Autonomous Truck Safety Certification

Motius GmbH
December 15, 2025 14:39 (451eeaf)

Autonomous Truck Safety Certification

Safety Engineering Autonomous Logistics

For a pioneer in autonomous trucking technology, Motius developed a comprehensive safety engineering framework enabling TÜV certification for autonomous transport solutions deployed within critical infrastructure. This project demonstrates how rigorous safety processes and certification expertise can accelerate market readiness for safety-critical autonomous systems.

This showcases how companies like Koenig & Bauer can navigate complex regulatory landscapes to bring autonomous technologies from prototype to certified commercial deployment.

The Challenge

Autonomous logistics faces stringent regulatory and safety requirements, particularly for critical infrastructure deployment:

- **Regulatory complexity**: IEC 61508 functional safety standards require extensive documentation and process compliance
- **Safety-critical operations**: Autonomous trucks operating in ports, logistics hubs, and industrial facilities demand SIL-2 certification
- **Cybersecurity threats**: Connected autonomous systems vulnerable to attacks requiring IEC 62443 compliance
- **Certification timeline pressure**: TÜV homologation process can delay market entry by years without proper preparation
- **Process maturity gaps**: Startup development practices often misaligned with safety certification requirements
- **Multi-domain integration**: Autonomous systems combining perception, planning, and control requiring holistic safety approach
- **Critical infrastructure deployment**: Ports and logistics facilities have zero tolerance for safety incidents

The customer, advancing autonomous trucking technology as part of Germany's ATLAS-L4 consortium, needed to achieve TÜV certification readiness while maintaining rapid development velocity.

Technical Innovation

Safety Software Gap Analysis

Comprehensive evaluation bridging existing practices with certification requirements:

- **IEC 61508 compliance assessment**: Detailed gap analysis of Parts 1 and 3 covering functional safety management
- **Process maturity evaluation**: Identifying discrepancies between current development workflows and safety standards
- **Actionable remediation roadmap**: Proposing specific corrective measures with implementation priorities
- **Agile gap tracking**: Implementing continuous monitoring system for addressing identified deficiencies
- **FSM compliance validation**: Ensuring functional safety management meets auditor expectations

Safety Software Development Lifecycle Redefinition

Restructured development processes aligned with certification standards:

- **IEC 61508-3 alignment**: Comprehensive lifecycle covering safety planning through validation
- **Integrated verification**: Safety checks embedded at every development stage, not as afterthought
- **Documentation framework**: Automated evidence collection supporting certification audit trail
- **Tool qualification**: Ensuring development and verification tools meet safety integrity requirements
- **Traceability architecture**: Linking requirements through implementation to validation test cases

System Safety Analysis

Rigorous hazard analysis and risk mitigation:

- **Single fault scenario evaluation**: Analyzing potential failures in system elements and software designs

- **FMEA implementation**: Systematic identification of failure modes and effects in autonomous operations
- **Safety function integrity**: Ensuring critical functions maintain integrity under fault conditions
- **Hazard and risk assessment**: Quantifying risks and demonstrating ALARP (As Low As Reasonably Practicable)
- **Safety architecture validation**: Verifying redundancy and fail-safe mechanisms in system design

Cybersecurity Assessment

Comprehensive security evaluation for connected autonomous systems:

- **IEC 62443 compliance**: Applying industrial automation cybersecurity standards to autonomous trucks
- **Threat modeling**: Identifying potential attack vectors and system vulnerabilities
- **Security risk assessment**: Quantifying cybersecurity threats to safety functions
- **Defense-in-depth architecture**: Implementing layered security controls protecting critical systems
- **Security lifecycle integration**: Ensuring ongoing security management throughout product life

Collaborative Autonomy Software Development

Direct engineering support accelerating development while maintaining safety:

- **Embedded team collaboration**: Motius engineers working alongside customer development teams
- **Safety-critical software development**: Hands-on implementation support for SIL-2 components
- **Autonomy algorithm optimization**: Balancing performance requirements with safety constraints
- **Code review and verification**: Ensuring software meets MISRA and safety coding standards
- **Continuous integration safety checks**: Automated verification of safety properties in CI/CD pipeline

Implementation Results

Certification Progress

- **TÜV certification pathway established**: Clear roadmap from current state to homologation readiness
- **IEC 61508 alignment achieved**: Development processes compliant with functional safety standards
- **IEC 62443 security framework**: Cybersecurity architecture meeting industrial automation standards
- **Gap closure tracking**: Systematic elimination of compliance deficiencies
- **Audit readiness**: Documentation and evidence supporting certification submission

Process Transformation

- **Safety culture integration**: Development teams adopting safety-first mindset throughout organization
- **Accelerated certification timeline**: Structured approach reducing typical multi-year certification cycles
- **Scalable safety framework**: Processes applicable across product portfolio and future platforms
- **Tool qualification completed**: Development and verification tools certified for safety use
- **Continuous compliance**: Ongoing processes maintaining certification status through product evolution

