

# Multi-Dimensional Synergy: FuSa, Cybersecurity, SOTIF and QM as One System

The key to safe SDV and AD systems

Tianhong Wu
Principal Engineer, System Safety | Mobility Services, Greater China | TÜV SÜD
Shanghai

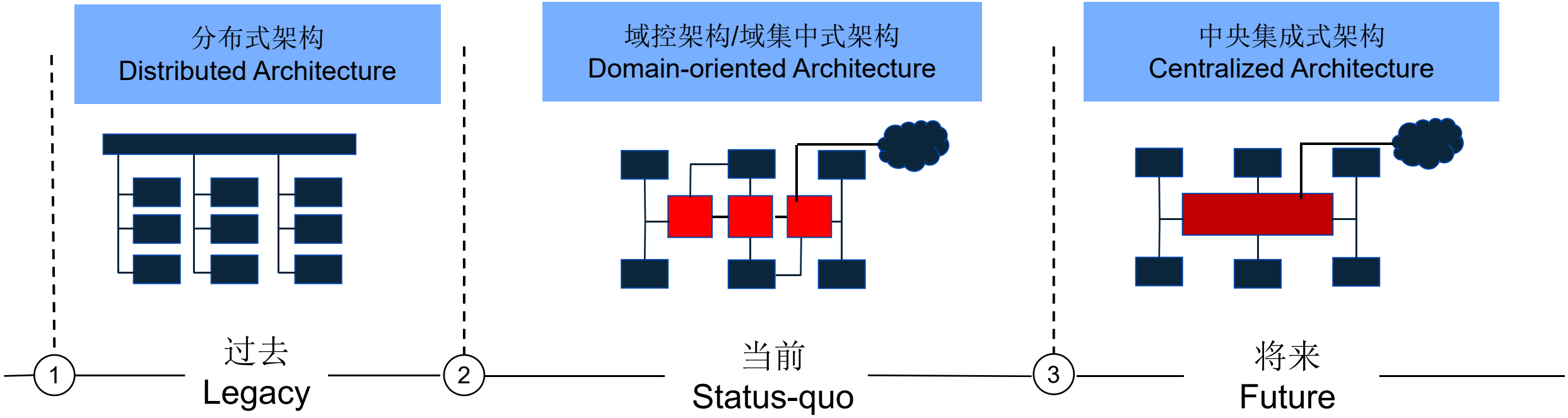
Add value.
Inspire trust.



# Multi-Dimensional Synergy: FuSa, Cybersecurity, SOTIF and QM as One System

| | |
|---|---|
| 01 | 多标准融合的必要性与价值<br>The necessity and value of multi-standard fusion |
| 02 | 多标准融合的实施挑战<br>Obstacles Implementing Multi-standard Fusion |
| 03 | 多标准融合的技术路径与方法论<br>Approaches & Methodologies for Multi-standard Fusion |
| 04 | 体系建设未来展望<br>Future prospect for multi-standard fusion |

