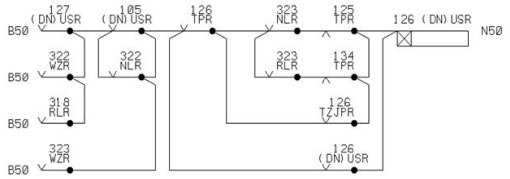
M&IT awards 2021
BRONZE WINNER

Evolution of Standards for High-Integrity Software in Railways

Roger Short




```
QR2  if   R2 a                        / Route label and availability
          P1 crf , P2 cnf             / Points test
          U10-AB f , U3-BC f          / Directly opposing route(s) test
     then R2 s                        / Route setting
          U3-CB 1 , U9-CA 1 , U10BA 1 , / Sub-route locking
          11-BA1 U12-BA1
          P1 cr , P2 cn               / Points controlling
          S1 clear bpull              / Signal clearing
```

From this ⟹ To this

Introduction

M&IT awards 2021
BRONZE WINNER

BS EN 50128:2001

Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems

Published: 15 May 2001 · Withdrawn: 31 Jul 2011

BS EN 50128:2011+A2:2020
Incorporating corrigendum February 2014

BS EN 50716:2023

Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems

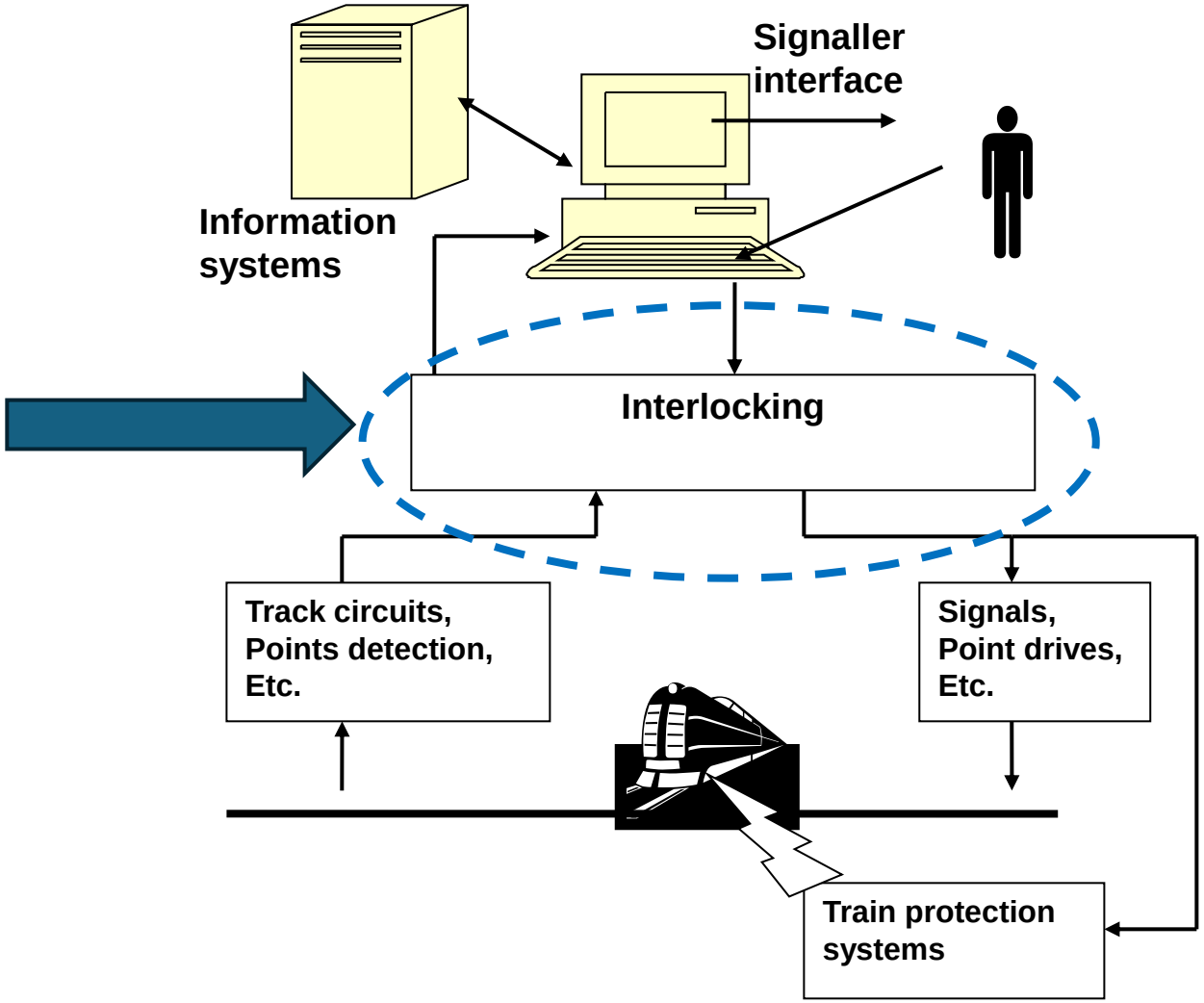
Railway Applications — Requirements for software development

This presentation outlines how standards for high integrity software in railways have evolved, starting from the earliest applications in railway signalling

