

■ **8th International Symposium**

Programmable Electronic Systems in Safety Related Applications



Development of Functional Safety for ATEX

■ Reasons for Coupling of Functional Safety for ATEX Application

- ATEX requirement framework
- No quantitative requirements
- No systematic requirements on lifecycle
- No systematic requirements and recommendations for failure avoidance and control
- No concrete requirements on tooling
- No requirements on assessment
-

■ Important issues in Coupling

- Which safety standards should be used
- How to decide a suitable integrity level
- Which roles can different safety standards play
- How to deal with production

■ Key Factors in Selection of Safety Standards

- Mode of operation
- New hardware
- Embedded software
- Architecture designated in 13849
- Complexity

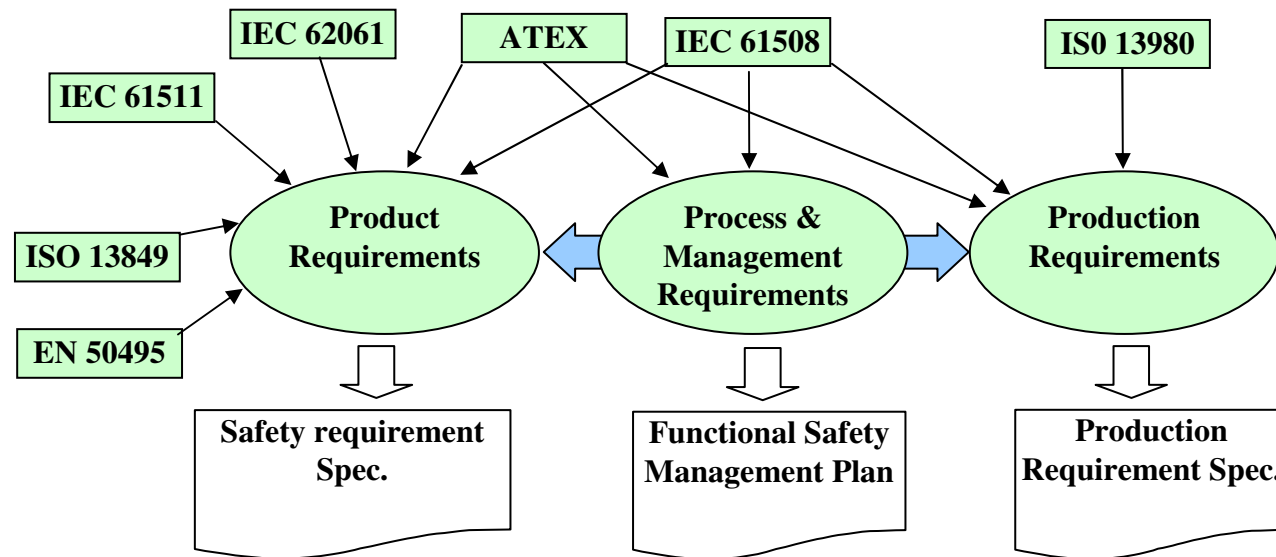
■ Example

■ IEC 61508

■ ISO 13849

■ ISO 13980

■ Requirement structure



■ Roles of safety standards

- In delivery of more concrete, systematic and detailed requirement
- In the requirement structure
 - ***Safety product requirements***
 - IEC 61508, ISO 13849, IEC62061, ATEX: common principle
 - ***Process and management requirements - lifecycle***
 - IEC 61508, ATEX: common principle
 - ***Production***
 - ISO 13980, ATEX

■ Issues in dealing with different safety standards

■ Difference in

- ❖ Quantitative measures
- ❖ Diagnostic coverage requirements
- ❖ Failure behavior

■ Clarification of roles

- ❖ Requirements
- ❖ Design and implementation
- ❖ Verification and validation
- ❖ Production

■ Relation between development and production



- Identification and traceability
- Change control
- Control of documents
- Test
- Purchase
- System architecture and design

■ Implementation of safety product requirements (1)



■ Safety concept and architecture

- Identification of architectural elements (function blocks and subsystems)
- Allocation of safety requirements to architecture elements
- Safety criticality analysis
- System-FMEA
- Diagnostic measures

