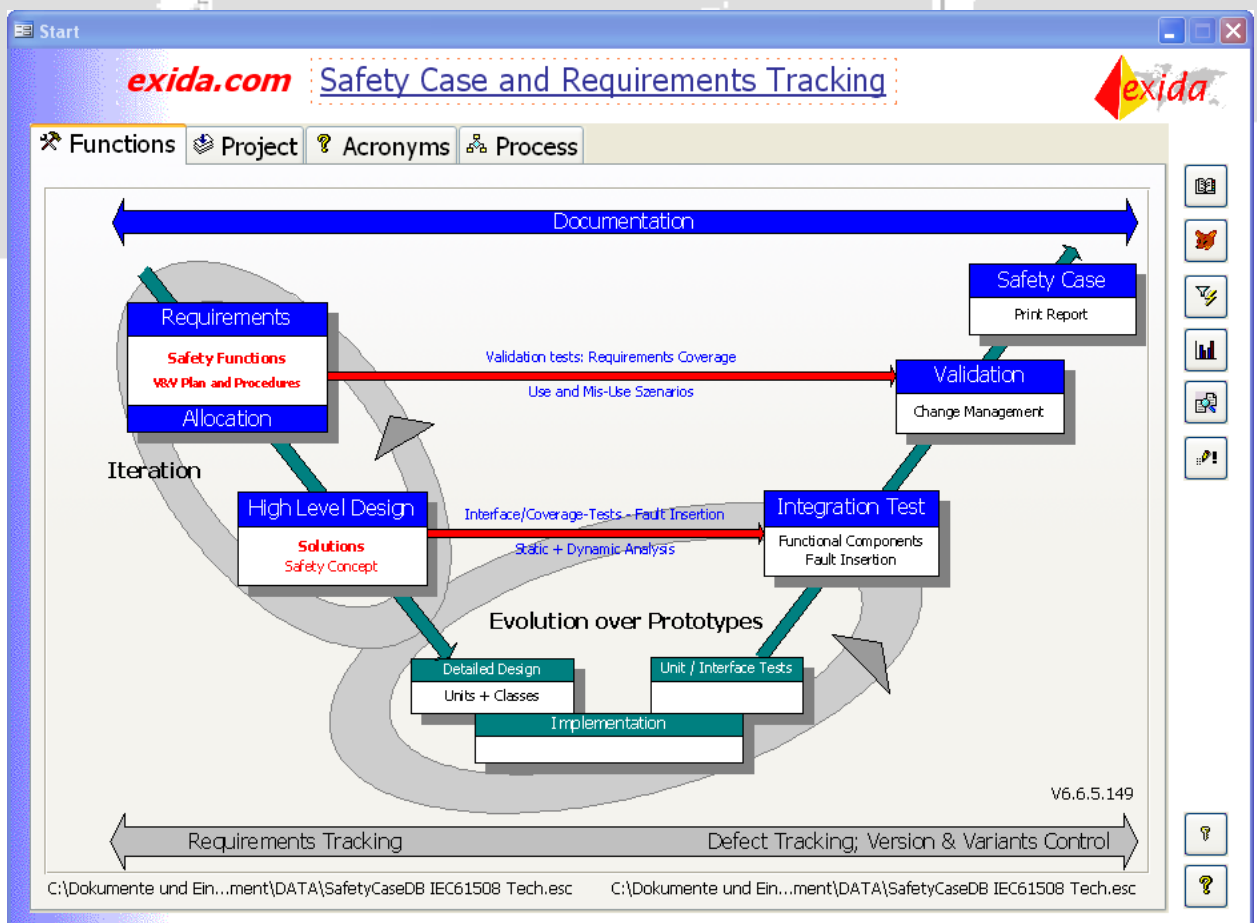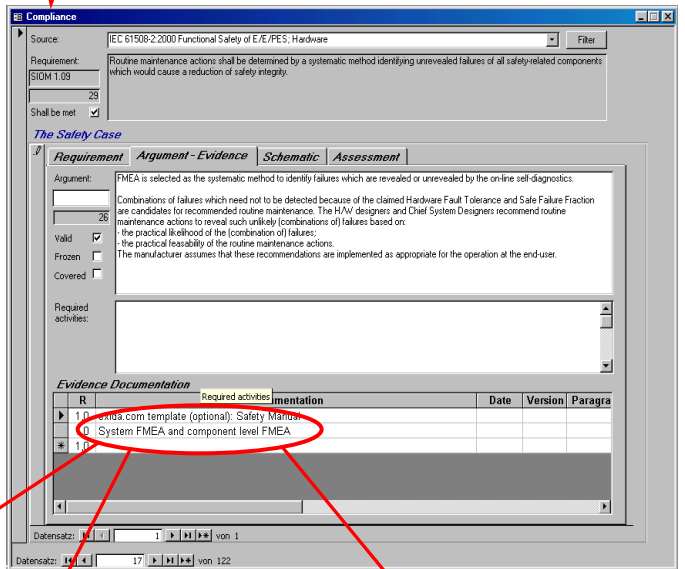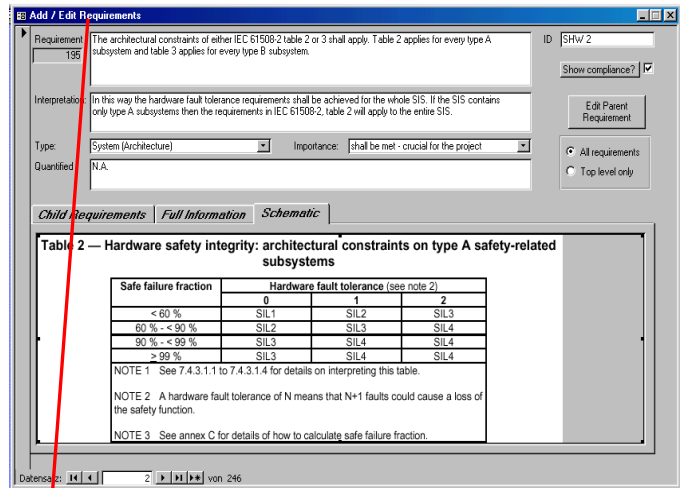# SafetyCaseDB
Functional Safety Knowledgebase