The Signalling System

BRONZE WINNER

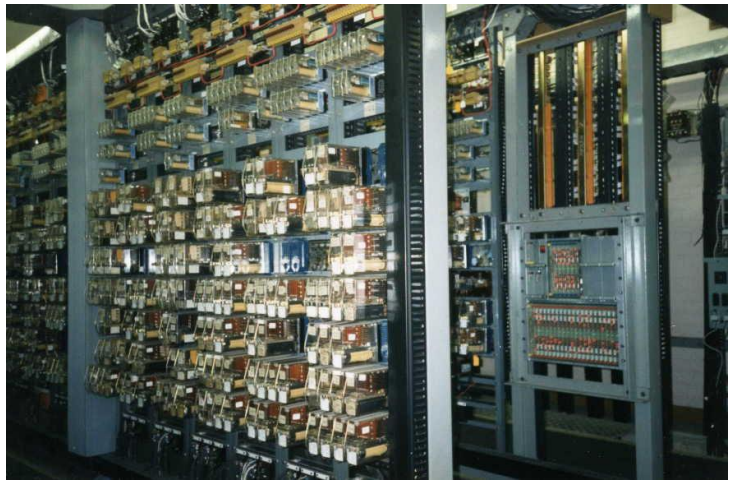
An interlocking is a system which allows a train to proceed only when all relevant conditions are safe.



