

STEINMETZ SECURITY SERVICES

Management systems under scrutiny!

Bridging the Gap

How Automotive Functional Safety and Cybersecurity Can Strengthen Each Other

Aligning ISO 26262 and ISO/SAE 21434 for shared risk analysis,

Integrated development, and unified verification — a practitioner's whitepaper.

Author Markus Steinmetz · Steinmetz Security Services

Date November 2025

Version 1.0

Executive Summary

The automotive industry faces an unprecedented challenge: vehicles are becoming increasingly complex, connected, and software-driven. This evolution demands excellence in both functional safety (ISO 26262) and cybersecurity (ISO/SAE 21434). While these domains have traditionally been treated separately, they share fundamental principles and methodologies that, when properly aligned, can create significant synergies.

This whitepaper explores how automotive functional safety and cybersecurity can mutually benefit from each other, particularly in three key areas:

1. **Risk Analysis Methodologies** — shared approaches to systematic risk identification and assessment.
2. **Structured Development Processes** — V-Model based lifecycle management and systematic engineering.
3. **Verification and Validation** — comprehensive methods to ensure correctness and completeness.

Organizations that successfully integrate these disciplines can achieve:

- Reduced development costs through shared processes and artifacts
- Enhanced product quality through complementary verification approaches
- Accelerated time-to-market by avoiding duplicate activities
- Improved regulatory compliance across both domains

Table of Contents

1. Introduction	5
1.1 The Convergence of Safety and Security	5
1.2 Why Integration Matters	5
2. Understanding the Standards	5
2.1 ISO 26262 — Functional Safety	5
2.2 ISO/SAE 21434 — Cybersecurity Engineering	6
2.3 Fundamental Similarities	6
3. Synergy Area 1 — Risk Analysis	6
3.1 Parallel Approaches to Risk	6
3.2 Integrated Risk Analysis Framework	6
3.3 Practical Benefits	7
3.4 Risk Analysis Synergies — Summary	8
4. Synergy Area 2 — Structured Development Process	8
4.1 V-Model Alignment	8
4.2 Process Integration Opportunities	8
4.3 Configuration and Change Management	10
4.4 Process Integration Benefits — Summary	10
5. Synergy Area 3 — Verification and Validation	10
5.1 Complementary V&V Approaches	10
5.2 Integrated Verification Strategy	11
5.3 Verification Independence	13
5.4 V&V Integration Benefits — Summary	13
6. Practical Integration Framework	14
6.1 Organizational Integration	14
6.2 Tool Integration	15
6.3 Process Integration Roadmap	15
6.4 Governance and Compliance	15
7. Challenges and Solutions	16
7.1 Common Challenges	16
7.2 Risk Mitigation Strategies	17
8. Case Studies	17
8.1 Case Study 1 — Automated Driving ECU	17
8.2 Case Study 2 — Over-the-Air Update System	18
8.3 Case Study 3 — V2X Communication Module	18
9. Recommendations	19
9.1 For Management	19
9.2 For Safety Engineers	19

9.3 For Security Engineers.....	19
9.4 For System Architects	20
9.5 For Tool and Process Owners	20
10. Conclusion	20
10.1 Key Takeaways.....	20
10.2 The Path Forward	21
10.3 Call to Action	21

1. Introduction

1.1 The Convergence of Safety and Security

Modern vehicles contain over 100 million lines of code and are increasingly connected to external networks. This connectivity creates new attack vectors that can directly impact safety-critical functions. A cyberattack on a vehicle's braking system, for instance, represents both a security threat and a safety hazard.

The automotive industry has recognized this convergence:

- **ISO 26262** (Functional Safety) — the standard series ensures safe system behavior even under fault conditions.
- **ISO/SAE 21434** (Cybersecurity) — the standard protects systems from malicious interference.

1.2 Why Integration Matters

Treating safety and security as isolated domains leads to:

- Duplicated efforts in risk analysis and assessment
- Inconsistent requirements and design decisions
- Conflicting verification activities
- Increased development costs and time
- Potential gaps in coverage

An integrated approach instead delivers:

- Unified risk understanding across both domains
- Consistent engineering processes and documentation
- Shared verification and validation activities
- Improved resource utilization
- A holistic view of vehicle integrity

2. Understanding the Standards

2.1 ISO 26262 — Functional Safety

Objective: Ensure electrical/electronic systems function safely, even in the presence of faults.

Key Principles

- Systematic fault avoidance through process rigor
- Fault detection and handling mechanisms
- ASIL (Automotive Safety Integrity Level) classification
- V-Model development lifecycle
- Comprehensive verification and validation

Scope: Hardware and software safety throughout the vehicle lifecycle.

2.2 ISO/SAE 21434 — Cybersecurity Engineering

Objective: Protect vehicle systems from malicious attacks throughout their lifecycle.