■ Detailed design

- Identification and design of design elements
- Safety criticality analysis
- Component-FMEA
- Safety calculation

■ Watchdogs

- Status, time, re-try

■ Implementation of safety product requirements (2)



■ Documentation

- Structured approach, semi-formal, viewpoints and views

■ Identification and traceability

- Two kinds of identification: type and instance identification
- Levels of identification depend on complexity

Example Identification and Traceability

Table 7 Type Identification		
Hardware	Products	
	Product 1	1PRO107xxxYxxxx
	Product 2	1PRO121010Rxxxx
	PC Boards	
	PC Board 1	1PRO121007R0202
	PC Board 2	1PRO121007R0101
	PC Board 3	1PRO121007R0302
	PC Board 4	1PRO121007R0312
	PC Board 5	1PRO121007R0102
Firmware	Firmware for Measurement	1PROFMU31
	Firmware for Output	1PROFOPT17
	Firmware for Logic Unit	1PORFLOGV3b
	Protection function TOL	1PRO135038R0005

■ Implementation of Process Requirements

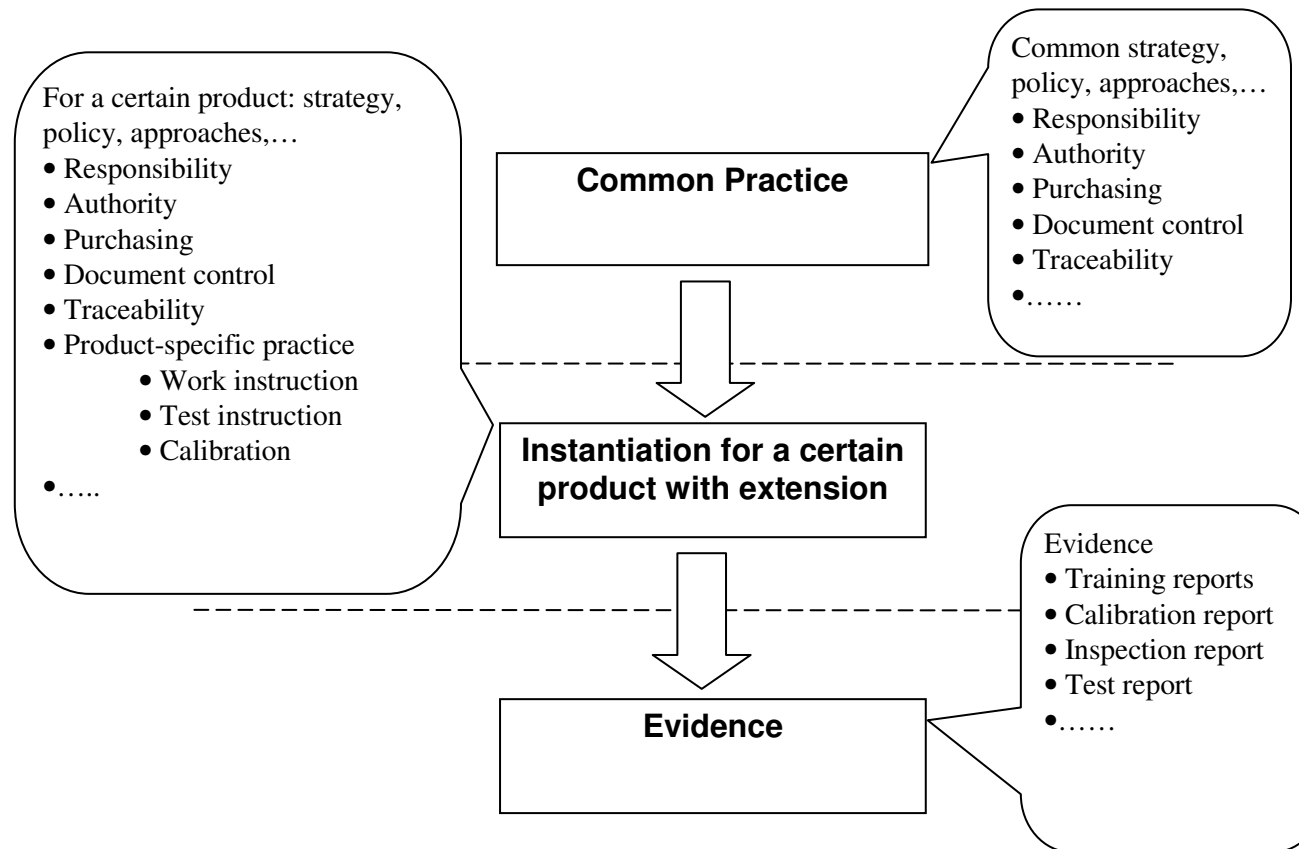
■ Lifecycle

- Control of complexity
- Activities
- Outputs / safety cases to be delivered

■ Change control procedure

- Which requirements, which parts, which phases of the development process
- Which production units, which production processes, which persons

Implementation of Production Requirements (1)

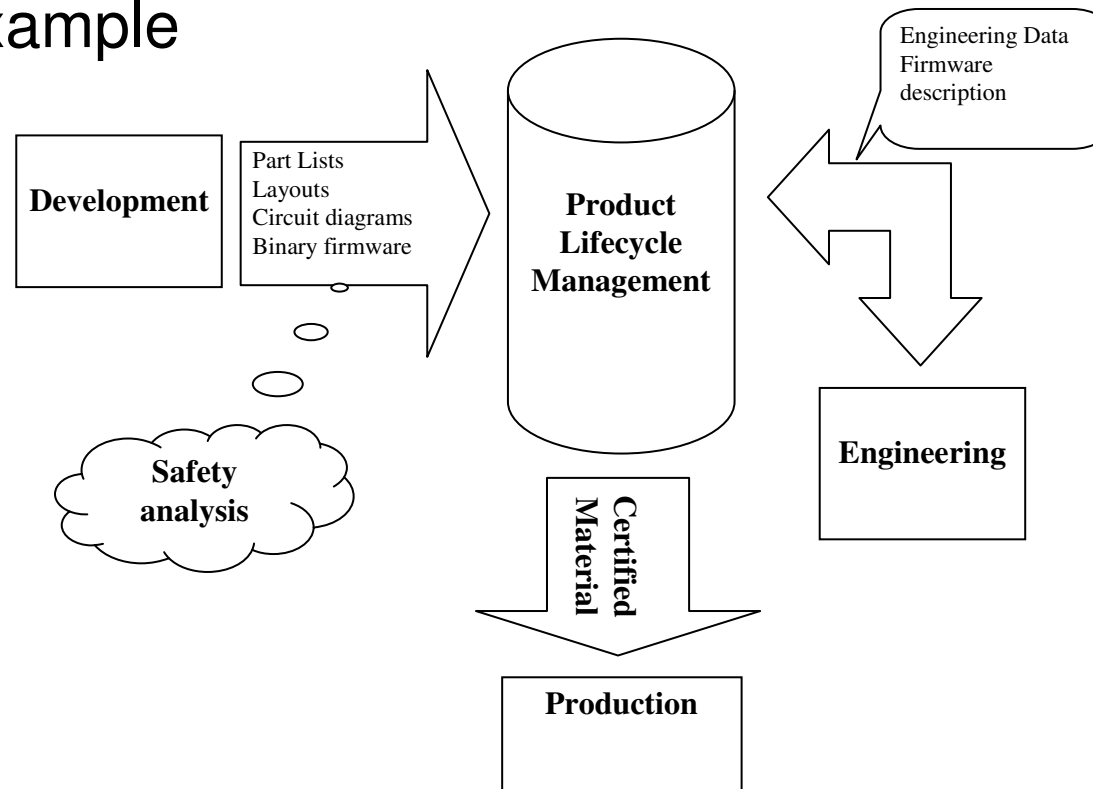


■ **Implementation of production requirements (2)**

– **Benefits**

- Clear responsibility
- Reusability
- Easy to assess

Relation between development and production– an example



Questions ??