Interlocking Technology

M&IT awards 2021
BRONZE WINNER

Mid 20th Century



Equipment Room

Relay

1980s onwards

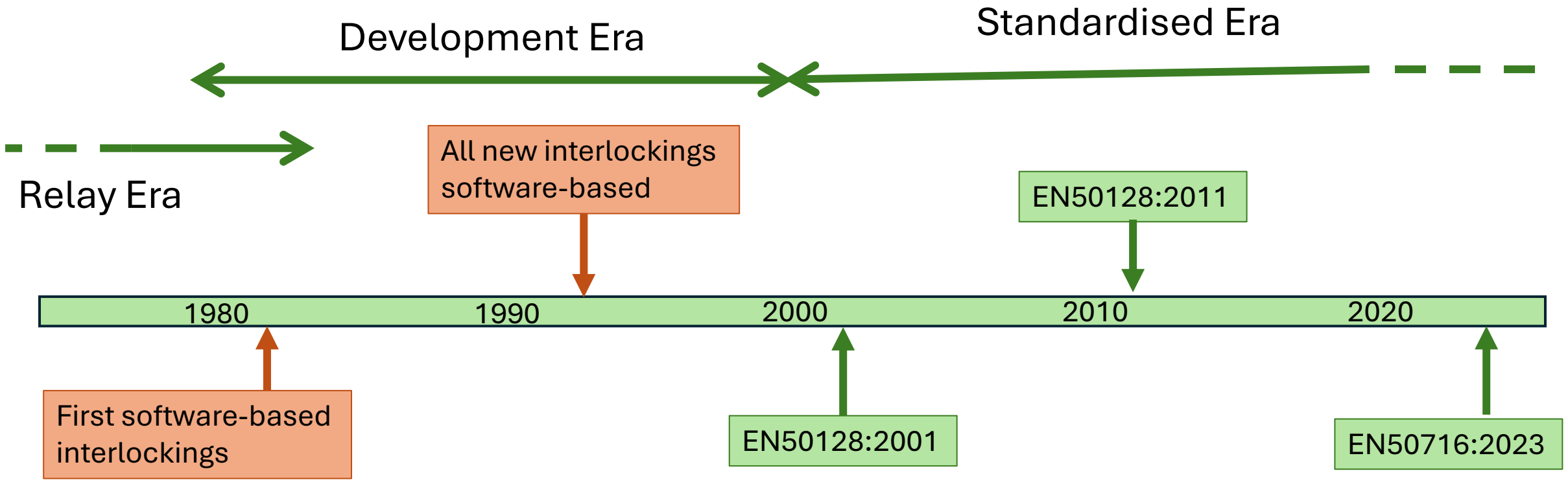
Central Interlocking

Lineside object controller

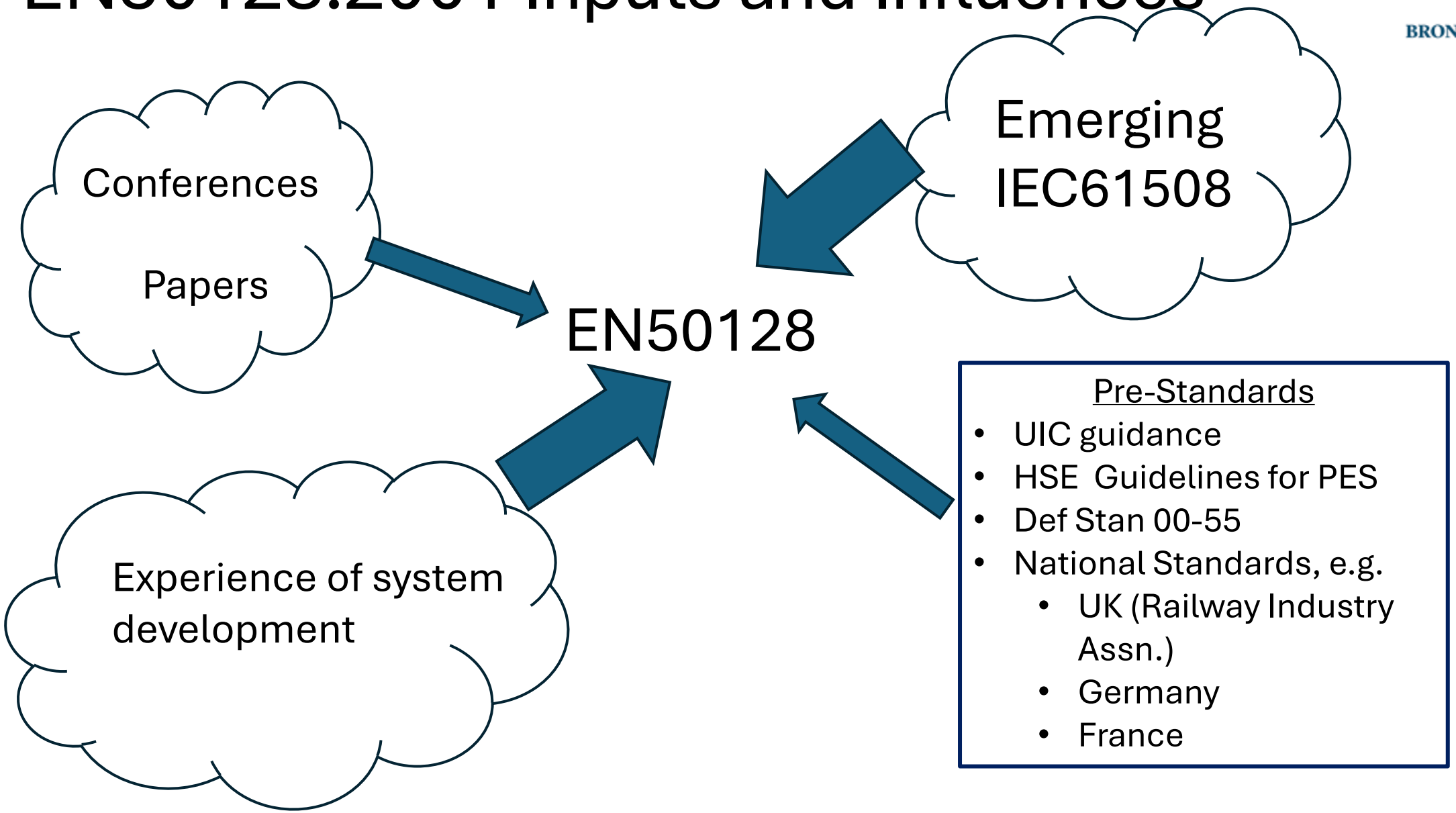
- Less equipment
- Smaller buildings
- Less cabling
- Less installation work
- Quicker and cheaper application design was hoped for (“it’s only software”) but achievement questionable.