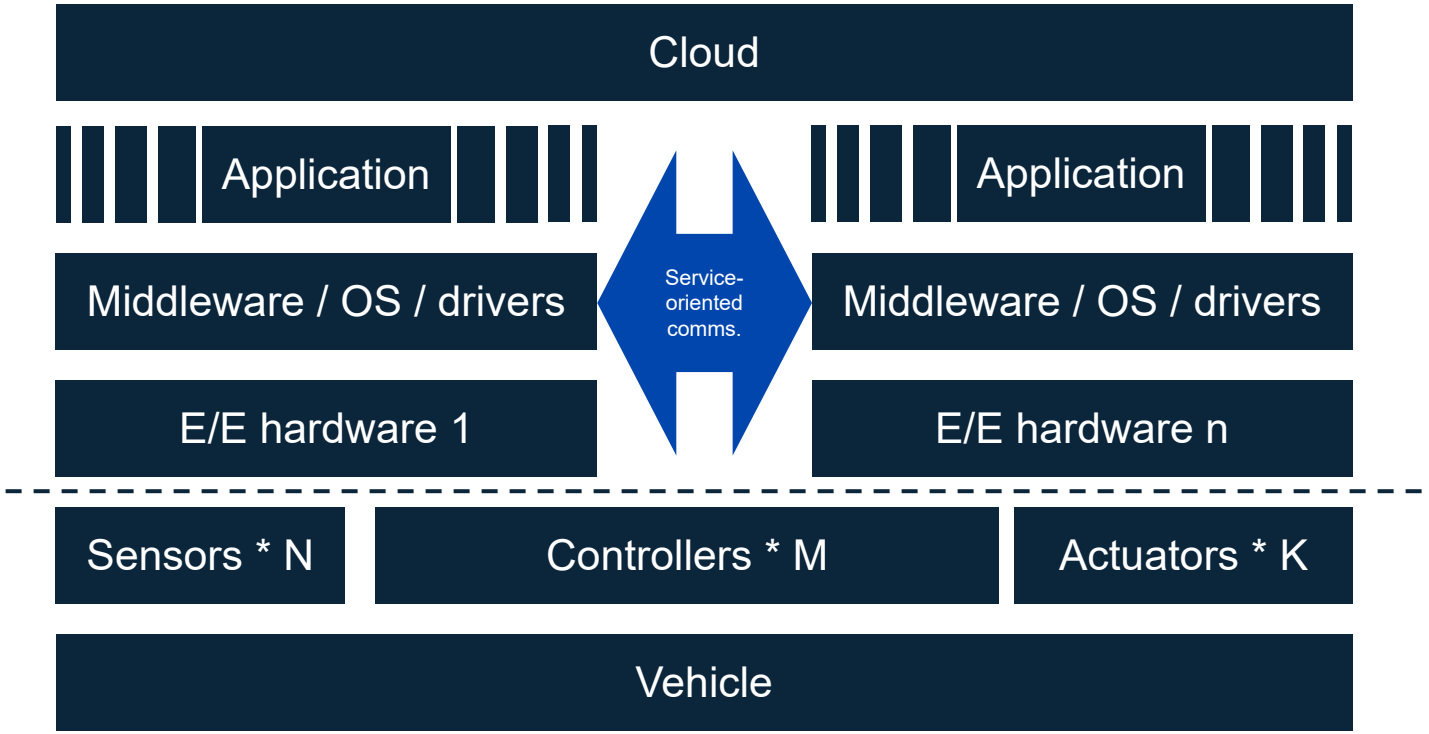
# The evolution of vehicular E/E architecture posts increasing threat




控制器的聚合逻辑正在从垂直（基于功能）转向水平（基于资源）

The clustering logic is transitioning from **vertical**(function based) to **horizontal**(resource based)

# E/E evolution makes safety cross-domain




| No. | Risk | Domain |
|---|---|---|
| 1 | **Critical systems exposed to attack** | **Cybersecurity** |
| 2 | Non-deterministic scheduling threatens non-fault anomalies | SOTIF / Cyber |
| 3 | Complexity raises systematic faults and vulnerabilities | FuSa / Cyber |
| 4 | Shared resources mean shared risk | FuSa / Cyber / SOTIF |

Automotive cyber-attacks: +25% YoY in 2024

# Standard-by-standard: the duplication tax




VS

Single-standard items

| | Items | Documents | Overlap |
|---|---|---|---|
| ASPICE | 171 | Core: 200+ | - |
| Functional safety | 105 | 140+ | ~80% |
| Cybersecurity | 41 | 50+ | ~50% |
| SOTIF | 13 | 40+ | ~20% |
| Total | 330 | 400+ | |