Technical Achievements

- **SIL-2 autonomy software**: Safety-critical algorithms meeting integrity requirements
- **Fault detection and mitigation**: Robust error handling ensuring safe degradation under failures
- **Security-hardened architecture**: Cyber-resilient systems protecting against attacks
- **Validated safety functions**: Emergency stop, collision avoidance, and fail-safe mechanisms certified
- **Real-world deployment readiness**: Autonomous trucks prepared for critical infrastructure operations

Business Impact

- **Market entry acceleration**: Certification readiness enabling commercial deployments in regulated environments
- **Critical infrastructure access**: Compliance unlocking deployment in ports and logistics facilities
- **Customer confidence**: Safety certification differentiating from competitors in risk-averse markets
- **Regulatory relationships**: Established credibility with TÜV and regulatory authorities
- **Technology leadership**: Positioning as safety-focused autonomous logistics pioneer

Development Approach

Structured Safety Engineering Methodology

The project employed systematic approach balancing agility with certification rigor:

Phase 1: Gap Analysis & Planning - Comprehensive assessment of current development maturity - Detailed mapping to IEC 61508 and IEC 62443 requirements - Prioritized remediation roadmap with timeline - Resource planning and team training needs

Phase 2: Process Implementation - Safety software development lifecycle rollout - Tool qualification and infrastructure setup - Documentation templates and workflow integration - Team training on safety engineering practices

Phase 3: Safety Analysis & Validation - System-level hazard and risk assessment - Component-level failure mode analysis - Verification and validation planning - Evidence collection for certification submission

Phase 4: Cybersecurity Integration - Threat modeling and security architecture - Vulnerability assessment and penetration testing - Security controls implementation and validation - Ongoing security monitoring framework

Phase 5: Collaborative Development - Embedded engineering support for safety-critical software - Code reviews and architecture validation - Continuous integration of safety checks - Preparation for TÜV audit

Agile Safety Management

Innovative approach combining certification rigor with development velocity:

- **Incremental compliance**: Addressing gaps progressively rather than big-bang transformation
- **Continuous evidence collection**: Automated documentation reducing manual overhead
- **Risk-based prioritization**: Focusing efforts on highest-impact safety improvements
- **Regular auditor engagement**: Early involvement of certification body preventing late surprises
- **Cross-functional safety teams**: Embedding safety expertise within development squads

Strategic Value for Autonomous Systems

This project demonstrates critical capabilities relevant to Koenig & Bauer's innovation strategy:

Certification Expertise

Navigating complex regulatory frameworks requires deep understanding of standards, auditor expectations, and efficient evidence generation.

Safety-First Culture

Successful autonomous systems depend on organizations where safety is intrinsic to development culture, not compliance checkbox.

Time-to-Market Optimization

Strategic certification planning accelerates rather than delays market entry through proactive gap closure and auditor engagement.

Technology Credibility

Safety certification differentiates serious autonomous technology providers from those with unproven solutions in risk-averse industries.

Industry Applications

The safety certification methodology applies to Koenig & Bauer's operations:

- **Autonomous material handling**: AGVs and AMRs requiring safety certification for factory deployment
- **Critical infrastructure robotics**: Robots operating in power, water, and transportation facilities
- **Medical device autonomy**: Autonomous functions in healthcare requiring rigorous safety validation
- **Aviation and rail systems**: Safety-critical autonomous functions in regulated transportation sectors
- **Process automation**: Industrial control systems requiring functional safety compliance

Customer Perspective

> "From the beginning, Motius has been proactively anticipating challenges before they arise. Their structured yet agile approach helped us push forward toward TÜV readiness with clarity and confidence."
>
> **Tillmann Ochs, Director of Systems, Safety and Cybersecurity**

Industry Context

Germany is rapidly advancing autonomous logistics. In May 2025, the ATLAS-L4 consortium – including the customer – successfully tested a fully automated electric truck for hub-to-hub transport on motorways, demonstrating real-world application of Germany's regulatory framework for autonomous driving to freight operations.

Future Development Pathways

The safety certification framework established a foundation for continued innovation:

Extended Certification Scope

- Additional operational design domains (ODDs) for diverse deployment scenarios
- Higher Safety Integrity Levels (SIL-3) for more critical applications
- International certification (EU, US DOT) for global market access

AI Safety Assurance

- Safety validation frameworks for machine learning perception systems
- Explainability and monitoring for AI-based decision-making
- Update and patching processes maintaining certification through ML model evolution

Fleet-Level Safety

- Multi-vehicle coordination safety analysis
- V2X communication security and reliability
- Fleet management system safety certification

Project developed in partnership with a leading autonomous trucking pioneer, demonstrating Motius's expertise in functional safety engineering, cybersecurity assessment, and navigating complex certification processes for autonomous systems deployed in critical infrastructure.