Evolutionary Timeline

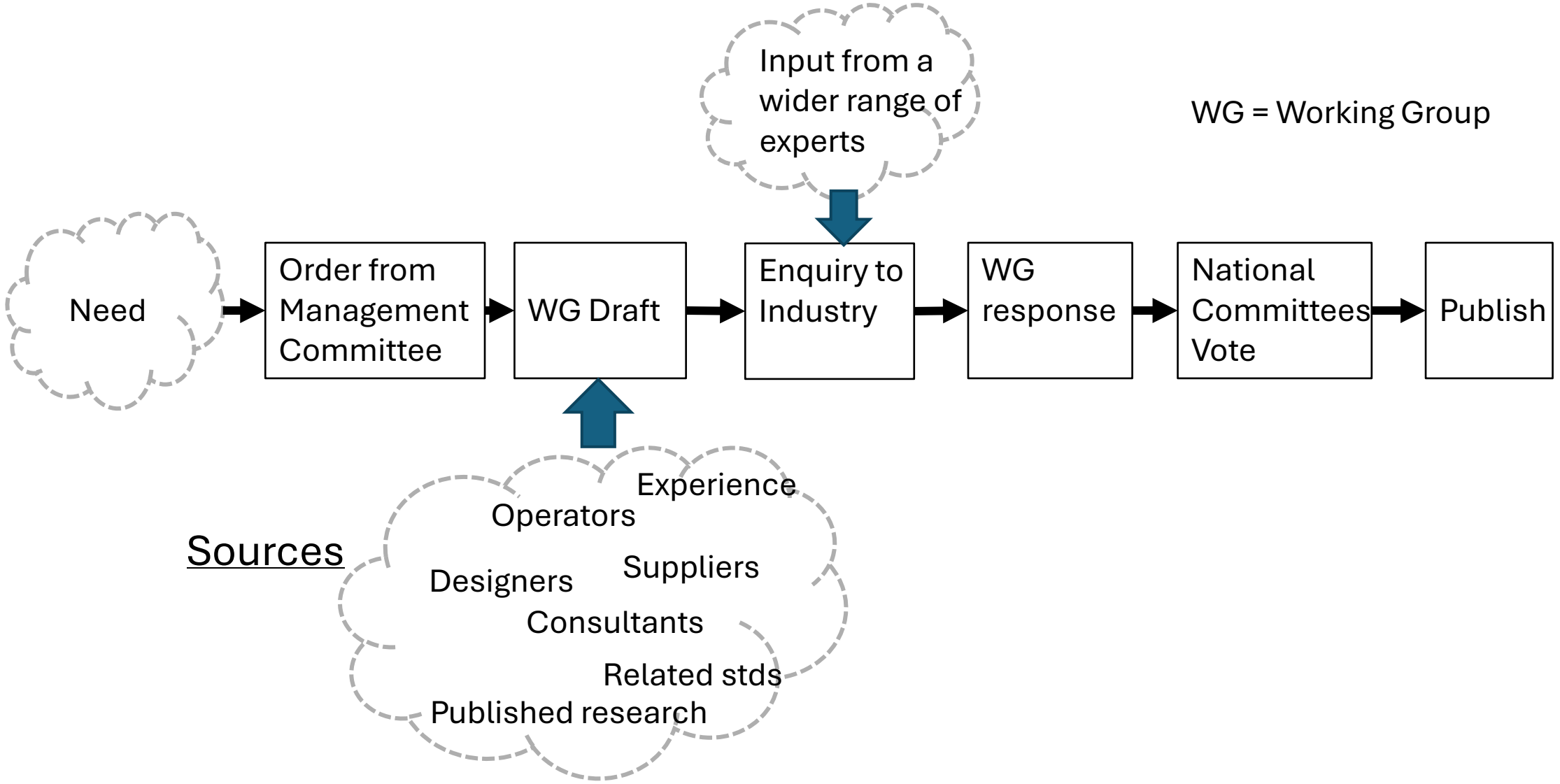
M&IT awards 2021
BRONZE WINNER



EN50128:2001 Inputs and Influences



CENELEC Process for Standards



Working Groups

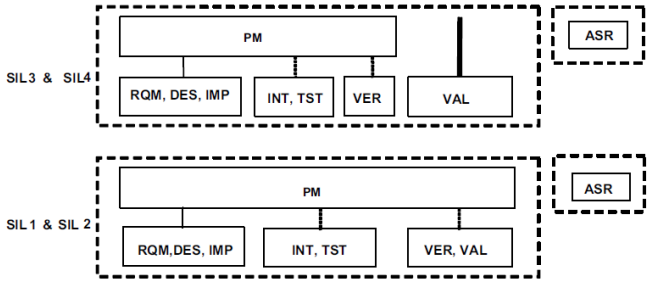
- Experts nominated by national standards organisations, e.g. BSI, volunteered by their employers.
- Usually act as individuals rather than national delegates.
- Can be multiple experts per country.

Expert being volunteered to a WG

Essence of EN50128

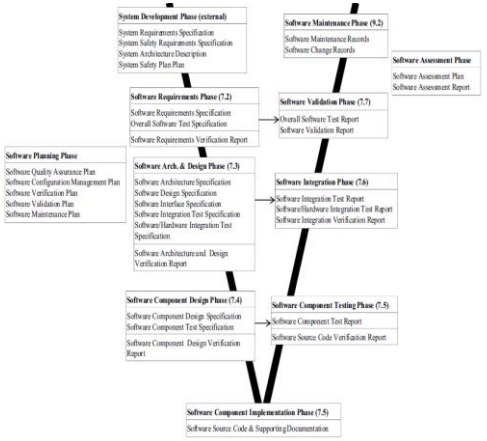
M&IT awards 2021
BRONZE WINNER

Safety Management



Organisation

Documentation



Lifecycle

Techniques and Measures

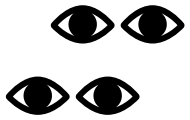
- Techniques which reduce the probability of software defects being introduced, e.g. improved programming languages, structured programming;
- Techniques which can show that the software will behave correctly, e.g. white box testing, symbolic execution;
- Techniques which detect anomalies but which do not show that software will behave correctly, e.g. structural analysis, data flow analysis

Examples of Requirements for Safety Management

M&IT awards 2021
BRONZE WINNER

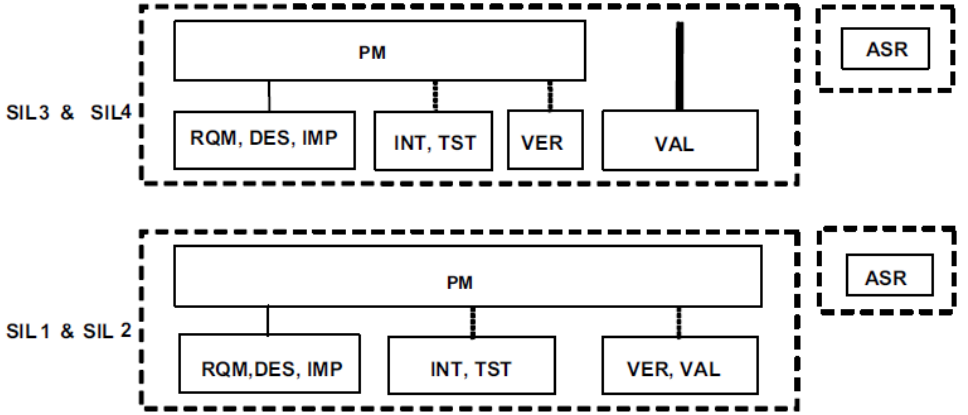
Organisation – Roles and Responsibilities

Important to ensure independence of roles with safety responsibilities, e.g. Verifier independent of Designer



Independence of Roles

Sometimes called the “4 eyes principle” but 2 brains is better

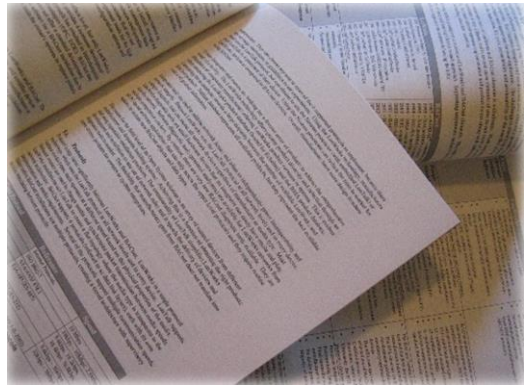


Documentation

Many specific documents are required.