**QM framework**

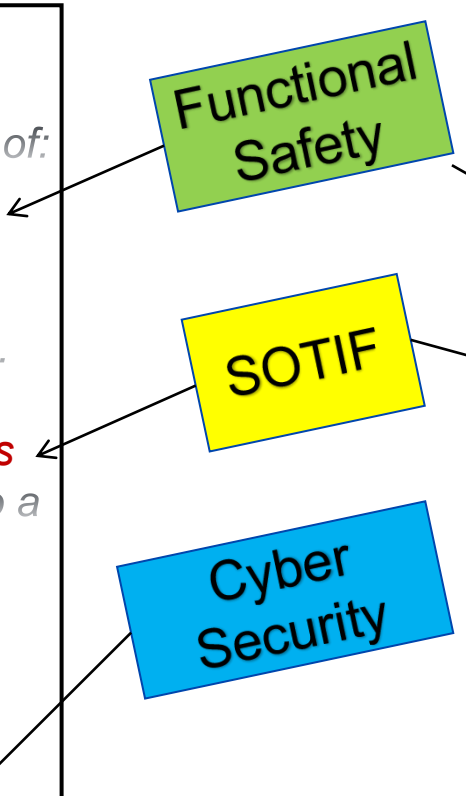
**+ risk measures**

Software complexity: 4x in 10 years (12% CAGR)

# Regulators already think in fused terms

UN Regulation No 171(DCAS) [2024/2689]

*Inspection of the safety approach at the concept (vehicle) level with confirmation that it includes consideration of:*
*(i) Interactions with other vehicle systems;*
*(ii) Malfunctions of the system, within the scope of this UN Regulation;*
*(iii) For functions defined in paragraph 3.2. of this UN Regulation:*
*- Situations when a system free from faults may create safety critical risks (e.g. due to a lack of or wrong comprehension of the vehicle environment);*
*- Operational and system limitations;*
*- Reasonably foreseeable misuse by the driver;*
*- Intentional modification of the system.*
*(iv) Cyber-attacks having an impact on the safety of the vehicle*




GB 47955-2026 | China mandatory, effective 2027-01-01

*Scope: safety requirements for combined driver-assistance systems - pilotage (NOA-style), basic single-lane and basic multi-lane functions - plus user information, system deactivation, track and road tests and type-approval judgement.*
*Annex C makes FuSa and SOTIF evidence mandatory: HARA summary, acceptance criteria and confirmation targets, safety strategy, vehicle- and system-level safety analyses, FuSa and SOTIF verification plans and results, safety assessment report - assessed against GB/T 34590 and GB/T 43267, with quantitative safety goals (e.g. unintended lateral motion, ASIL D).*
*Annex E and F add safety-assurance processes (safety policy, risk management, independent internal audits, supplier control) and event data recording (collision and collision-risk events, -15 s to +5 s window).*

# The value of one fused system

## Compliance & reputation




- EU and China market access in one argument.
- One safety case answers R155/156/171 and CN access.
- Audit-ready evidence reduces approval surprises.

## Lower cost



- 'One-for-all': one analysis serves four standards.
- ~80% less duplicate documentation vs ASPICE baseline.
- Less rework when a single standard changes.