Key Principles

- Cybersecurity-by-design approach
- Threat Analysis and Risk Assessment (TARA)
- CAL (Cybersecurity Assurance Level) classification
- Continuous cybersecurity activities
- Vulnerability management

Scope: Cybersecurity risk management from concept through decommissioning.

2.3 Fundamental Similarities

Table 1: Comparison of key aspects of the two standards

Aspect	ISO 26262	ISO/SAE 21434
Lifecycle Approach	V-Model based	V-Model compatible
Risk-Based	HARA (Hazard Analysis)	TARA (Threat Analysis)
Classification	System ASIL (A–D)	CAL (1–4) *
Requirements Management	Systematic tracing	Systematic tracing
Verification Focus	Correctness & completeness	Correctness & completeness
Documentation	Comprehensive evidence	Comprehensive evidence

* Not mandatory (informative); see ISO/SAE CD PAS 8475 for further information.

3. Synergy Area 1 — Risk Analysis

3.1 Parallel Approaches to Risk

Both standards employ structured risk analysis methodologies.

ISO 26262 — HARA (Hazard Analysis and Risk Assessment)

- Identifies hazardous events from system malfunctions
- Assesses Severity, Exposure, Controllability
- Results in ASIL classification (QM, A, B, C, D)

ISO/SAE 21434 — TARA (Threat Analysis and Risk Assessment)

- Identifies attack paths and threat scenarios
- Assesses Impact and Feasibility (attack potential)
- Results in CAL classification (CAL 1–4)

3.2 Integrated Risk Analysis Framework

Step 1 — Combined Item Definition

- Define system scope considering both safety and security aspects

- Identify interfaces, dependencies, and assumptions
- **Benefit:** a single source of truth for system understanding

Step 2 — Unified Asset Identification

- **Safety:** critical functions and failure modes
- **Security:** assets, attack surfaces, threat actors
- **Benefit:** a comprehensive view of what needs protection

Step 3 — Parallel Risk Assessment

HARA and TARA run side by side on the same system model and converge into a single, integrated risk picture:

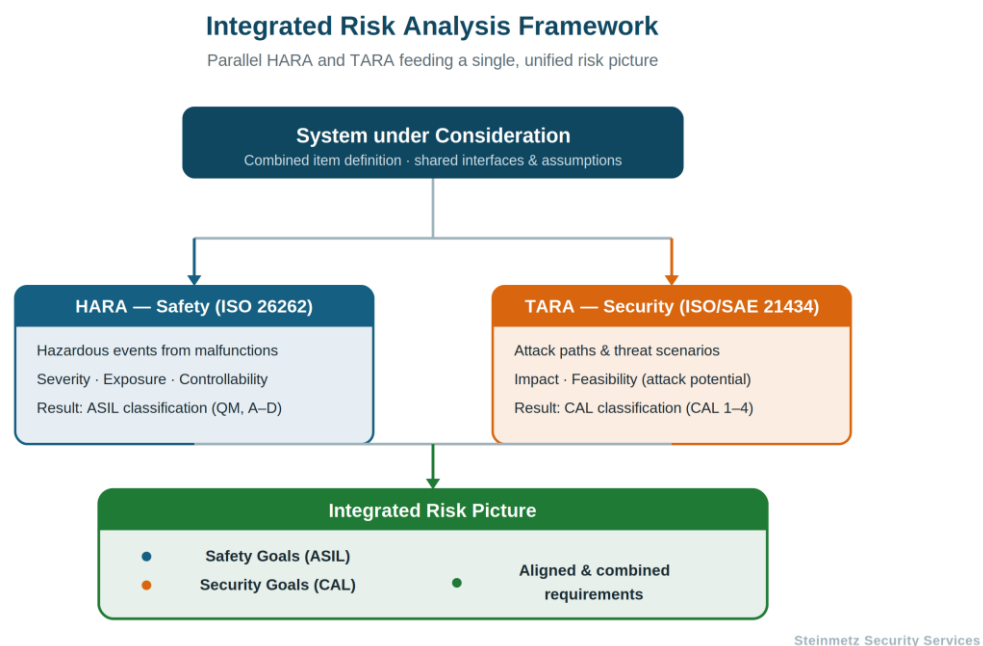


Figure 1: Parallel HARA and TARA converging into one integrated risk picture

Step 4 — Cross-Domain Impact Analysis

- Identify where security threats can cause safety hazards
- Determine where safety mechanisms can mitigate security risks
- **Benefit:** discover hidden dependencies and optimize countermeasures

3.3 Practical Benefits

Example — Electronic Brake System

Table 2: Example content for a jointly conducted analysis

Analysis Type	Finding	Classification	Countermeasure
HARA	Unintended braking	ASIL D	Redundant sensors, plausibility checks
TARA	CAN message injection attack	CAL 3	Message authentication (MAC)
Integration	Attacks can cause safety hazard	ASIL D + CAL 3	Combined: authenticated messages + plausibility checks + fallback strategy

Resource Savings

- Single item-definition workshop instead of two separate sessions
- Shared documentation of system architecture and interfaces
- Combined review meetings
- **Estimated time saving: 20–30%**

