www.thalesgroup.com/germany

Leittechnik für Bahnsysteme mit Eclipse

Software-Entwicklung bei Thales Transportation Systems GmbH

Christian Scholz

Sicherheit und Mobilität in einer vernetzten Welt.

THALES

Content

- HMI for Railway Operators
- HMI Technics
- HMI Safety and Reliability
- Agile and CENELEC
- Organzational Aspects Safe HMI
- Questions

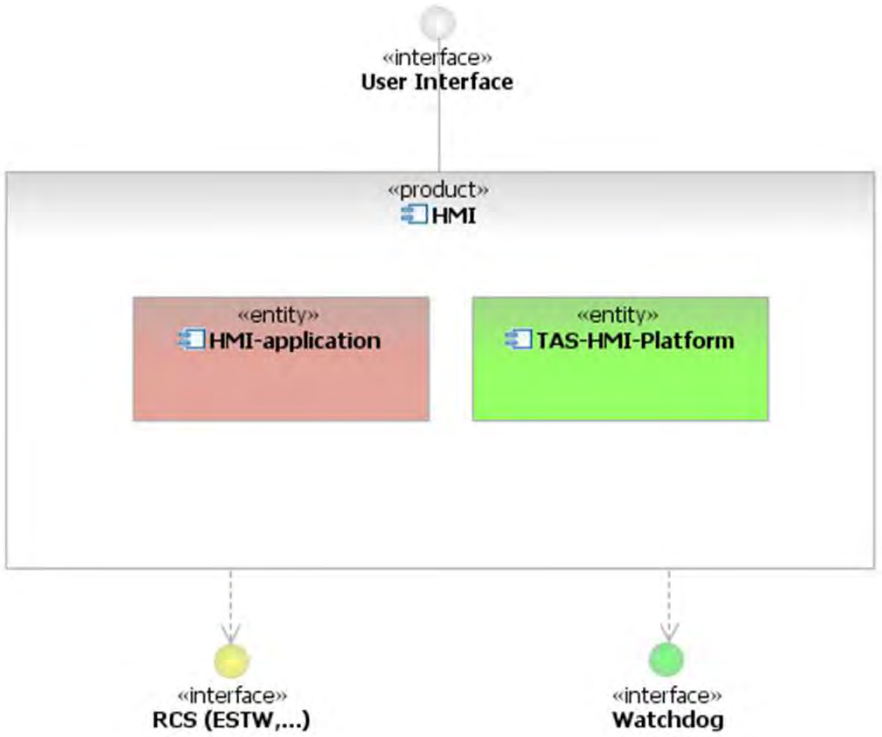
THALES

Content

- HMI for Railway Operators
- HMI Technics
- HMI Safety and Reliability
- Agile and CENELEC
- Organzational Aspects Safe HMI
- Questions