Do not despise documentation. System development and safety assurance are **socio-technical** processes. Without good documentation the **SOCIO** part won’t work and the **TECHNICAL** part will go wrong!

- Plans
- Specification
- Designs
- Analyses
- Reports



Techniques and SIL

M&IT awards 2021
BRONZE WINNER

20+ tables of recommended techniques and measures.

To claim that a required SIL has been achieved, all relevant approved combinations must be used.

Note: In all versions of the standard, the recommendations for SIL1 and SIL 2, and for SIL3 and SIL4 are always the same

Table A.5 – Verification and Testing (clause 11)

TECHNIQUE/MEASURE	Ref.	SWSIL 0	SWSIL 1	SWSIL 2	SWSIL 3	SWSIL 4
1. Formal Proof	B.31	-	R	R	HR	HR
2. Probabilistic Testing	B.47	-	R	R	HR	HR
3. Static Analysis	dt8	-	HR	HR	HR	HR
4. Dynamic Analysis and Testing	dt2	-	HR	HR	HR	HR
5. Metrics	B.42	-	R	R	R	R
6. Traceability Matrix	B.69	-	R	R	HR	HR
7. Software Error Effect Analysis	B26	-	R	R	HR	HR

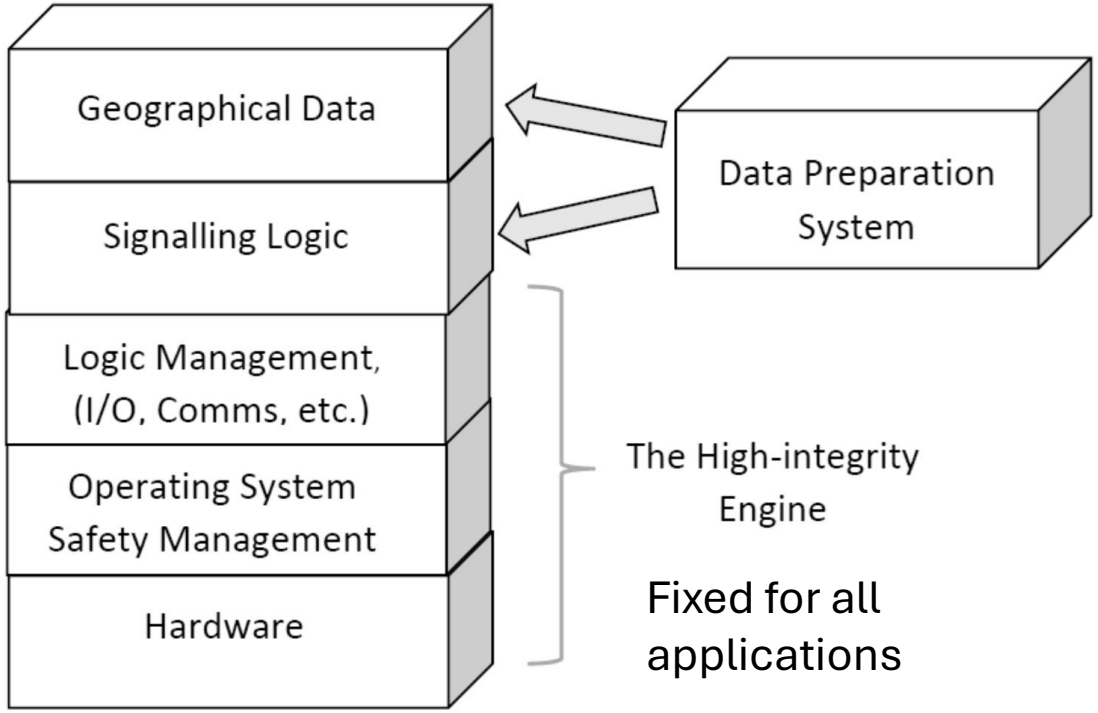
Requirements

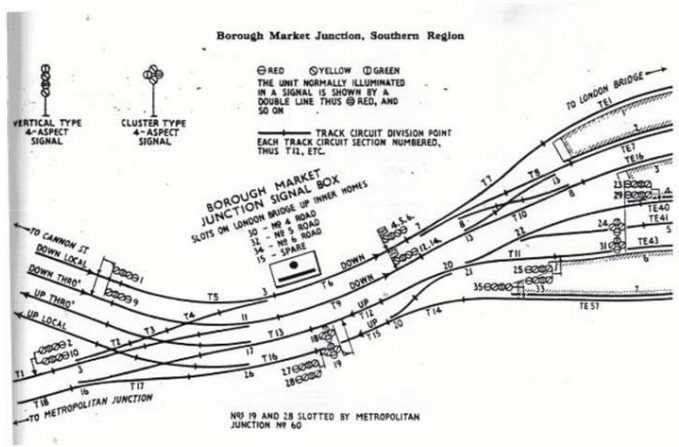
1. For Software Safety Integrity Level 3 or 4, the approved combinations of techniques shall be:
   a) 1 and 4
   or b) 3 and 4
   or c) 4, 6 and 7
2. For Software Safety Integrity Level 1 or 2, the approved combinations of techniques shall be:
   a) 1
   or b) 3 and 4
   or c) 4

