Ensure Safety for Rail Projects
from planning to operation

René Bambor,
Business Unit Manager - Rail Services , TÜV SÜD

Add value.
Inspire trust.

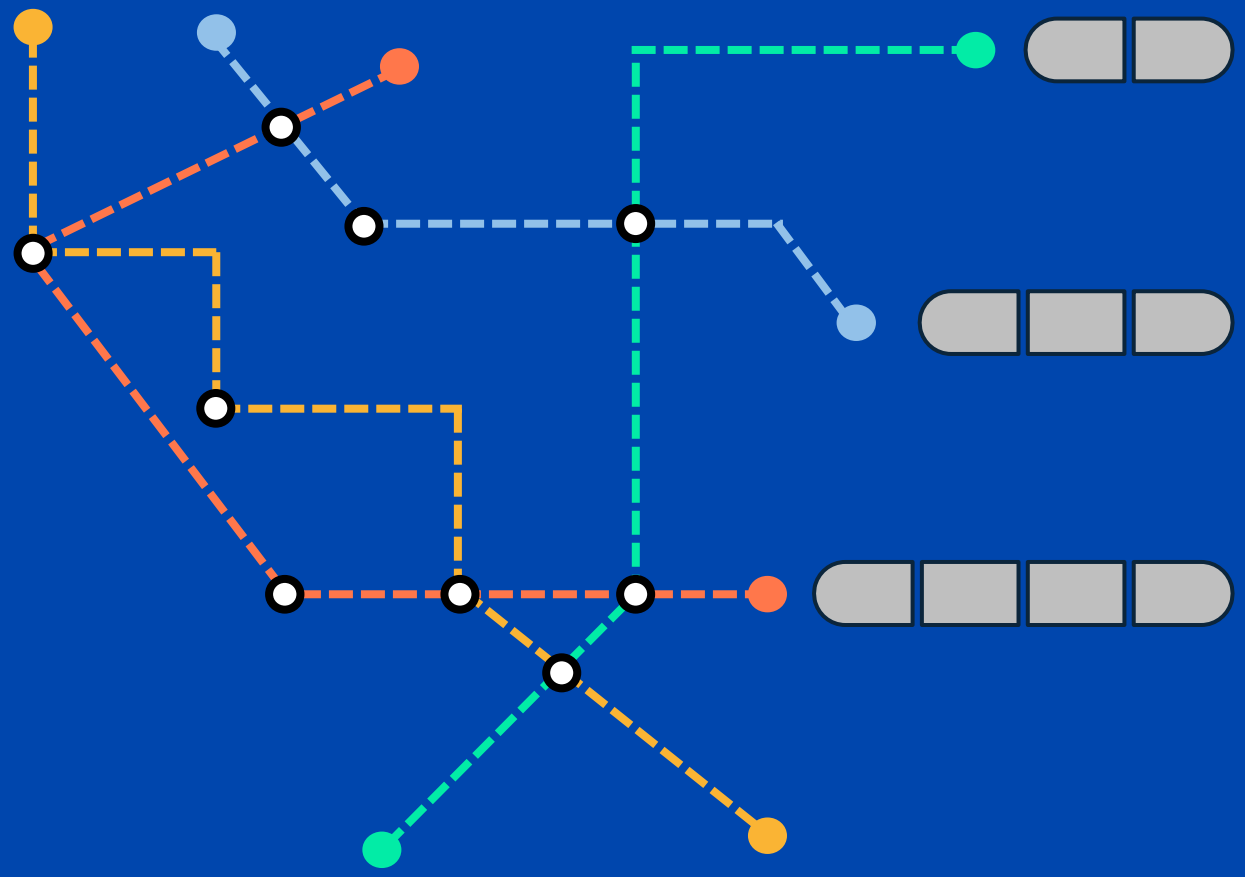
“I want to take you on a journey”

- “Rail – transport of today and future”
- Safe and reliable mobility
- Most sustainable mode of transport
- Industry drive innovations, safety and addressing passengers’ comfort
- Increasing railway projects, need for faster realization

Ensuring safety from planning to operation is key.