THALES

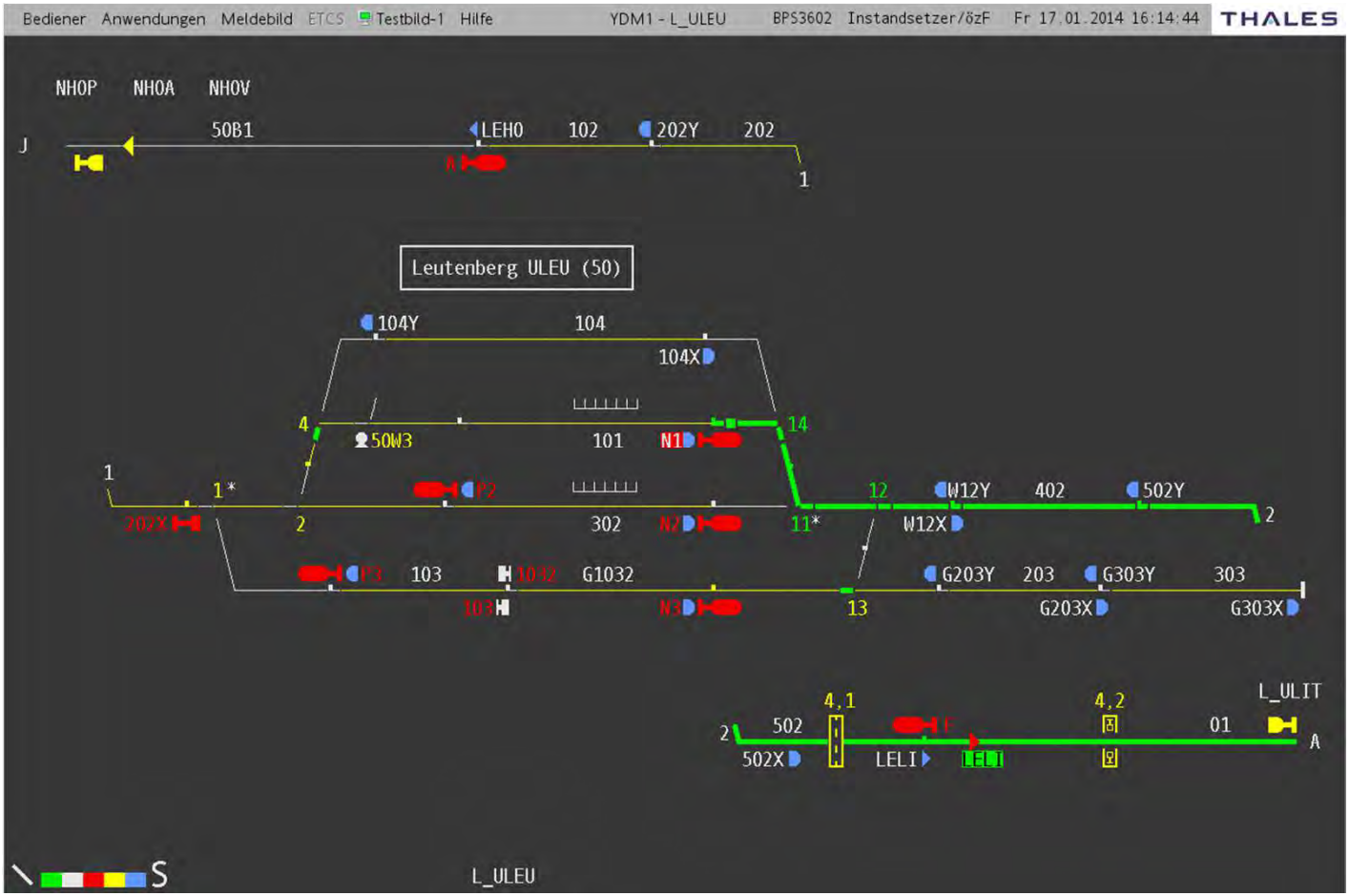
HMI for Railway Operators



- HMI application based on the TAS-HMI-Platform
- Connects Railway Control Systems to operational personal
- Provides a Human-Machine-Interface
- Maintenance and operational activities keeping the Railway System in safe and efficient state.
- Provides a human comprehensible representation of different aspects of Railway Control Systems and capabilities to influence the state

THALES

Track Perspective



- Visualization of element states
- Safe display
- Operator can rely on the displayed states