3.4 Risk Analysis Synergies — Summary

- **Shared understanding:** both teams work from the same system model
- **Efficiency:** avoid duplicate analysis of the same system
- **Completeness:** security threats that impact safety are not overlooked
- **Traceability:** clear links between safety goals and security objectives
- **Optimization:** countermeasures can address both domains simultaneously

4. Synergy Area 2 — Structured Development Process

4.1 V-Model Alignment

Both ISO 26262 and ISO/SAE 21434 build on V-Model principles. Their phases map onto one another almost one-to-one, which is what makes parallel execution practical:

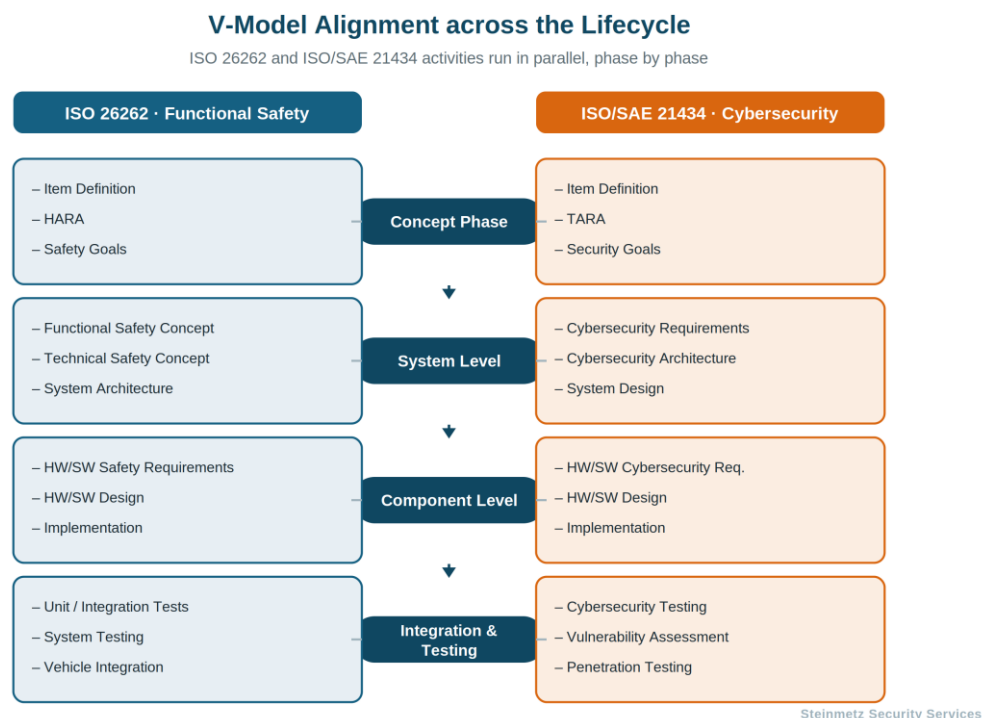


Figure 2: Phase-by-phase alignment of the ISO 26262 and ISO/SAE 21434 lifecycles

4.2 Process Integration Opportunities

4.2.1 Concept Phase Consolidation

Traditional Approach

- Separate safety concept workshops
- Separate security concept workshops

- Different teams, different schedules
- Risk of inconsistencies

Integrated Approach

- **Combined item definition** covering both aspects
- **Parallel HARA and TARA** in joint sessions
- **Integrated safety and security concept** document
- **Shared architectural assumptions**

Benefits

- Faster concept development
- Better alignment between teams
- Early identification of conflicts
- Single source of system understanding

4.2.2 Requirements Engineering Synergies

Table 3: Jointly developed, generalized requirements

Category	Safety (ISO 26262)	Security (ISO/SAE 21434)	Integration Opportunity
Functional	Safe behavior under faults	Secure behavior under attacks	Combined functional specification
Performance	Timing constraints for safety	Timing for security mechanisms	Unified performance requirements
Diagnostics	Fault detection	Intrusion detection	Integrated monitoring architecture
Redundancy	Fault tolerance	Attack resilience (defense-in-depth)	Optimized redundancy strategy

Example — Integrated Requirement

SYS-REQ-001 — Authenticated Emergency Braking Command

Safety Aspect (ASIL D)

- Emergency braking shall activate within 100 ms of a valid trigger
- System shall detect and handle invalid sensor data
- Fallback braking strategy shall be available

Security Aspect (CAL 3)

- Emergency braking commands shall be authenticated using HMAC-SHA256
- Invalid authentication shall be logged as a security event
- System shall resist replay attacks through message counters

Combined Implementation

- Single message-processing pipeline with integrated checks
- Shared timing budget for authentication and safety monitoring
- Common logging and diagnostic framework

4.2.3 Architecture and Design Integration

Unified System Architecture

- Security zones and safety partitions aligned
- Communication channels serve both purposes
- Shared hardware security modules (HSM) for crypto and safety
- Freedom from interference considers both random faults and attacks

Design Patterns Supporting Both

- **Separation of concerns:** reduces attack surface and fault propagation
- **Defensive programming:** handles both unexpected inputs and malicious data
- **Fail-safe defaults:** the secure state is also the safe state
- **Monitoring and logging:** detects both faults and attacks

4.3 Configuration and Change Management

Both standards require rigorous configuration management.