Jump on **and let’s go ahead.**

Agenda

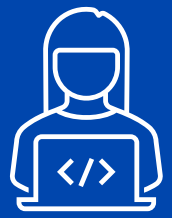


- Stakeholder, trends and challenges
- Rail project lifecycle and examples
- Independent Safety Assessment Bodies (ISA)

Different stakeholder, different expectations

Passengers

Comfortable, reliable and safe transport



Authorities

Technical / legal safety framework

Safety targets / safe operation

Zero accidents

Operators

Efficient, reliable, safe operation & maintenance

Owner / Contractor

Competitive price, high quality of public transport

Turnkey Supplier

Economic rail systems

Safe integrated systems

Subsystem Supplier

Provide competitive subsystems

Compliant to safety regulation

Rail lifecycle: Trends and challenges

PLANNING AND DEVELOPMENT | MANUFACTURING AND INSTALLATION | OPERATION AND MAINTENANCE | MODIFICATION AND DECOMMISSIONING

TRENDS

- More sustainability
- Urbanization
- **Cyber security / AI**
- **Fully automated operation**
- High performance
- Global supply chains
- …

CHALLENGES

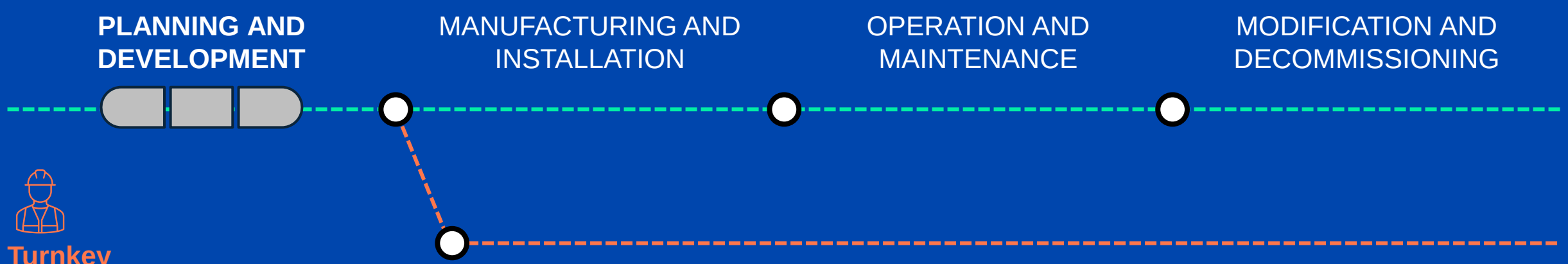
- Increasing regulations
- High safety demands
- **High complexity**
- **New technology**
- Lack of skilled workers
- **Challenging risk management**
- Faster realization demands

How safe is safe enough?

Safety (*noun*)

1. “Condition of being protected from or unlikely to cause danger, risk, or injury.“
   [Dictionary]
2. “Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment”
   [MIL-Std-882C]
3. “Freedom from **unacceptable** risk.”
   (*note: risk related to human health or to the environment*)
   [EN 50126-1]
4. “Condition in which risk of harm to persons or damage to property is reduced to, and maintained at an **acceptable level** through continuing process of hazard identification and risk management.”
   [ARP 4761A]

Planning and Development



Turnkey Supplier

- Concept phase
- **Preliminary design**
- **Risk analysis**
- Final system design
- Subcontracting
- Supplier management
- Subsystem design

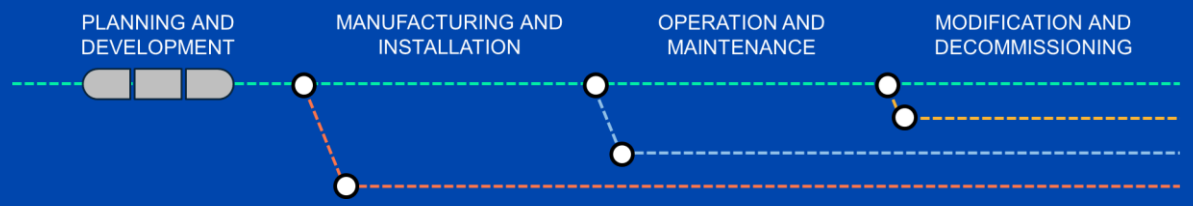
Challenges:

- **Right architecture & allocation of system (safety) requirements**
- **Handling shared/exported risks**
- Feasible RAMS targets
- Handling safety-related application conditions (SRAC)
- **Transparent interfaces**
- Suitable quality gates