## Faster launch



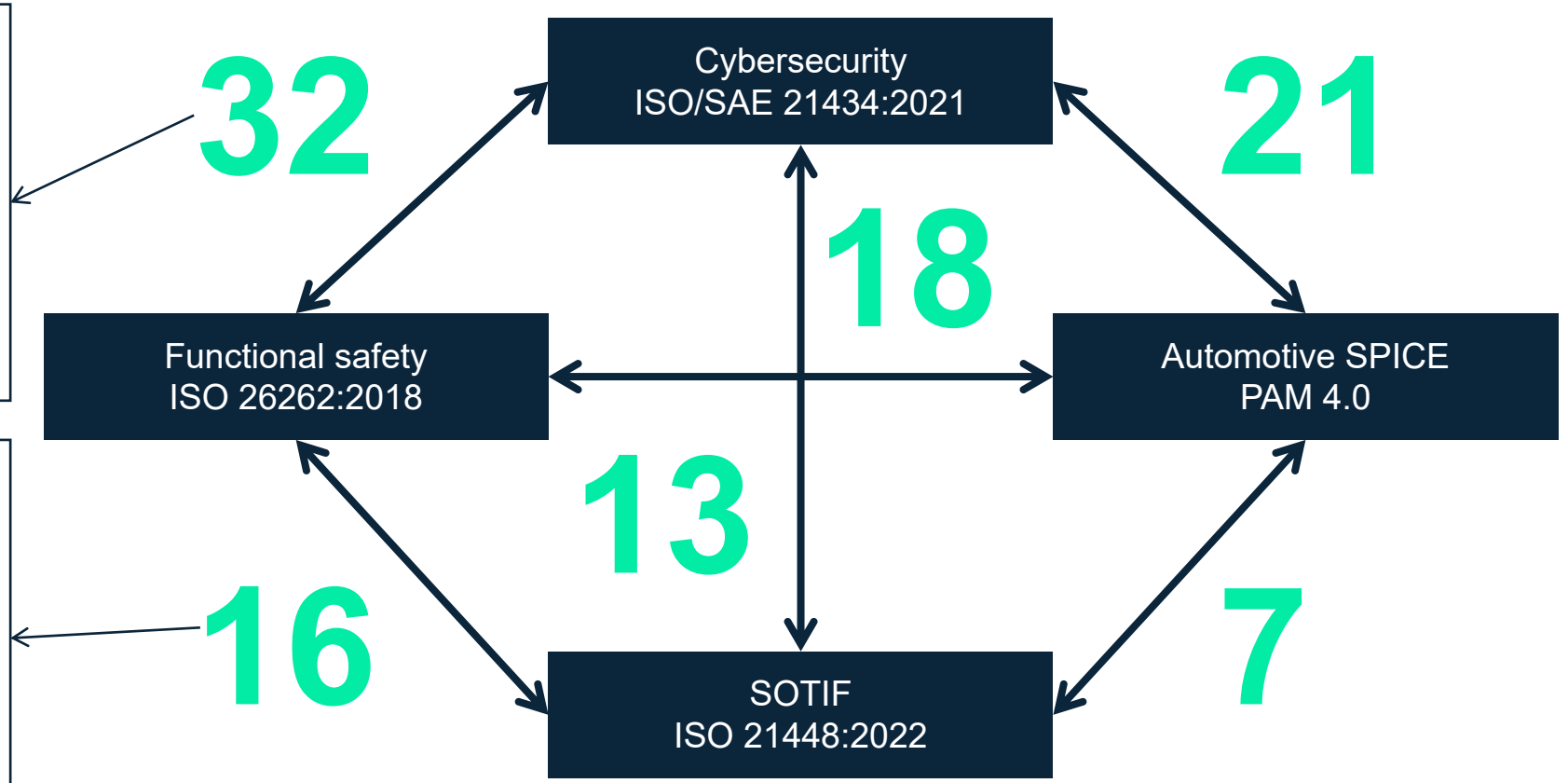
- Parallel certification instead of sequential.
- Earlier release gates shorten time-to-market.
- Demonstrable safety culture becomes brand equity.

# Overlap is not sameness: coupling points

Same process area, different requirements - coupled and mutually influencing.

- Examples:
- Redundancy adds assets: re-assess damage scenarios and attack paths.
- A cyber mechanism failing against a safety goal needs a FuSa mechanism.

- Examples:
- Limiting the ODD may lower the SOTIF risk score.
- A heterogeneous sensor added for SOTIF needs FuSa constraints.



# The second battle is organizational

## Cross-department alignment

- Core: R&D, safety and quality interpret the fused standards differently, so communication slows and goals diverge; functional safety optimises risk avoidance while agile teams optimise iteration speed.
- Symptom: no shared collaboration platform; requirement changes do not sync in real time, rework rises.
- Cost: safety decisions wait on bilateral meetings; issues surface late in verification.

## Process integration burden

- Core: ASPICE stresses process maturity, ISO 26262 functional safety, SOTIF scenario risk; their process, document and verification expectations differ, so integration is hard.
- Symptom: overlapping and redundant activities inflate team load.
- Cost: teams maintain parallel document sets; audits sample the wrong one.