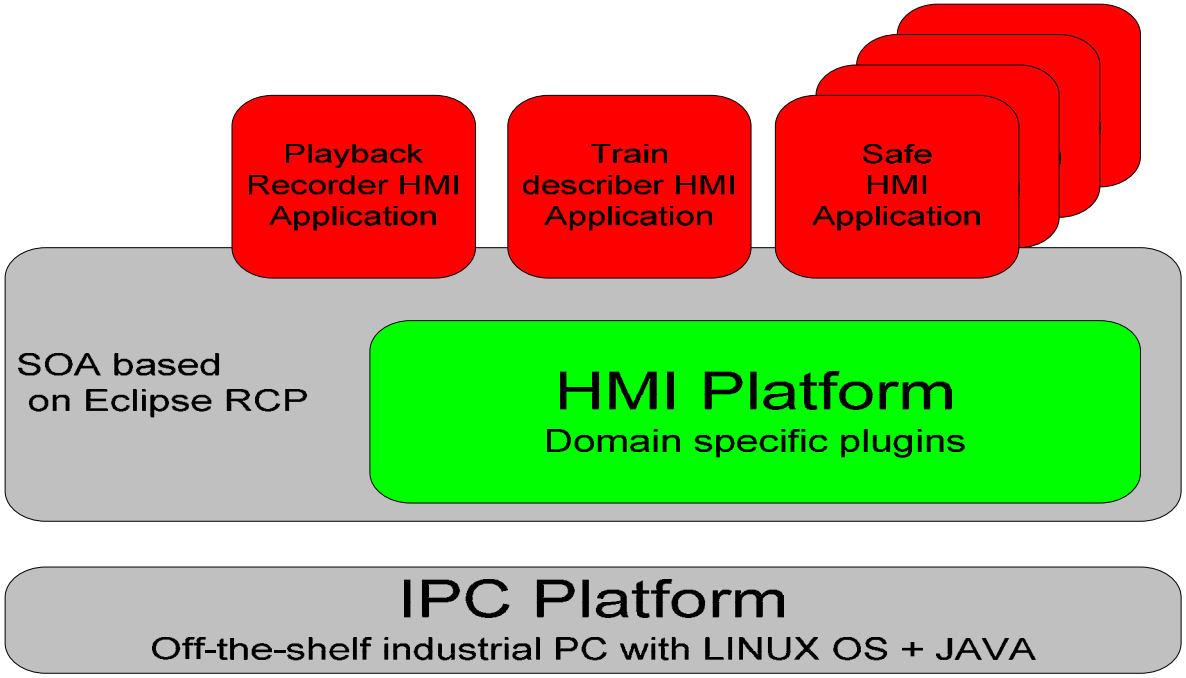
THALES

Content

- HMI for Railway Operators
- HMI Technics
- HMI Safety and Reliability
- Agile and CENELEC
- Organzational Aspects Safe HMI
- Questions

THALES

Concept of Safety HMI



- Usage of standard PC hardware
- Software Architecture based on Eclipse RCP
- HMI Platform – Core plugins
  - Safety services
  - Visualization services
- HMI Application
  - Customer specific plugins
- Increasing Productivity by setting up a domain middleware and focusing on application software

THALES

Technology - Safety HMI

- **Technological background**
  - Extensible Domain specific middleware with Eclipse Rich Client Platform
  - State of the art technical software based on LINUX and latest JAVA technology
  - Future safe 2D graphics with SVG and OpenGL
  - Data Generation and Exchange based on wide spread XML Technologies (e.g. XSD & XSLT)
  - Domain Modelling – Railway MIB (pre-engineered rail world on Domain level)
  - MIB: base for CAE data generation and Code generation
  - Excessive usage of Open Source components Eclipse RCP, JGroups, log4j
  - Common look & feel of HMI applications forced by Eclipse SWT Widget Toolkit
  - Multi Monitor Support

HMI in TTS

- **Mission-Critical and Safe HMI for Display and Commands**
- For Transportation System, related skills includes:
  - Railway Teams (Railway Control System Model)
  - Graphic engine - 2D graphics with SVG and Open GL
  - User Interfaces (Eclipse SWT Widget Toolkit)
  - Interface designers (Communication Adapter: Ilx, ETCS, ARAMIS, Automatic Route Setting, others)
  - Software engineers implementing User Interfaces (Plugins, Authorisation and Authentication, Alarm and Diagnose Interface)
  - Extensible Domain specific HMI middleware & tools (Eclipse RCP)
  - Extensive Usage of Open Source
  - Data Generation and Exchange based on wide spread XML Technologies
  - HW: COTS Components

Content

- HMI for Railway Operators
- HMI Technics
- **HMI Safety and Reliability**
- Agile and CENELEC
- Organzational Aspects Safe HMI
- Questions

THALES

Temporary Speed Restrictions

Derailment
Rheinweiler 1971

- **Safety aspects TSR**
  - Temporary Speed Restriction limit speed of automatically guided trains
  - Reasons for temporariness:
    - Damages in track system
    - Work on tracks or bridges
    - Windstorm hazards
  - It is necessary to ensure that speed is limited
    - to the correct value and
    - At the correct position on the line
  - Otherwise the speed of the trains may exceed the highest possible value, which lead to a derailment:

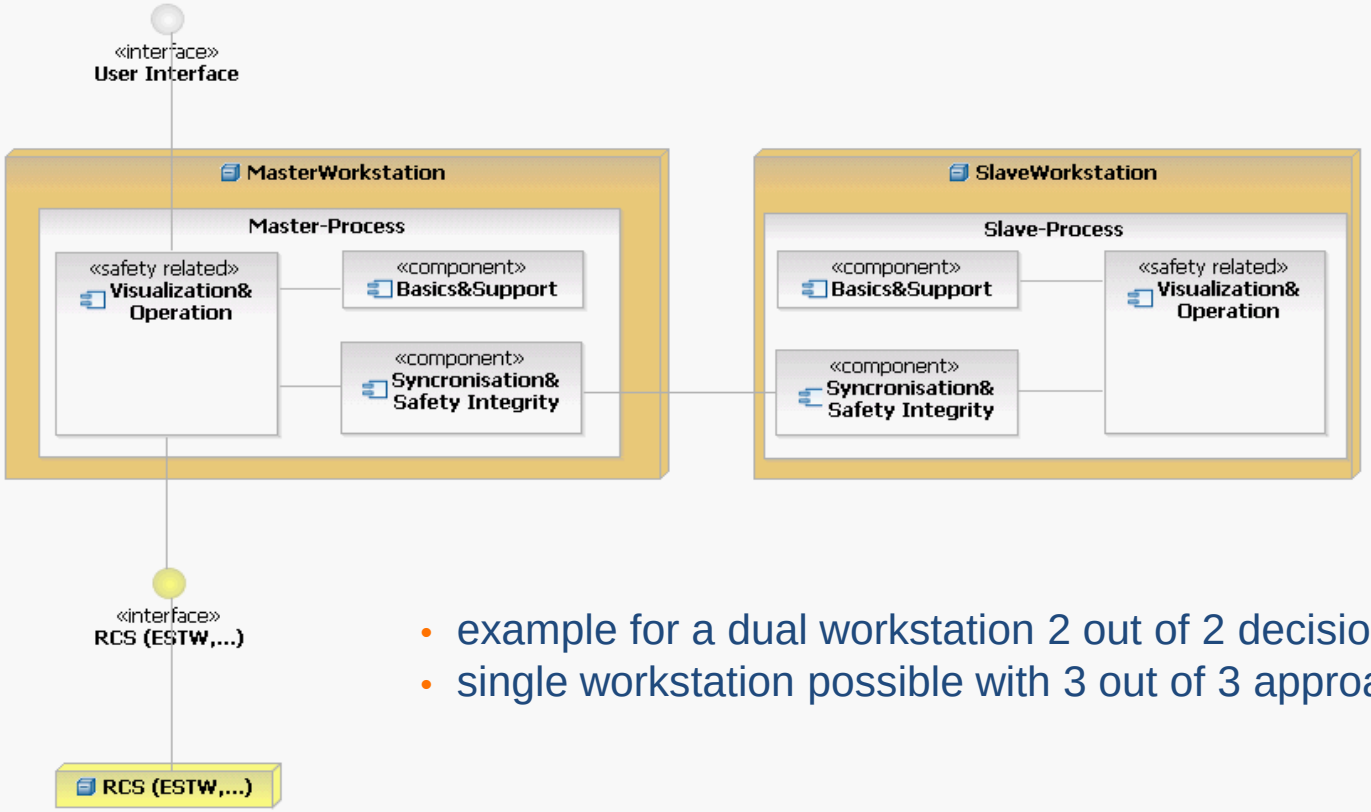
THALES

Justification Fail Save HMI

- **Example SIL 0 functions**
  - Disposition Client on HMI
  - Setup Route via regular operation
- **Example SIL 2 functions**
  - Manual Cancel Route
  - Temporary Speed Restriction
  - Barrings
  - Level Crossing remote controlled
  - Written order to a train
- **Example SIL 4 functions**
  - Manual and critical operator commands
- **Depending on the operational needs the Safety integrity level may vary**

THALES

Safety HMI Architecture



- example for a dual workstation 2 out of 2 decision approach
- single workstation possible with 3 out of 3 approach

THALES

Online Verification

- **OLT SIL 2**
  - Master/Slave Picture Verification
  - Master/Slave Data model verification
  - Master/Slave Read back of video memory
  - Test element check covering common parts of software
  - CPU/JVM check
  - Resource supervision
  - Safe state for unexpected failures incl. Check that safe state is reachable
  - Safety guard for controlled access API
  - Check timeliness and responsiveness
  - De-synchronize master / slave, different JVM configuration
- **OLT Transition SIL 2 to SIL 4 (COTS treatment)**
  - Verification of correct function of use COTS SW
  - Continuous frozen area check
  - Provide external check program diversely implemented