Solutions:

- Early O-ISA involvement
- **Interface management**
- **Integral safety view**
- Analyze use cases
- Focus on shared risks

Ensuring safety during Planning and Development



Real example:
Subway GOA4 using CBTC/ATC system

Vehicle subsystem

Identified hazard:

- Passengers fall off moving train after untimed emergency door opening

Safety requirements:

- After emergency door switch activation door remain closed until standstill, release at v = 0

CBTC/ATC subsystem

Identified hazard:

- Collision between vehicles due to running trains into occupied sections

Safety requirements:

- Route setting ensure occupied sections set zero-speed zone around occupied section

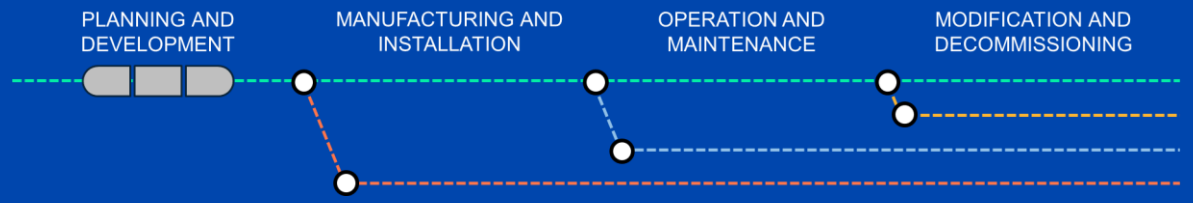
Missing hazard on system level:

- People exiting vehicle might suffer electrocution by powered rail or hit by other vehicles (2nd line)

Missing safety requirement (vehicle to ATC):

- Immediate depowering of power rail
- zero-speed zones (2nd line or full-stop)
- Activated video surveillance

Ensuring safety during Planning and Development



Results and measures:

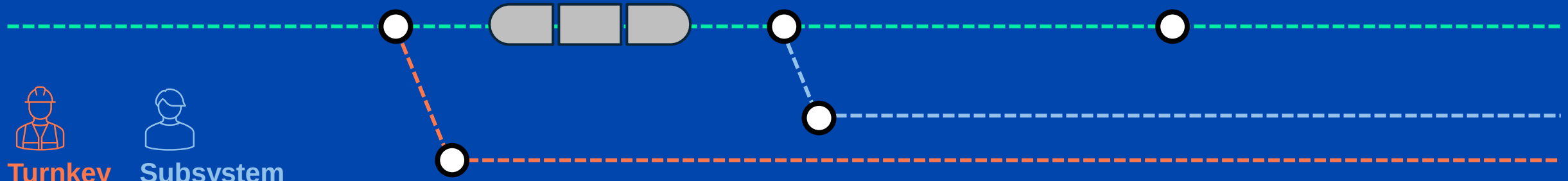
- Subsystems correctly faced own hazards / risks
- Use case evaluation & system level hazard identification was partly missing
- Overall-ISA was engaged at very late stage of project from System Integrator
- **Missing system view**, major delays and add. costs

How can this be avoided:

- Engage Overall-ISA on system level from beginning
- Focus on shared / exported risks and mitigations to operation
- Align Subsystem ISA with the Overall ISA to prevent safety gaps

Manufacturing and Installation

PLANNING AND DEVELOPMENT | **MANUFACTURING AND INSTALLATION** | OPERATION AND MAINTENANCE | MODIFICATION AND DECOMMISSIONING



Turnkey Supplier | **Subsystem Supplier**

- Production
- Manufacturing
- **Installation**
- Integration
- **Testing and commissioning**
- Acceptance

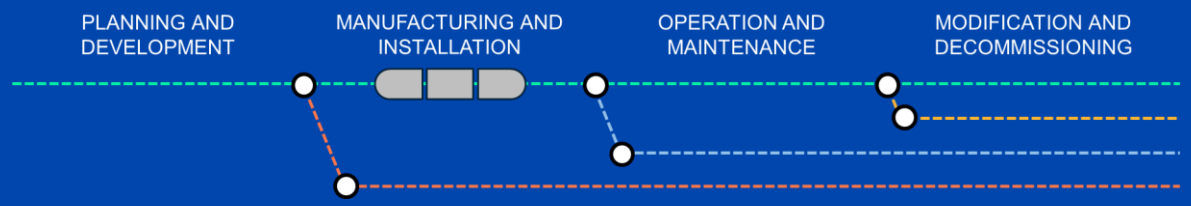
Challenges:

- New technologies
- Compatibility of subsystems
- Quality issues
- Integral vs. subsystem testing
- **Coping of non-conformities**
- **Change Management**

Solutions:

- **Robust Change Management regarding Safety**
- Synchronized Validation & Verification
- Expert steering groups
- Interface testing / integration
- Assessment of Factory Acceptance Tests (FAT)

Ensuring safety during Manufacturing and Installation



Real example:

Unintended safety brakes of tram

- Mixed mode of operation (manual & fully-automated)
- Brake-curves monitoring active in both modes (specified for automated operation)
- During testing **many unintended spurious safety brakes** occurred in manual mode
- High pressure for Permit to Operate

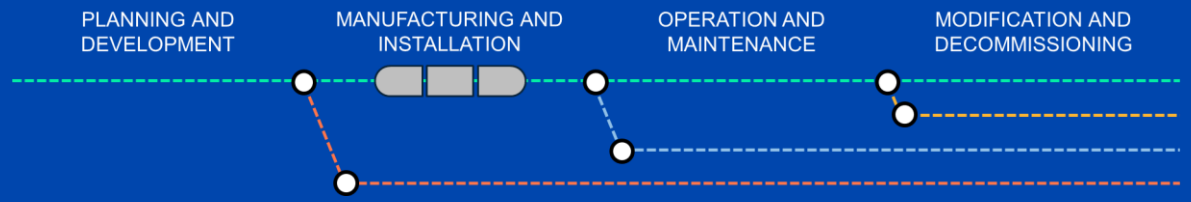
Vehicle and ATC subsystem:

- Not aligned requirement **specs for different operation modes** leading to design changes
- During change management many discussions if **unintended safety brakes are hazards or not**
- Misunderstandings on safety targets / specified reactions
- High number (>10) of safety brakes caused **increased risk for passengers**, (if not preventing accidents)

Consequences from a system safety perspective:

- **Proper risk-analysis** (integrated in Change Management) could have avoided this back-and-forth discussion

Ensuring safety during Manufacturing and Installation



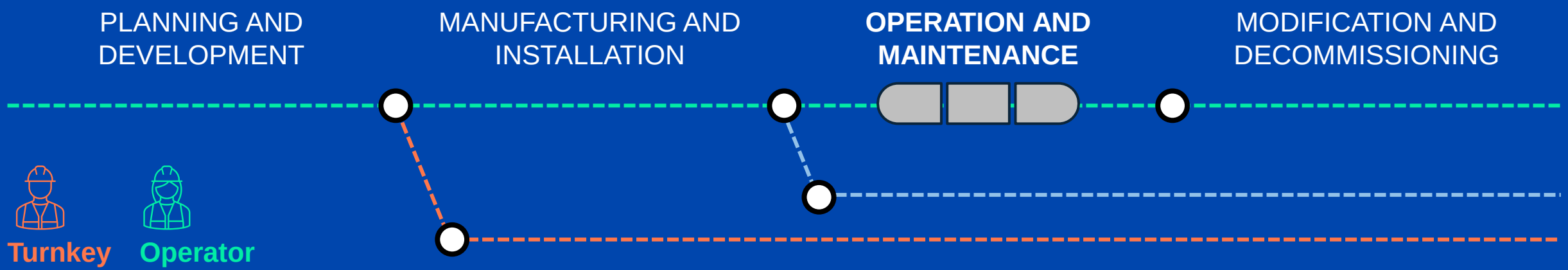
Results and measures:

- System behavior not properly specified
- Testing revealed gaps, huge efforts for correction
- Consequences of safe reactions not properly evaluated on system level
- Extensive stakeholder discussions in late project phase caused further delays

Support of an Independent Assessor:

- Focus on proper change management, considering safety impacts
- Focus on shared / exported risk and mitigations
- Manage interfaces between subsystems to avoid shifting risks and responsibilities back and forth