Configuration Logic and Data

M&IT awards 2021
BRONZE WINNER

Repeated for each application



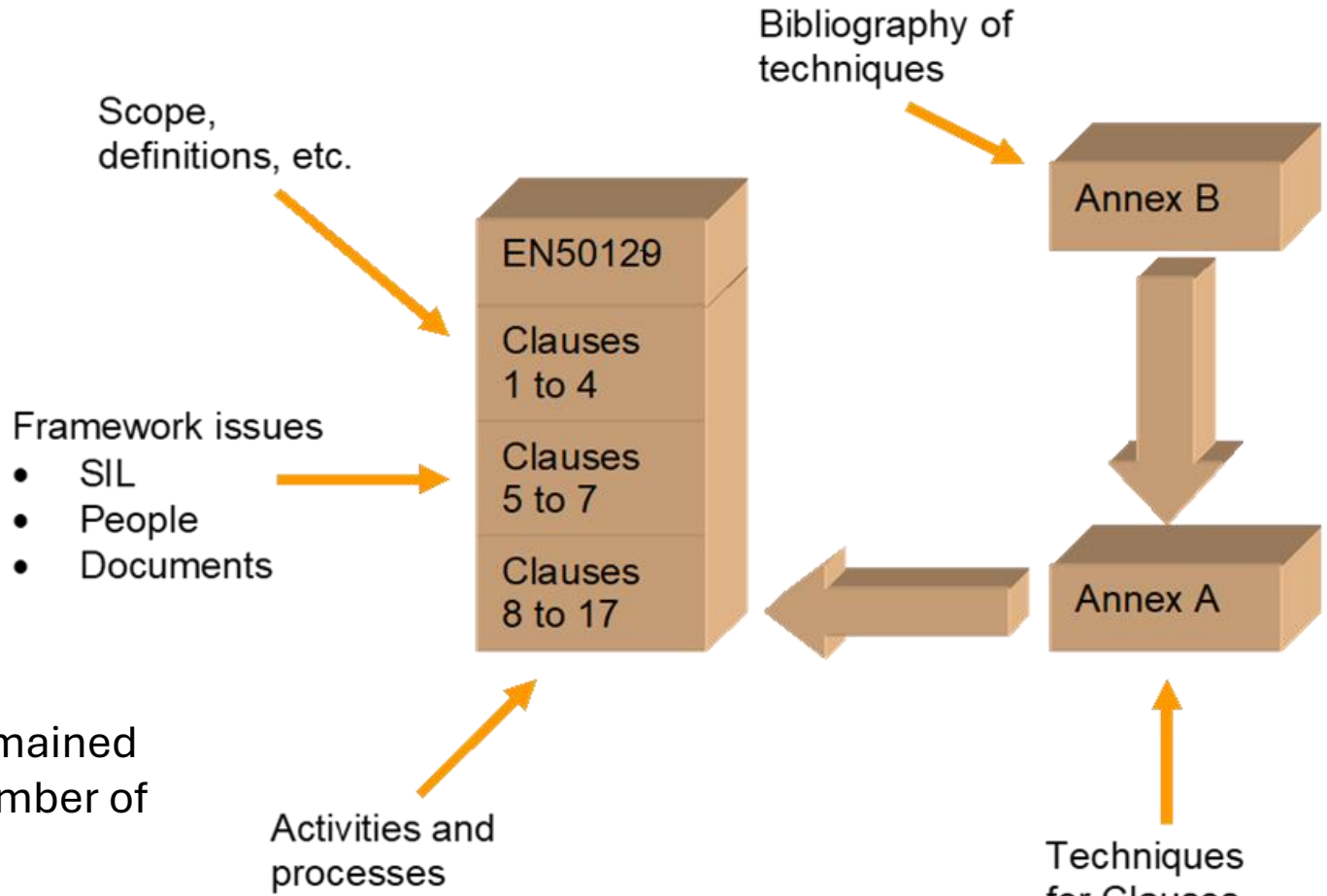


Area under control

Signal interlocking systems need to be configured to the area under control

All versions of the Standard include a chapter on development of application logic and data

Structure of EN50128



The structure has remained constant, but the number of annexes has grown

Changes in EN50128:2011

- Organisational requirements expanded
- Key responsibilities more fully defined
- Competence requirements now included

2001 version

2011 version

Includes requirements for competence

Annex B
(normative)

Key software roles and responsibilities

Changes in EN50128:2011

- Additional requirements for documentation, including generic requirements for document quality.
- Additional generic requirements for software assurance.
- Generic requirements for support tools.
- SIL0 becomes Basic Integrity.

2001 version

2011 version

EN 50657:2017 – Software for Rolling Stock

M&IT awards 2021
BRONZE WINNER

- Effectively EN 50128:2011 adapted to rolling stock applications.
- Changes mainly concerned with terminology.
- Structure and technical content transposed from EN 50128.
- Minor technical changes.