Shared CCM Activities

- Version control of specifications and code
- Change impact analysis
- Traceability matrices
- Baseline management

Integration Benefits

- Single CCM tool and process
- Unified change review board
- Combined impact assessment (safety + security)
- Consistent versioning across domains

4.4 Process Integration Benefits — Summary

- **Reduced cycle time:** parallel rather than sequential activities
- **Consistency:** requirements don't conflict between domains
- **Efficiency:** shared documentation and review meetings
- **Quality:** cross-domain expertise in design decisions
- **Cost savings:** estimated 25–40% reduction in process overhead

5. Synergy Area 3 — Verification and Validation

5.1 Complementary V&V Approaches

Both standards emphasize comprehensive verification and validation.

ISO 26262 — V&V Focus

- Correctness of implementation against requirements
- Completeness of safety mechanisms
- Fault injection testing
- Safety analysis methods (FTA, FMEA)

- Independence of verification activities

ISO/SAE 21434 — V&V Focus

- Security requirements coverage
- Vulnerability analysis
- Penetration testing
- Fuzzing and attack simulation
- Security testing independence

5.2 Integrated Verification Strategy

5.2.1 Requirements Verification

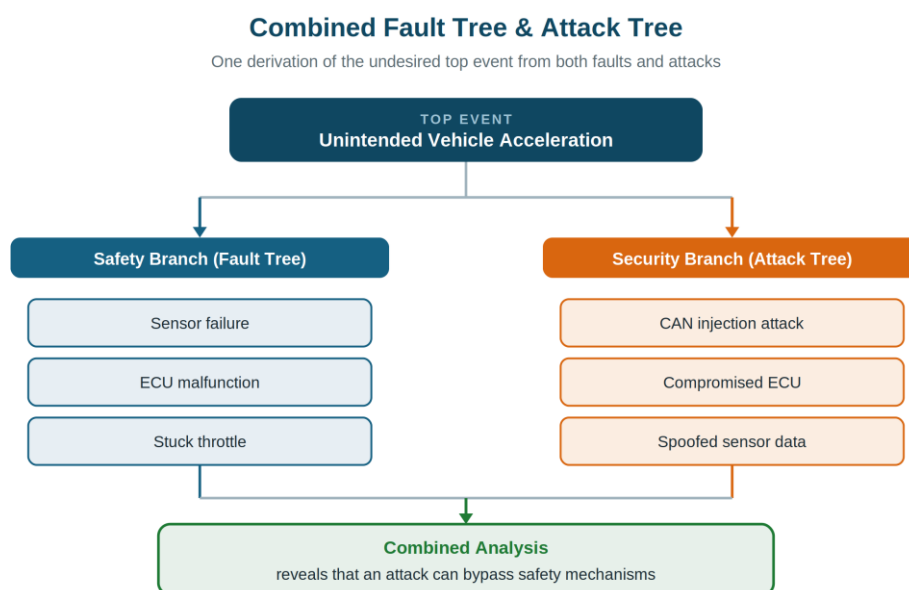
Table 4: Review objectives

Verification Criteria	Safety Check	Security Check	Integration Benefit
Correctness	Implements safety requirement	Implements security requirement	Single review with dual perspective
Completeness	All hazards addressed	All threats addressed	No gaps between domains
Consistency	No internal conflicts	No security conflicts	Cross-domain consistency verified
Traceability	Links to safety goals	Links to security goals	Unified traceability matrix
Verifiability	Testable safety criteria	Testable security criteria	Shared test strategy

5.2.2 Design Verification Methods

1. Fault Tree Analysis (FTA) ↔ Attack Trees

- **Safety:** analyzes how component failures lead to safety goal violations (hazards)
- **Security:** analyzes how attack steps lead to compromise or threat realization
- **Integration:** combined trees show a complete derivation of the undesired state or event



Steinmetz Security Services

Figure 3: A combined fault/attack tree derives the same top event from both faults and attacks

2. FMEA ↔ STRIDE Threat Modeling

- **FMEA:** systematic analysis of failure modes
- **STRIDE:** systematic analysis of threat categories
- **Integration:** a single table captures both failure and attack scenarios