Content

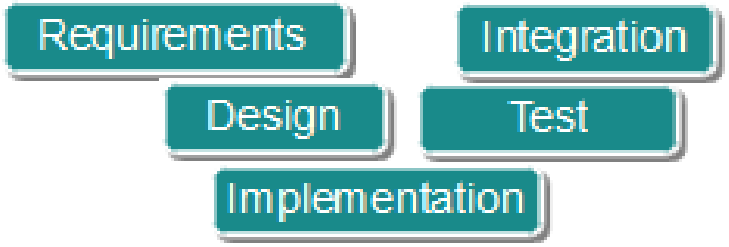
- HMI for Railway Operators
- HMI Technics
- HMI Safety and Reliability
- **Agile and CENELEC**
- Organzational Aspects Safe HMI
- Questions

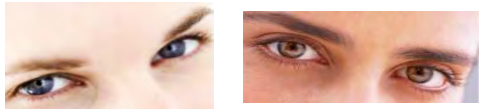
THALES

Agile Software Development – CENELEC?

Detailed study of CENELEC EN 50128

- **Assumption: Standard asks for traditional V-Model**
- **Goal of the standard**
  - Reduce systematic errors – down to a tolerable level
  - By setting standards on the process
- **Requires mandatory development phases**
  - Strict sequence is impractical
  - Accommodates refinement, prototyping or incremental approaches
- **Additional software assurance activities**
  - Verification, Validation and Assessment
    - Obey rules of interdependency
    - Two pairs of eyes are better than one