Changes in EN50716:2023

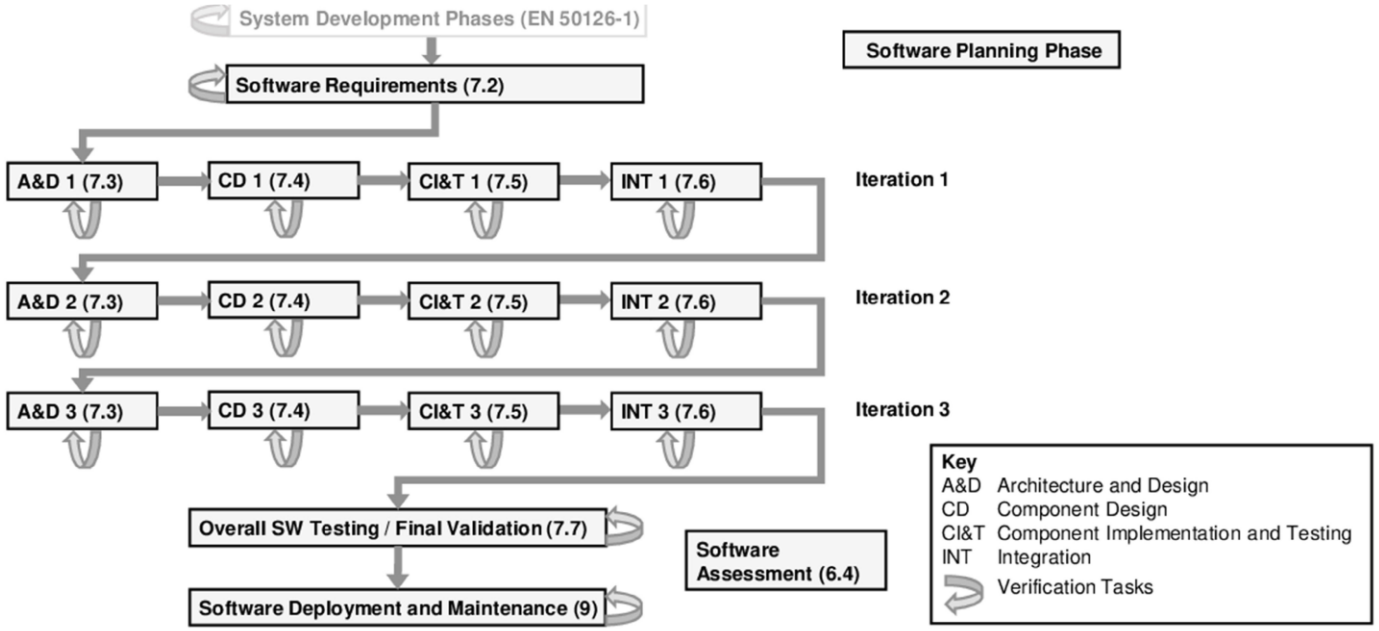
M&IT awards 2021
BRONZE WINNER

- Merged with EN 50657:2017
- Role independence requirements simplified → Various special cases and relaxations dropped
- Additional guidance on:
  - Alternative Lifecycles
  - Modelling → 
  - AI/ML → Caused some alarm in the AI community

Not this sort!

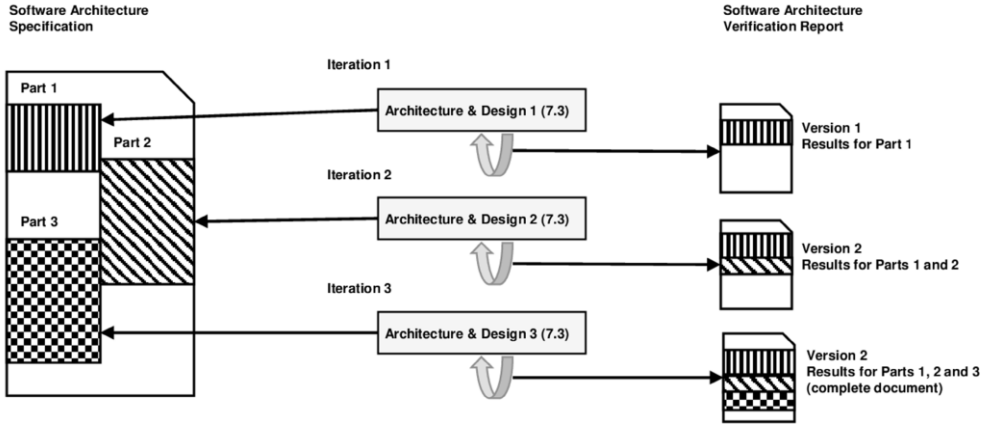
Also detailed changes in recommended techniques, e.g. recommending properties of programming languages rather than specific languages.

Lifecycles



Example of Iterative Lifecycle

Guidance is given on iterative alternatives to the classic linear V lifecycle



Example of iterative development of a work product

Modelling

M&IT awards 2021
BRONZE WINNER

"A model is a logical representation aimed at developing, understanding, communicating, or explaining aspects of a system, entity, or process."

The annex provides guidance on how to apply the requirements of the standard when modelling is used in software development.

Table C.2 — Component implementation and testing typical adaptation for modelling

SUBCLAUSES	TYPICAL ADAPTATION FOR MODELLING
7.5.4.2 The size and complexity of the developed source code shall be balanced.	7.5.4.2 The size and complexity of the developed model shall be balanced.
7.5.4.3 The Software Source Code shall be readable, understandable and testable.	7.5.4.3 The model shall be readable, understandable and testable.
7.5.4.4 The Software Source Code shall be placed under configuration control before the commencement of documented testing.	7.5.4.4 The model shall be placed under configuration control before the commencement of documented testing.