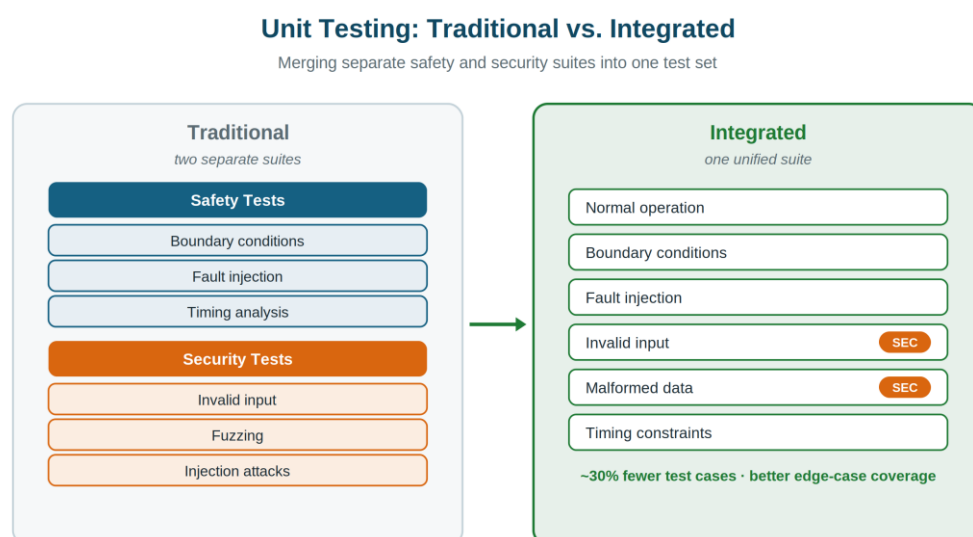
3. Code Review Consolidation

- **Safety-critical review focuses on:** correctness, complexity, timing
- **Security review focuses on:** input validation, injection flaws, crypto usage
- **Integration:** a single review with a combined checklist

5.2.3 Testing Synergies

Unit Testing

Merging the traditionally separate safety and security suites removes duplicate cases while widening edge-case coverage:



Steinmetz Security Services

Figure 4: Consolidating separate safety and security unit tests into one integrated suite

Integration Testing

- **Combined test scenarios:** a fault occurs during an attack, or vice versa
- **Shared test infrastructure:** test benches, simulators, monitoring
- **Cross-domain test cases:** a security mechanism must not impair a safety function

System Testing

Table 5: System test objectives

Test Type	Safety Focus	Security Focus	Integration
Functional	Correct behavior	Secure behavior	Combined test scenarios
Robustness	Fault tolerance	Attack resilience	Fault + attack combinations
Performance	Timing guarantees	Crypto overhead	Verify both are met
Stress Testing	Overload conditions	DoS scenarios	Shared stress tests

5.2.4 Specialized Testing Approaches

Fault Injection + Penetration Testing

- **Safety:** inject hardware/software faults to verify detection
- **Security:** inject malicious inputs to verify defenses
- **Combined:** inject faults and attacks simultaneously to verify system resilience

Example Test Case — INT-TEST-042

Scenario: CAN bus attack during a sensor fault

Setup

1. Induce a sensor fault (safety scenario)
2. Simultaneously inject spoofed CAN messages (security attack)

Expected Behavior

- Safety mechanism detects the sensor fault → enters safe state
- Security mechanism detects invalid messages → logs intrusion
- System maintains the safe state despite the attack
- Driver receives an appropriate warning

Verification

- ASIL D requirement: safe state maintained
- CAL 3 requirement: attack detected and logged

5.3 Verification Independence

Both standards require independence in verification.

Levels of Independence

- **Level 1:** different person from the same team
- **Level 2:** different team in the same organization
- **Level 3:** external / independent organization

Integration Benefit

- **A shared independent assessor** can review both safety and security
- Combined assessments reduce costs
- The assessor develops a holistic view of product quality
- A single audit / assessment cycle instead of two

5.4 V&V Integration Benefits — Summary

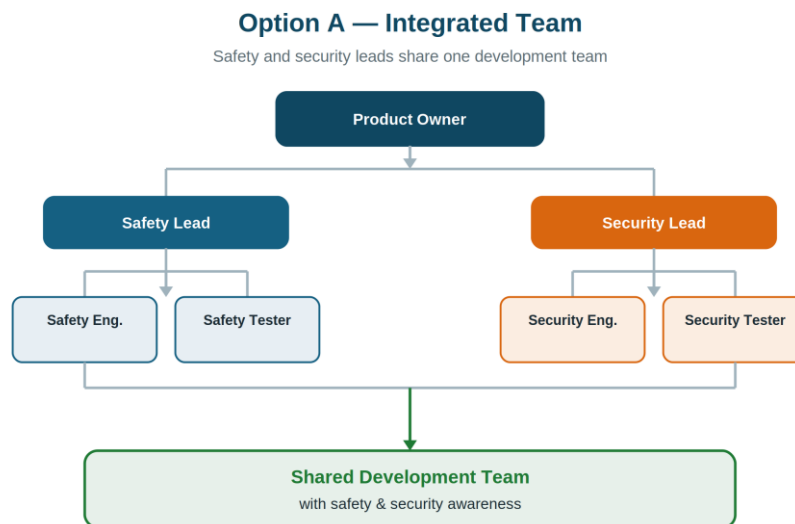
- **Test efficiency:** eliminate duplicate test cases (30–40% reduction)
- **Better coverage:** cross-domain scenarios catch more issues
- **Shared infrastructure:** test environments, tools, automation
- **Unified evidence:** a single verification report for both domains
- **Risk reduction:** discover interactions between faults and attacks early

6. Practical Integration Framework

6.1 Organizational Integration

Two team structures work well in practice. Option A embeds both disciplines in one team; Option B keeps teams separate but tightly synchronised.