## Culture and change resistance

- Core: departmental silos and process inertia block fusion; safety teams lean waterfall while agile teams demand fast change, and the culture clash defeats collaboration.
- Symptom: staff resist new rituals such as cross-department risk reviews, seeing overhead without visible value.
- Cost: fusion survives only while top management pushes; it decays afterwards.

# A process is WHO does WHAT, WHEN, HOW

Process = when, how and what.

WHEN?

HOW?

WHAT?

WHEN: elastic implementation

HOW: systematic methodology

WHAT: differentiated processes







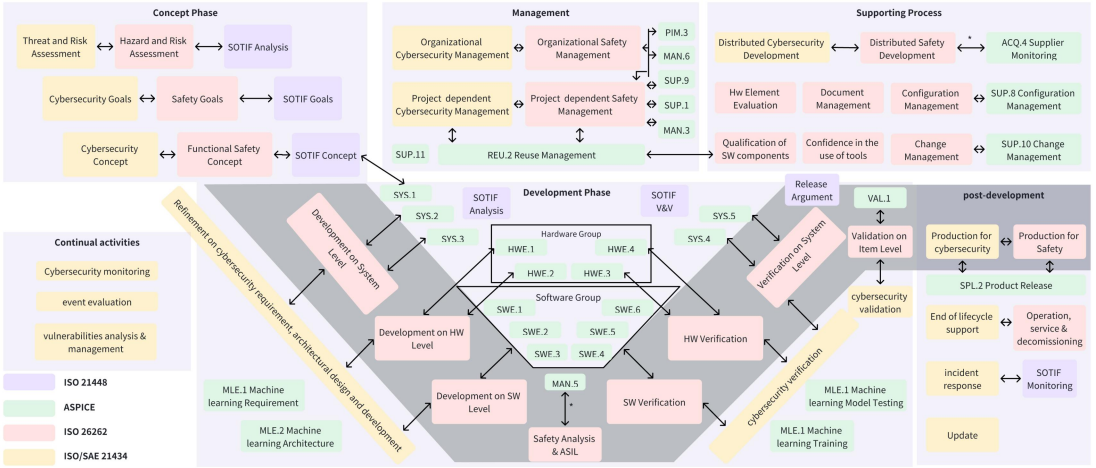
# WHEN: design the process like software

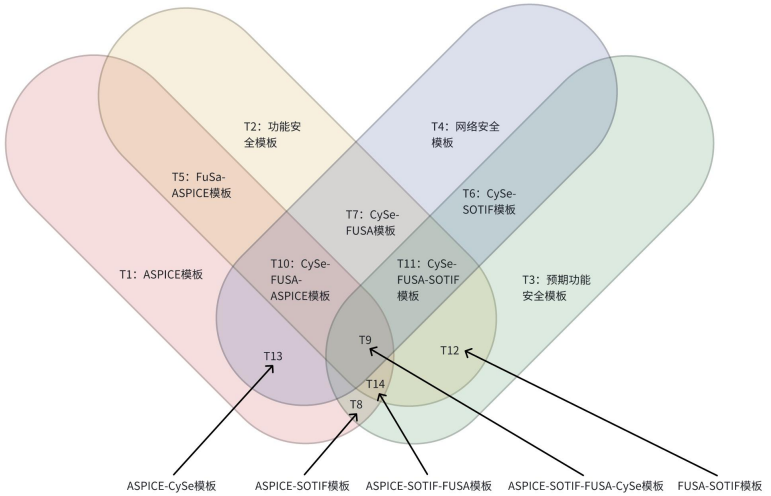
Treat the process system as an architecture:

High cohesion + Low coupling

One process domain satisfies all standards together.