Operation and Maintenance



Turnkey Supplier

- **Staff training / qualification**
- **Operating the System**
- Maintenance
- Monitoring
- Safety Management

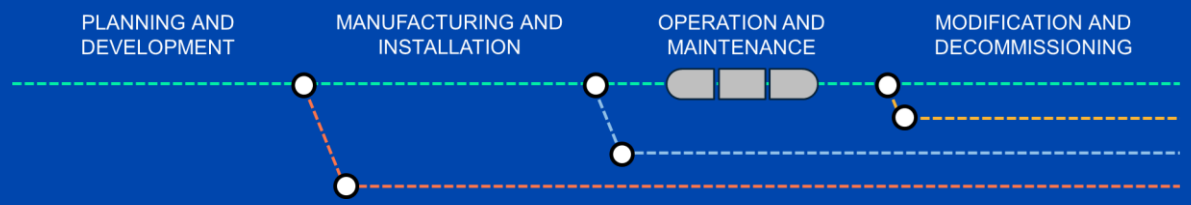
Challenges:

- **Readiness to operate**
- Qualified staff
- **Comprehensive manuals**
- Management systems
- Responsibility takeover

Solutions:

- **Define acceptable risk level based on system maturity**
- Management system certification
- **Transparency of manuals**
  etc. prior to operation

Ensuring safety during Operation and Maintenance



Real example:

Inadequate operating manuals for driver

- Driver's manual handed over to operator
- Temporary instructions with **some hundred compensation measures** (immature vehicle)
- Driver was not trained on temporary instructions
- Authorization was granted
- Many critical situations in operation

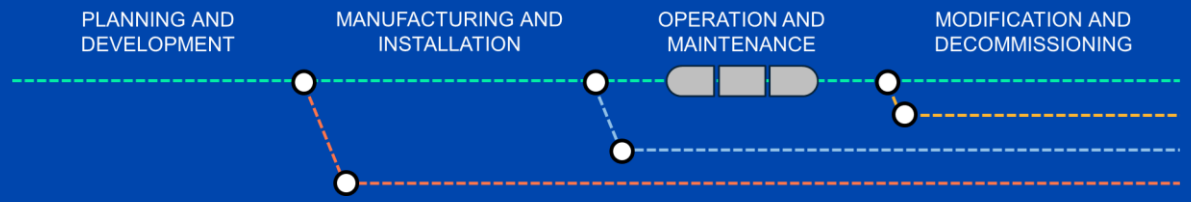
Root causes:

- Too many technical deficiencies solved by temporary restrictions / instructions
- Human reliability reduced due to complexity
- Operator didn't follow SMS procedures

System safety perspective:

- Fixing technical deficiencies by paper is no solution
- Holistic view to systems / subsystems including "How to operate" and human behavior needed
- Understand different stakeholder interests

Ensuring safety during Operation and Maintenance



Results and measures:

- Main supplier interest - vehicle authorization - overruled **demand for technical maturity**
- Work-arounds on paper to solve deficiencies
- **Human behavior** to deal with complexity ignored
- Basic concept of “Safety of Machinery” neglected

Support of Independent Assessor

- **Assess appropriateness** of application conditions incl. manuals / instructions
- Highlight conditions and instructions with **intention to close open technical issues**
- Mediation of interests related to safety and reliability

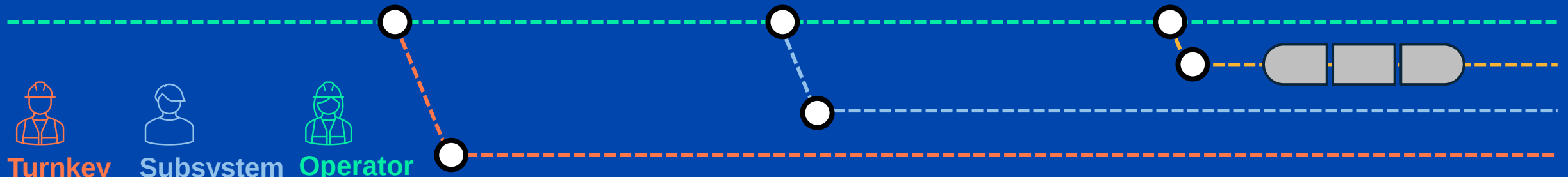
Modification and Decommissioning

PLANNING AND DEVELOPMENT

MANUFACTURING AND INSTALLATION

OPERATION AND MAINTENANCE

MODIFICATION AND DECOMMISSIONING



Turnkey Supplier | **Subsystem Supplier** | **Operator**

- Modifying functions / new technology
- **Obsolescence Management**
- Second source / spare parts
- Operational changes