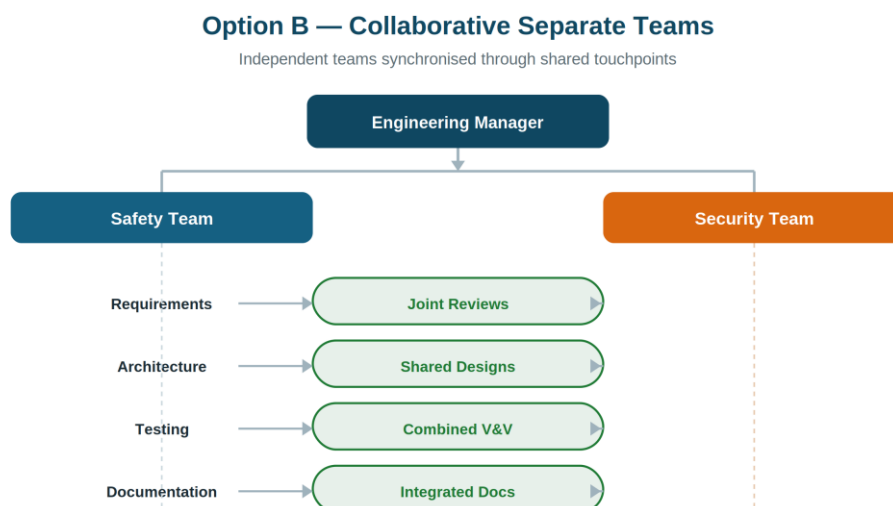
Option A — Integrated Team



Steinmetz Security Services

Figure 5: An integrated team with safety and security leads over a shared development team

Option B — Collaborative Separate Teams



Steinmetz Security Services

Figure 6: Separate teams synchronised through shared requirements, designs, V&V, and documentation

Key Success Factors

- Regular joint meetings and design reviews
- Shared responsibility for integrated requirements

- Cross-training between teams
- Common tooling and processes

6.2 Tool Integration

Table 6: Recommended tools for an integrated approach

Tool Type	Purpose	Integration Benefit
Requirements Management	DOORS NG, Polarion, Jama	Single requirements database with safety & security attributes
Modeling	Enterprise Architect, Rhapsody	Unified system models with dual perspectives
Risk Analysis	Medini Analyze, SAHARA	Combined HARA/TARA workflows
Static Analysis	Polyspace, Coverity, CodeSonar	Detects both safety and security issues
Test Management	TestRail, PractiTest	Unified test planning and execution
Configuration Management	Git, SVN with ALM integration	Single source of truth for all artifacts

6.3 Process Integration Roadmap

Phase 1 — Foundation (Months 1–3)

- Establish a joint safety-security working group
- Map ISO 26262 and ISO/SAE 21434 processes
- Identify integration opportunities
- Define integrated templates and checklists

Phase 2 — Pilot Project (Months 4–9)

- Select a suitable pilot project
- Implement the integrated approach for the concept phase
- Conduct a combined HARA/TARA
- Create an integrated requirements specification
- Measure effort and quality metrics

Phase 3 — Scaling (Months 10–15)

- Extend to system design and implementation
- Implement the integrated verification approach
- Establish shared testing infrastructure
- Train the broader organization

Phase 4 — Optimization (Months 16+)

- Refine processes based on lessons learned
- Automate integrated checks
- Establish a continuous improvement cycle
- Share best practices across projects

6.4 Governance and Compliance

Integrated Management Plan

- Single project plan covering both standards
- Unified milestone structure
- Combined progress reporting
- Shared risk and issue management

Compliance Evidence

- Integrated safety case and cybersecurity case
- Cross-referenced work products
- Unified traceability
- Combined assessment reports

7. Challenges and Solutions

7.1 Common Challenges

Challenge 1 — Different Team Cultures

Problem

- Safety engineers: conservative, risk-averse, process-focused
- Security engineers: adversarial thinking, assume breach, agile
- Communication gaps and misunderstandings

Solution

- **Cross-training programs:** safety teams learn security thinking, and vice versa
- **Joint workshops:** build shared mental models
- **Common language:** define unified terminology
- **Rotation programs:** temporary assignments to the other team

Challenge 2 — Conflicting Requirements

Problem

- Security may add latency that violates safety timing requirements
- Safety diagnostics may expose information useful to attackers
- Redundancy approaches may conflict