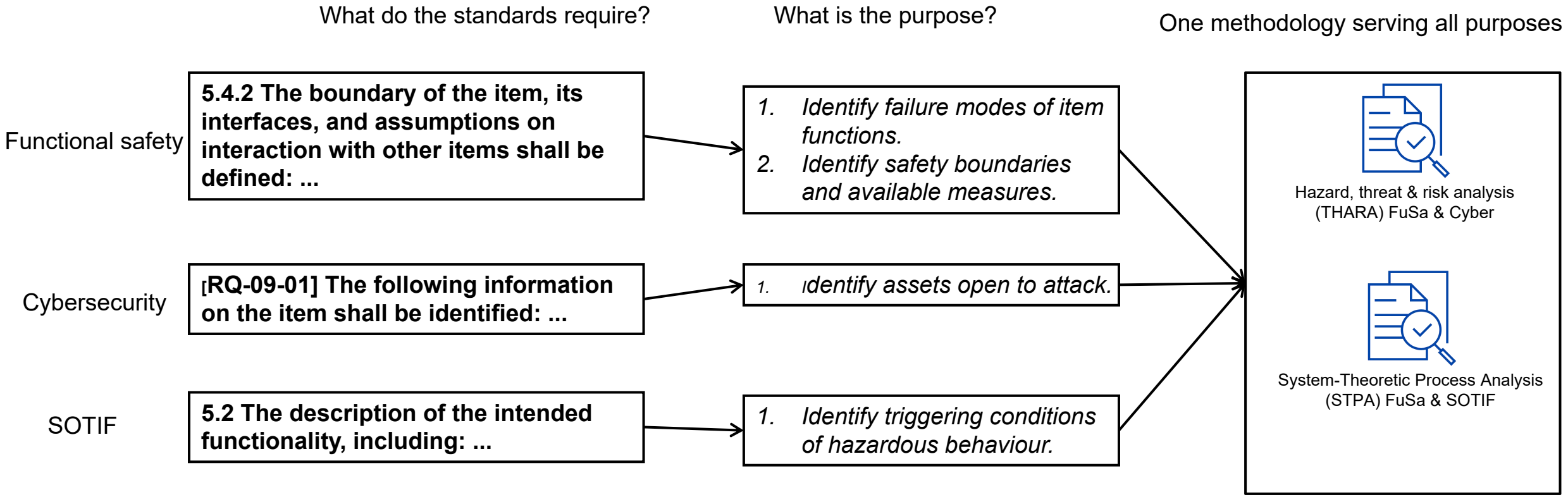
Standard-specific requirements isolated, so projects can tailor.



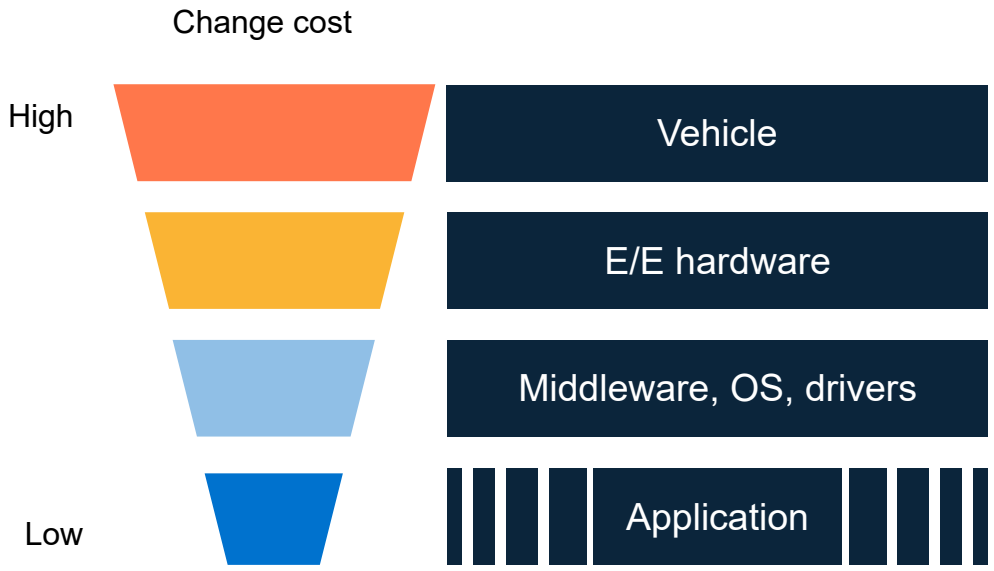
# HOW: first principles above the standards

Ask why behind each requirement, then build one methodology above the standards.