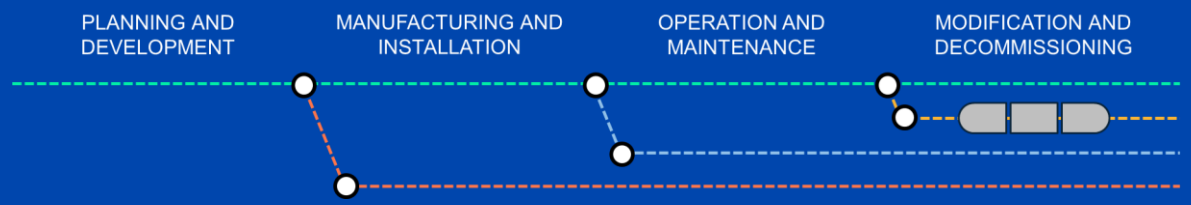
Challenges:

- **Impact on safety**
- Impact on interfaces
- Impact on mission profile
- Adequate documentation
- Responsibility limitations

Solutions:

- **Robust Change Management regarding Safety**
- Ensure availability of proper system documentation
- **Proper impact analysis** before modifying

Ensuring safety during Modification / Decommissioning



Real example:

Replacement of brake discs / pads

- Obsolescence of parts led to replacement
- OEM out of warranty
- Replacement based on dimensions, driven by costs
- No impact analysis
- Changes indicated to authority as minor

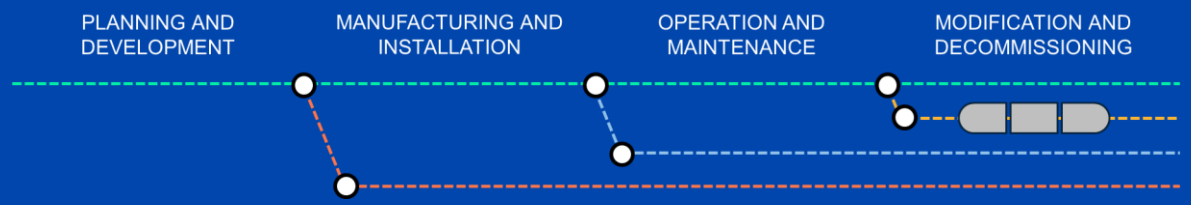
Identified gaps:

- Vehicle brake behavior not seriously evaluated
- Impact to maintenance procedures, change intervals, installation etc. not properly considered
- Proof of safety not valid anymore

System safety perspective:

- Modification evaluated via impact analysis needed
- Including technical, operational & maintenance aspects
- Safety-related changes must follow risk management life cycle
- Entity in Charge of Maintenance processes

Ensuring safety during Modification / Decommissioning



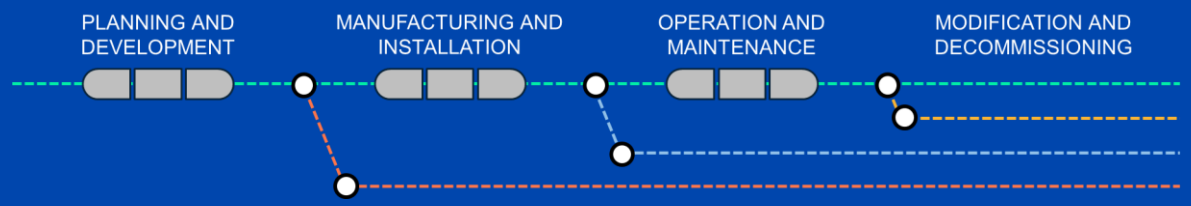
Results and measures:

- Impacts seen from operational / practical aspect only
- Safety impacts not properly evaluated
- Initial vehicle documentation incomplete
- Maintenance entity neither trained nor experienced in risk management procedures
- Maintenance management system not in place

Support of Independent Assessor:

- Certify maintenance management systems
- **Proper impact analysis**, independently evaluated
- Back into life cycle - starting with design
- Reveal safety requirements to **demonstrate min. same level of safety** as without change

Safety with innovations / new technologies



Real example: **Hydrogen powered train**

- Designed with focus on technical risks only
- Only safety requirements related to gas tightness of pipes, pressure tanks, valves etc. considered

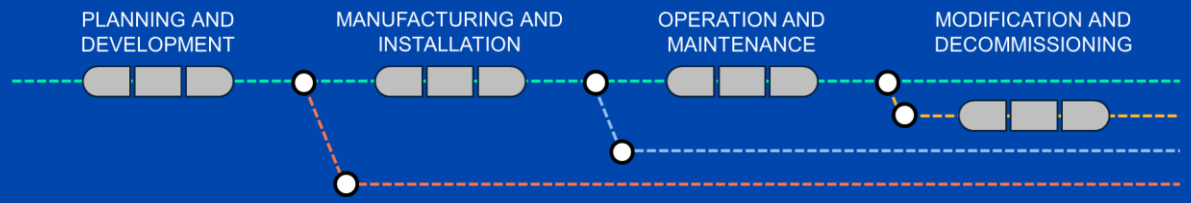
Identified gaps:

- Additional operational risks from maintenance, parking and refueling not seen
- Essential risks for refueling neglected (similarity assumptions from road vehicles)

System safety perspective:

- Holistic approach for new technologies and innovations
- Risk evaluation / use case analysis for entire system including technology, operation and maintenance
- Conventional risk-free situations may be different

Added value from Independent Safety Assessors



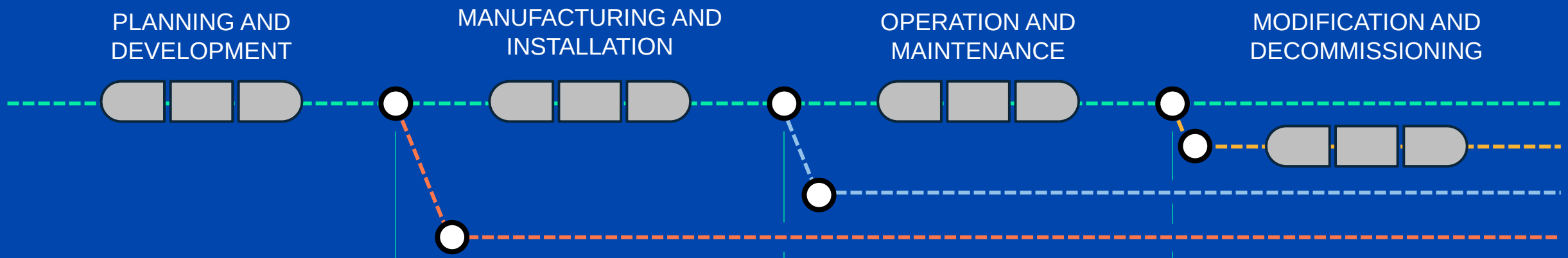
Provide ISA and O-ISA services:

- Identify gaps arising from poor interface management
- Holistic view, combining technology, operation, maintenance and human behavior
- Protect different stakeholder interests without bias
- Avoid shifting of risks and mitigations between subsystems
- Latest technological expertise ensures innovative solutions

Provide advisory and trainings:

- Risk management processes, standards, regulations etc.
- Narrow gaps between stakeholders & independent bodies
- Operation and Maintenance trainings including SMS, ECM..
- Methods, principles and risk management setup to ensure safety perspective and holistic view of staff