Solution

- **Early architecture decisions:** address conflicts at system level
- **Trade-off analysis:** document and justify decisions
- **Integrated design patterns:** solutions that satisfy both domains
- **Performance budgeting:** allocate resources for both needs

Challenge 3 — Tool and Process Maturity

Problem

- Safety tooling is mature; security tooling for embedded systems is evolving
- ISO 26262 processes are well-established; ISO/SAE 21434 is newer
- Legacy projects were not designed for integration

Solution

- **Phased tool integration:** start with requirements and testing
- **Process harmonization:** align templates and workflows gradually
- **Retrofit strategy:** for legacy projects, add security incrementally
- **Pilot projects:** learn on new developments before scaling

Challenge 4 — Resource Constraints

Problem

- Budget limitations for dual compliance
- Limited availability of experts in both domains
- Pressure to meet time-to-market targets

Solution

- **Business case development:** quantify integration benefits
- **Focused integration:** start with high-value synergies
- **External expertise:** specialist support for the initial setup
- **Long-term view:** integration pays off over multiple projects

7.2 Risk Mitigation Strategies

Table 7: Risk mitigation strategies

Risk	Impact	Mitigation
Requirements conflicts	Medium–High	Early joint reviews, clear decision authority
Skill gaps in teams	Medium	Training, hiring, external support
Tool incompatibility	Medium	Common data formats, API integration
Schedule pressure	High	Realistic planning, management support
Regulatory uncertainty	Medium–High	Engage with authorities early, document approach

8. Case Studies

8.1 Case Study 1 — Automated Driving ECU

Context

- Level 3 automated driving controller
- ASIL D safety requirements
- High cybersecurity exposure (V2X, cloud connectivity)

Integration Approach

- Combined item-definition workshop (2 days vs. separate 3 + 3 days)
- Parallel HARA/TARA identified 15 scenarios requiring both safety and security measures
- Integrated architecture with security zones aligned to safety partitions
- Combined testing: 40% reduction in test cases through shared scenarios

Results

- **Development time:** 6 months faster to SOP
- **Cost savings:** 35% reduction in concept and verification costs
- **Quality:** zero post-launch safety or security issues in the first year
- **Compliance:** successful ISO 26262 and ISO/SAE 21434 assessments

Key Success Factors

- Executive sponsorship for the integrated approach
- A dedicated safety-security architect role
- Investment in integrated tooling upfront
- Continuous team collaboration

8.2 Case Study 2 — Over-the-Air Update System

Context

- OTA update capability for vehicle software
- Safety-critical components (ASIL B–D)
- A high-value security target for attackers

Integration Approach

- Unified requirement: updates must be authenticated (security) AND verified for correct installation (safety)
- Shared test infrastructure for update scenarios
- Combined failure-mode and threat analysis
- Integrated rollback mechanisms (safety + security triggers)

Results

- **Requirement efficiency:** 50% fewer requirements through combination
- **Testing:** a single test suite covering safety and security aspects
- **Performance:** optimized crypto and safety checks in a single pass
- **Customer confidence:** a robust update mechanism with dual assurance

Lessons Learned

- Early architectural decisions are critical
- Performance optimization is required for resource-constrained ECUs
- A clear ownership model is necessary for integrated requirements

8.3 Case Study 3 — V2X Communication Module

Context

- Vehicle-to-Everything communication
- Safety-relevant messages (collision warnings)
- Exposed to network attacks

Integration Approach

- TARA identified attacks that could cause safety-relevant message corruption
- HARA considered security failures as potential fault sources
- Combined message authentication and plausibility checking
- Unified monitoring detects both network attacks and message failures

Results

- **Architecture:** a single message-validation pipeline
- **Latency:** met safety timing despite added security checks
- **Robustness:** the system handles attack + fault combinations
- **Compliance:** satisfied both ISO 26262 ASIL C and ISO/SAE 21434 CAL 3

Takeaway

- A single validated pipeline can satisfy stringent safety and security targets at once

9. Recommendations

9.1 For Management

Strategic Decisions

1. **Commitment to integration:** make it an organizational priority, not optional
2. **Invest upfront:** tooling, training, and process development pay off
3. **Measure benefits:** track time, cost, and quality improvements
4. **Support collaboration:** create structures that enable teamwork
5. **Think long-term:** benefits compound across multiple projects

Resource Allocation

- Budget for integrated tooling and training
- Allow time for process development and pilots
- Hire or develop cross-domain expertise
- Support communities of practice

9.2 For Safety Engineers

Mindset Shifts

6. **Embrace adversarial thinking:** consider malicious actors, not just random faults
7. **Understand attack surfaces:** learn basic security concepts
8. **Collaborate actively:** engage with the security team early and often
9. **Adapt processes:** be open to modifications that serve both domains
10. **Keep learning:** the security landscape evolves rapidly

Practical Actions

- Participate in combined HARA/TARA sessions
- Review security requirements for safety implications
- Include attack scenarios in test planning
- Attend security training and conferences