During the years between 1980 and the appearance of the first version of the standard in 2001, much work was published on representations (models as defined above by EN50716) which would have alleviated some of the problems of system development. The delay in their recognition is surprising.

AI and Functional Safety – State of the Art

BRONZE WINNER

PD ISO/IEC TR 5469:2024

BSI Standards Publication

Artificial intelligence — Functional safety and AI systems

AI technology Class III covers applications which would be classed as SIL1 – SIL 4 in EN 50716

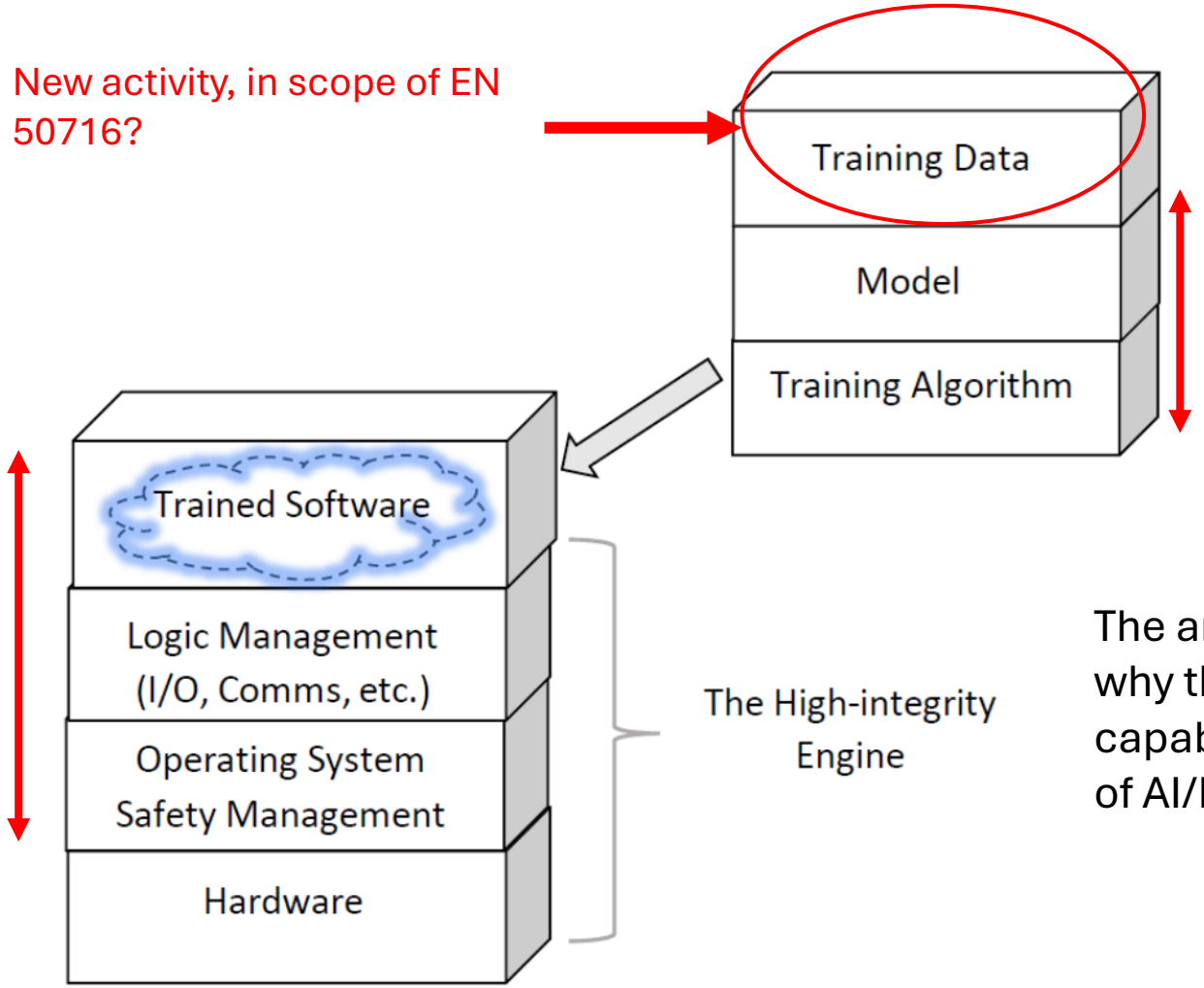
AI Technology Class => AI application and usage level	AI technology Class I	AI technology Class II	AI technology Class III
Usage Level A1 (1)	Application of risk reduction concepts of existing functional safety International Standards possible	Appropriate set of requirements (3)	At the time of writing this document no appropriate set of properties with related methods and techniques is known to achieve sufficient reduction of risk
Usage Level A2 (1)		Appropriate set of requirements (3)	
Usage Level B1 (1)		Appropriate set of requirements (3)	
Usage Level B2 (1)		Appropriate set of requirements (3)	
Usage Level C (1)		Appropriate set of requirements (3)	
Usage Level D (2)	No specific functional safety requirements for AI technology, but application of risk reduction concepts of existing functional safety International Standards		

AI Classification Table from TR 5469

AI/ML Gaps in EN50716

BRONZE WINNER

New activity, in scope of EN 50716?



EN 50716

Revised lifecycle and some new or enhanced techniques

EN 50716

New or enhanced V&V techniques needed

The High-integrity Engine

The annex to EN50716 explains why the current version is not capable of ensuring the safety of AI/ML applications.