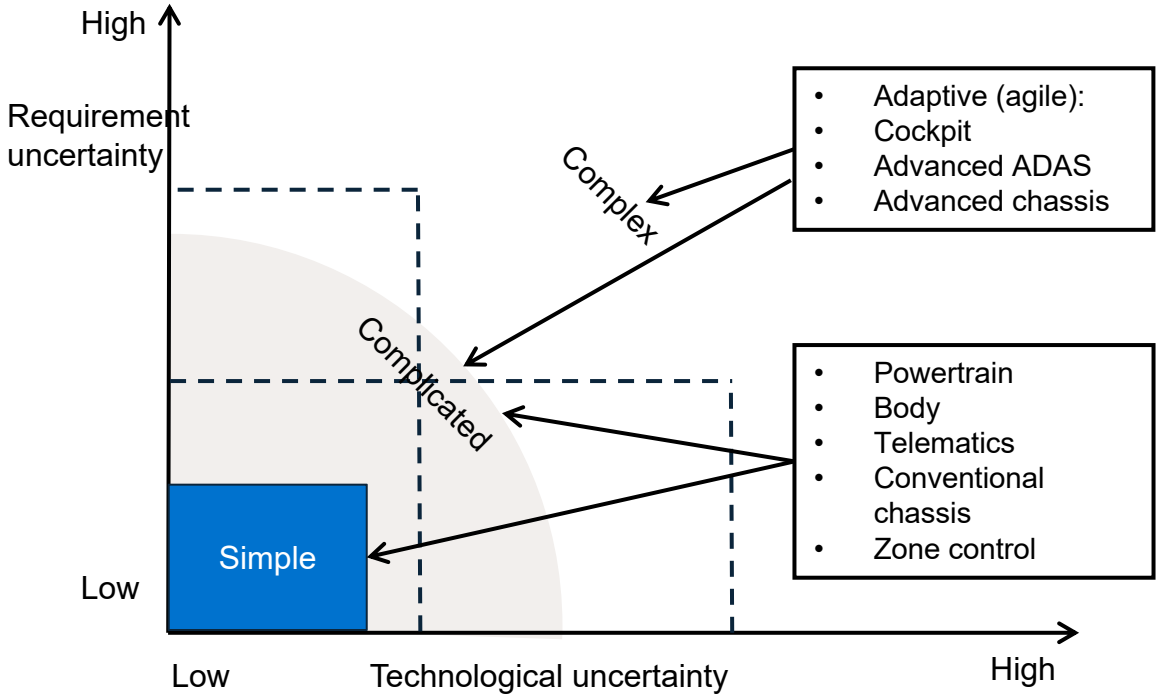


# WHAT: tailor by stack

From one-size-fits-all to fit-for-purpose, by tech stack and product stack.