9.3 For Security Engineers

Mindset Shifts

11. **Respect safety rigor:** understand why process discipline matters
12. **Consider availability:** security must not prevent safe operation
13. **Work within constraints:** automotive systems have resource limitations

14. **Value verification:** embrace systematic V&V approaches

15. **Think about lifecycle:** security is not just about development

Practical Actions

- Learn safety concepts and terminology
- Consider the safety impact of security measures
- Participate in FMEA and FTA activities
- Review safety requirements for security gaps
- Respect automotive timing and resource constraints

9.4 For System Architects

Design Principles

16. **Secure by design AND safe by design:** both from the start

17. **Defense in depth:** multiple layers serve both domains

18. **Fail secure AND fail safe:** aligned safe states

19. **Monitor everything:** logging serves safety diagnostics and security detection

20. **Simplicity:** reduces both attack surface and failure modes

Architecture Patterns

- Security zones aligned with safety partitions
- Hardware separation (HSM, secure enclaves) with safety isolation
- Secure communication channels with safety-relevant data integrity
- Unified monitoring and diagnostic infrastructure
- Graceful degradation strategies

9.5 For Tool and Process Owners

Integration Priorities

21. **Requirements tools:** single source with dual attributes (ASIL + CAL)

22. **Traceability:** end-to-end links across both standards

23. **Test management:** unified planning and execution

24. **Document templates:** combined work-product formats

25. **Dashboards:** integrated status reporting

Success Metrics

- Requirements coverage (safety + security)
- Verification status (combined)
- Issue aging (no discrimination between safety and security defects)
- Process efficiency (time spent on integration activities)
- Quality metrics (defects found, customer incidents)

10. Conclusion

10.1 Key Takeaways

The integration of automotive functional safety (ISO 26262) and cybersecurity (ISO/SAE 21434) is not just beneficial — it is essential for modern vehicle development.

Risk Analysis Synergies

- 20–30% time savings through combined HARA/TARA
- Better identification of safety-security interactions
- Optimized countermeasures addressing both domains
- A unified risk picture driving prioritization

Process Integration Benefits

- 25–40% reduction in process overhead
- Accelerated development through parallel activities
- Consistent requirements and design decisions
- Better cross-domain communication

Verification Excellence

- 30–40% fewer test cases through intelligent combination
- Improved coverage of edge cases and interactions
- Shared infrastructure and tooling
- More robust products that handle real-world complexity

Bottom line: Organizations that successfully integrate safety and security achieve faster time-to-market, lower development costs, and higher-quality products that truly meet the challenges of connected, automated vehicles.

10.2 The Path Forward

Start Small, Think Big

1. Begin with pilot projects to learn
2. Focus on high-value integration points first
3. Build expertise and confidence gradually
4. Scale successful approaches systematically

Continuous Evolution

- Both standards will continue to evolve
- Technological advances will create new challenges
- The regulatory landscape will develop further
- Integration approaches must adapt

Cultural Change

- Integration requires organizational commitment
- Success depends on collaboration, not just process
- Cross-domain expertise is a competitive advantage
- Safety and security together define product integrity

10.3 Call to Action

The convergence of safety and security is inevitable. The question is not whether to integrate these disciplines, but how quickly and effectively your organization can do so.

Next Steps

1. **Assess your current state:** where are you today in integration maturity?
2. **Define your vision:** what does success look like for your organization?
3. **Build the business case:** quantify the benefits for your context
4. **Start the journey:** launch a pilot project and learn by doing
5. **Share and scale:** expand successful practices across the organization

The automotive industry is at an inflection point. Vehicles are becoming software-defined, connected, and increasingly autonomous. Success in this new era requires excellence in both functional safety and cybersecurity — and the wisdom to integrate them effectively.

About the Author

Markus Steinmetz operates Steinmetz Security Services (SSS), providing freelance security services — support and guidance, training, and advisory services — in functional safety, product cybersecurity, information security, and OT security for the automotive, industrial, agriculture, and railway sectors.

His expertise spans ISO 26262, IEC 61508 and ISO 13849 (functional safety); ISO/SAE 21434 and UNECE R155/R156 (product cybersecurity); ISO 27001 and TISAX (information security); and IEC 62443 (OT security), alongside emerging regulation such as the Cyber Resilience Act (CRA) and NIS-2. He helps organizations bridge the gap between safety and security through practical, integrated approaches.

Contact

Email: markus@steinmetz-security.de

Website: steinmetz-security.de

LinkedIn: linkedin.com/in/markus-steinmetz-78052817

References

1. ISO 26262:2018 — Road vehicles — Functional safety
2. ISO/SAE 21434:2021 — Road vehicles — Cybersecurity engineering
3. SAE J3061 — Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
4. NHTSA — Cybersecurity Best Practices for Modern Vehicles
5. UNECE WP.29 Regulations on Cybersecurity (R155) and Software Updates (R156)