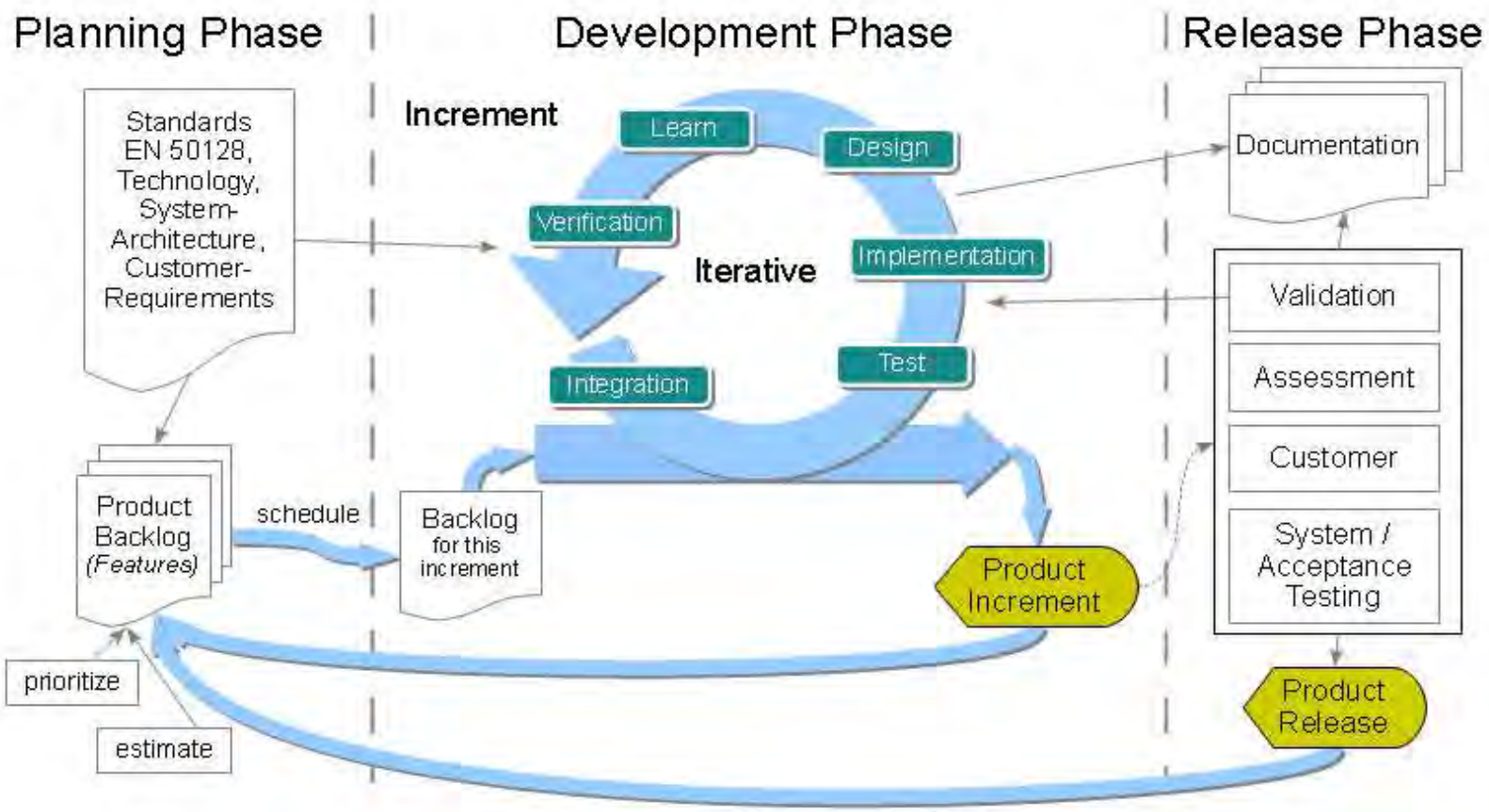
THALES

Results

- **Standard and Agile – analogue objectives**
  - Aim for quality
  - Big focus on testing
- **Agile's incremental and iterative approach – allowed**
- **Simple agile approach needs enhancements**
  - Additional assurance activities
  - More documentation
  - ✓ Agile methodologies are highly adaptable
- **Define own process life cycle model**