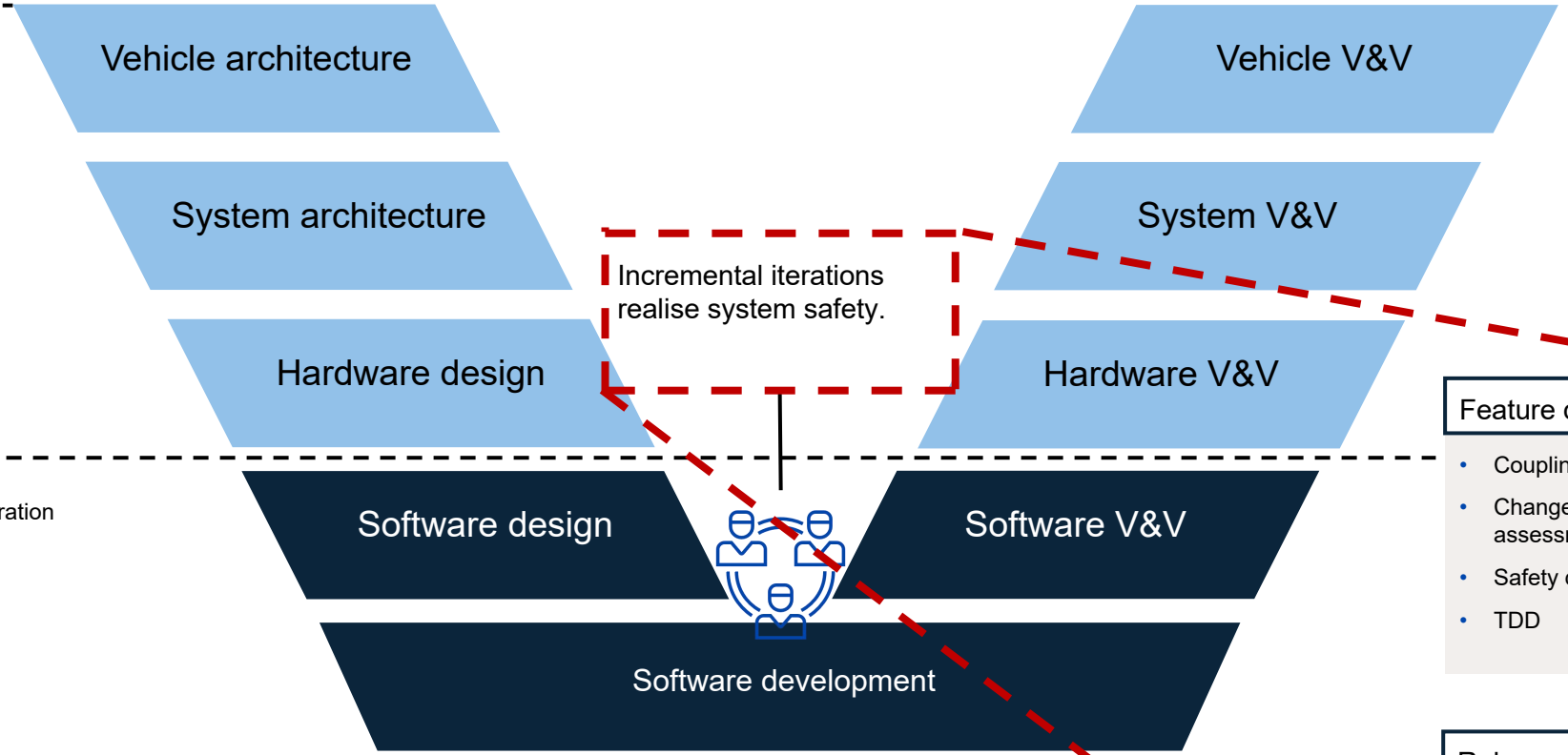

Change cost differs by tech stack.




Uncertainty differs by product stack.

# WHAT cont.: V-model above, agile below

Systems engineering
on DRIFT principles
defines the architecture.




Agile
small steps, continuous iteration
delivering product value.

**Feature development**

- Coupling analysis
- Change safety assessment
- Safety development
- TDD

**Feature verification**

- CI/CD verification
- Known unsafe scenarios
- Simulation
- Fault injection
- Scanning

**Release gate**

- Process audit
- Product assessment
- Release report

**Confirmation**

- Road fleet
- Issue reporting

# Where it goes: The living safety case

## Compliance as a subscription




- Field data and OTA updates keep the safety case current after SOP
- Surveilalance moves from point-in-time approval to continuous oversight
- Every change re-opens the argument automatically
- The certification is a subscription, not a purchase

## An industry case-law library




- Regulators accept argued trade-offs
- The scarce asset is accepted precedent
- Share anonymized balance decisions across OEMs, suppliers
- A neutral convener keeps the library credible

# Thank you



**Tianhong Wu | Principal Expert System Safety, TÜV SÜD Greater China**

**tianhong.wu@tuvsud.com | +86 135 8550 2471**

**Follow us on:**

tuvsud.com
info@tuvsud.com