SafetyCaseDB combines all features of a Requirements Management Tool and an extensive Knowledgebase of arguments to specifically understand and meet IEC 61508 / ISO 26262 throughout the whole development cycle.

- ⧫ manages and allocates requirements – pre-filled with ISO 26262 / IEC 61508 / IEC 61511 / IEC 60880 content licensed with IEC / VDE / DIN
- ⧫ facilitates requirements tracking throughout the whole development
- ⧫ supports development of a Safety Case
- ⧫ pre-filled with extensive arguments on how to meet IEC 61508 with related IEC 61508 and ISO 26262 template documents
- ⧫ stores related evidence documents
- ⧫ supports definition of integration and validation test cases
- ⧫ eases assessments

Key Features

- **Requirements** – Hierarchical structuring of requirements. Extensive knowledgebase of IEC 61508-2, –3, ISO 26262, IEC 61511, IEC 60880 requirements

- **Documents** – Link to and storage of Verification & Validation documents

- **Allocation** of requirements to subsystems and project phases.

- **Safety Case – Arguments and Evidence** Extensive knowledgebase of arguments on how to meet the requirements of IEC 61508-2 and –3 and associated evidence templates for:
    - Item definition & ISO 26262 Safety Concepts
    - Safety Requirements Specification;
    - Functional Safety Management and V&V Plan;
    - UML Architectural Design Specification;
    - Test Specification;
    - Proven-in-Use demonstration.

- **Tests** – Specification of test cases and documentation of test execution.

- **Reporting** – to Microsoft Word™.

- **Importing** – from tagged Microsoft Word™ and XML / XLS files.

Table 2 — Hardware safety integrity: architectural constraints on type A safety-related subsystems

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.

NOTE 2 A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.

NOTE 3 See annex C for details of how to calculate safe failure fraction.

Functional Safety Management / V&V Plan

2   Roles
3   Reference Documents
    3.1 Structuring of the Project Documentation
    3.2 Documentation provided by Product Management
    3.3 Documentation provided by Customer(s)
    3.4 Company specifications and quality documents
    3.5 Laws
5   Functional Safety Management Requirements
    5.1 Definition of policy and strategy
    5.2 Allocation of responsibilities
    5.3 Configuration management requirements
    5.4 Development Process
        5.4.1 Detailed Structuring of the Project
        5.4.2 Phase 1: Specification of extent and scope of the safety
        5.4.3 Phase 2: System / architecture specification
        5.4.4 Phase 3: Detailed hardware and software design
        5.4.5 Phase 4: Integration testing
        5.4.6 Phase 5: Documentation
        5.4.7 Phase 6: System validation
        5.4.8 Modification and defect tracking
    5.5 Documentation Requirements
        5.5.1 System and H/W Documentation
        5.5.2 Software documentation
        5.5.3 Test documentation
    5.6 Functional safety assessment requirements
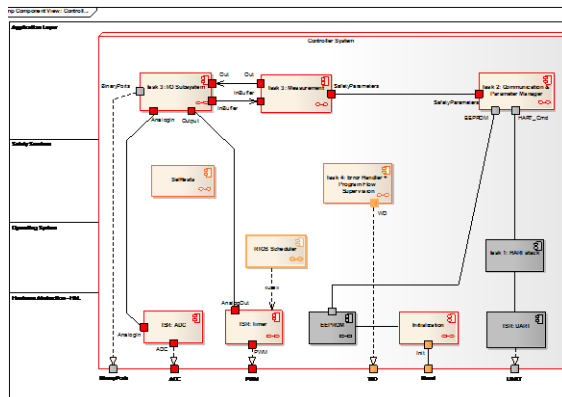
Safety Requirements Specification

5   Safety Requirements
    5.1 Operating Modes
    5.2 Safety Functions
    5.3 Separation and collaboration of safety and non safety functions
    5.4 Safety settings / configuration
    5.5 User Programming
    5.6 Safety-Related Interfaces
        5.6.1 Safety-Related Process and Power Supply Interfaces
        5.6.2 Safety Communication Requirements (optional)
        5.6.3 Man Machine Interface Requirements (optional)
        5.6.4 Internal Safety-Related Interfaces
        5.6.5 Internal Data Safety Requirements (optional)
    5.7 Safety Integrity Requirements
        5.7.1 Failure / Error Detection and Reaction Requirements
        5.7.2 Quality Factors (optional)
        5.7.3 Security Requirements (optional)

Related Services

Verification-driven Design
Improve a product / system and its development process to meet safety standards.