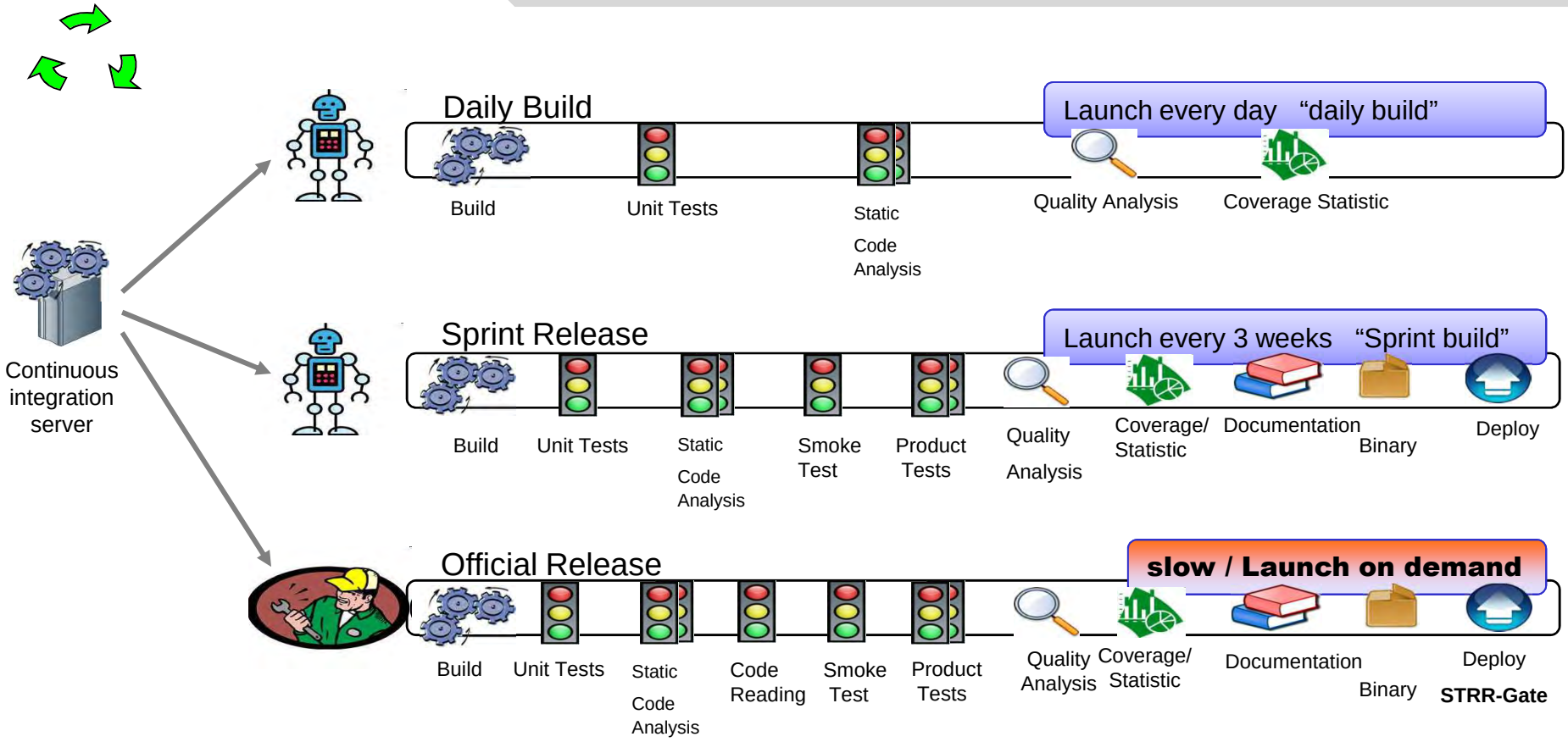
THALES

Safety-related agile software process model



THALES

Continuous Integration HMI detailed



THALES

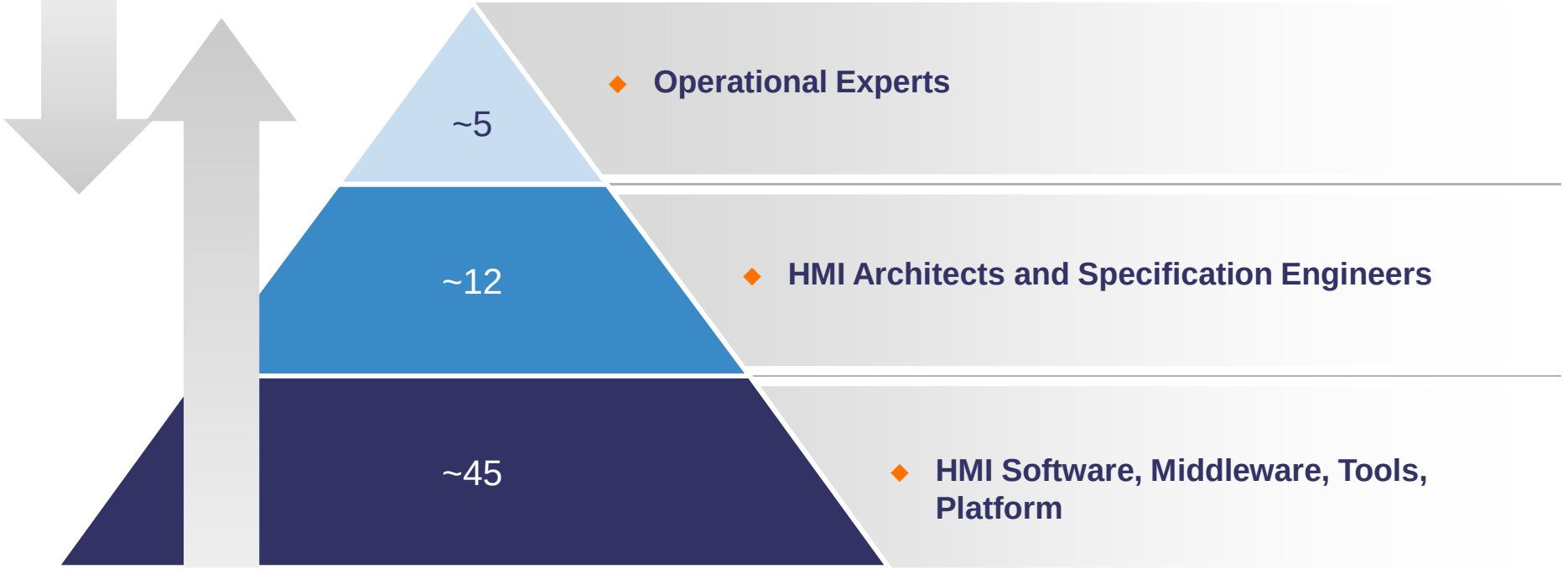
Content

- HMI for Railway Operators
- HMI Technics
- HMI Safety and Reliability
- Agile and CENELEC
- **Organzational Aspects Safe HMI**
- Questions

THALES

TTS situation / safety critical HMI

Customer



- **Operational Experts**
- **HMI Architects and Specification Engineers**
- **HMI Software, Middleware, Tools, Platform**

THALES

THALES

Content

- HMI for Railway Operators
- HMI Technics
- HMI Safety and Reliability
- Agile and CENELEC
- Organzational Aspects Safe HMI
- Questions

THALES