TÜV SÜD services in a nutshell, some examples…



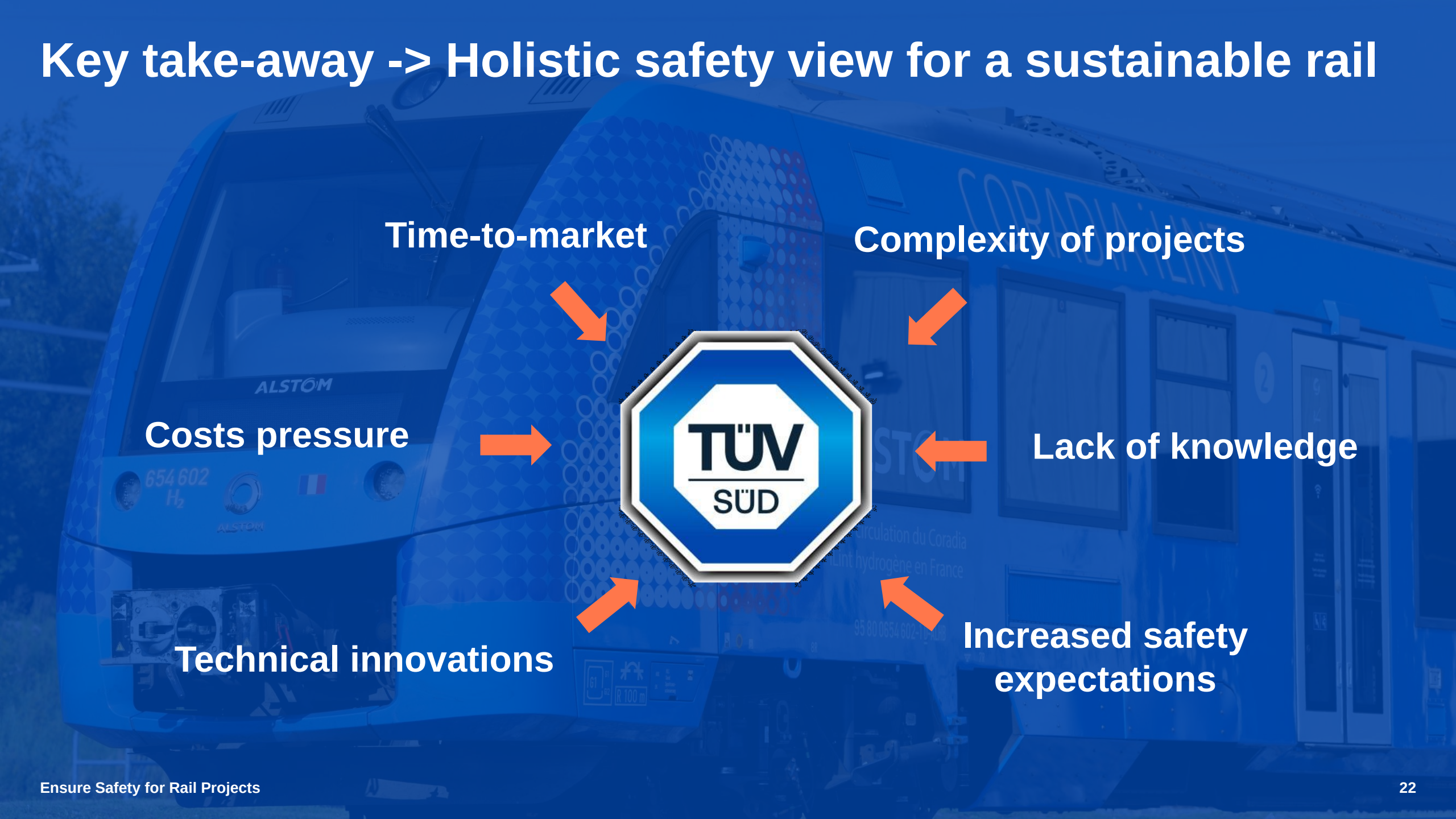
- Overall-Independent Safety Assessment
- Assessment of subsystems, interfaces
- Advisory for new technologies
- Advisory for safety-related standardization / regulation
- …

- Overall-Independent Safety Assessment
- Assessment of subsystems, interfaces and **integration**
- Independent V&V
- Construction supervision, quality control / safety audits
- …

- SMS / ECM advisory and certification
- Rail-specific trainings with personal cert. program
- Comprehensive Training Operation Managers
- …

- Independent impact analysis
- Assessment of IT security
- …

Key take-away -> Holistic safety view for a sustainable rail



We are happy to support you…

René Bambor

Business Unit Manager - Rail Services

Mobile: +49 151 20450658
rene.bambor@tuvsud.com

tuvsud.com/globalrail

Mohamad Afiq

Business Development – Rail Services
Region ASEAN

Mobile +6019 334 1225
afiq.samad@tuvsud.com

www.linkedin.com/in/mohamadafiqabdulsamad/