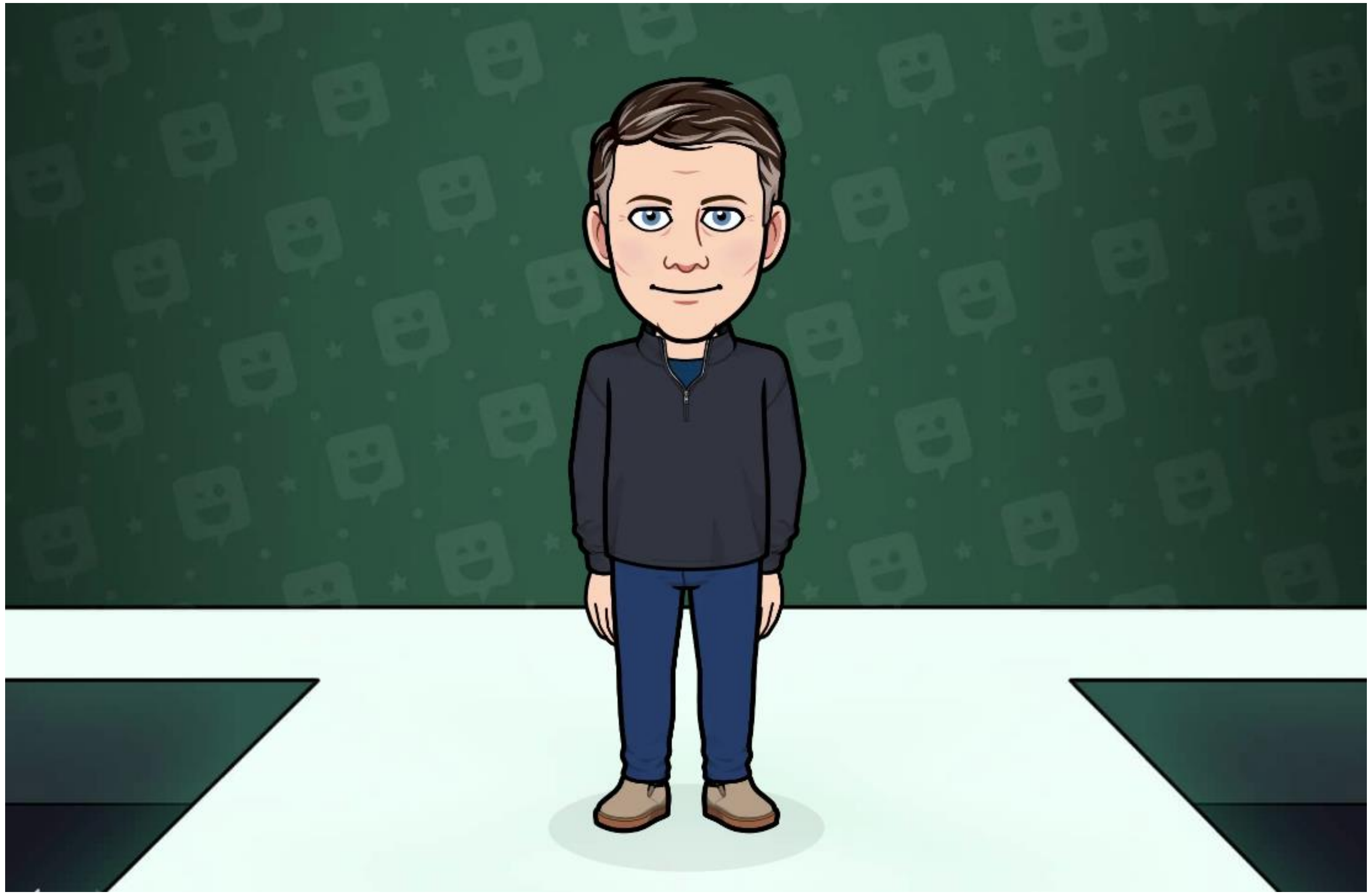
Bits, Bytes, and Brakes: Decrypting ISO/SAE 21434 Certification

Vince Schira

12 September 2024

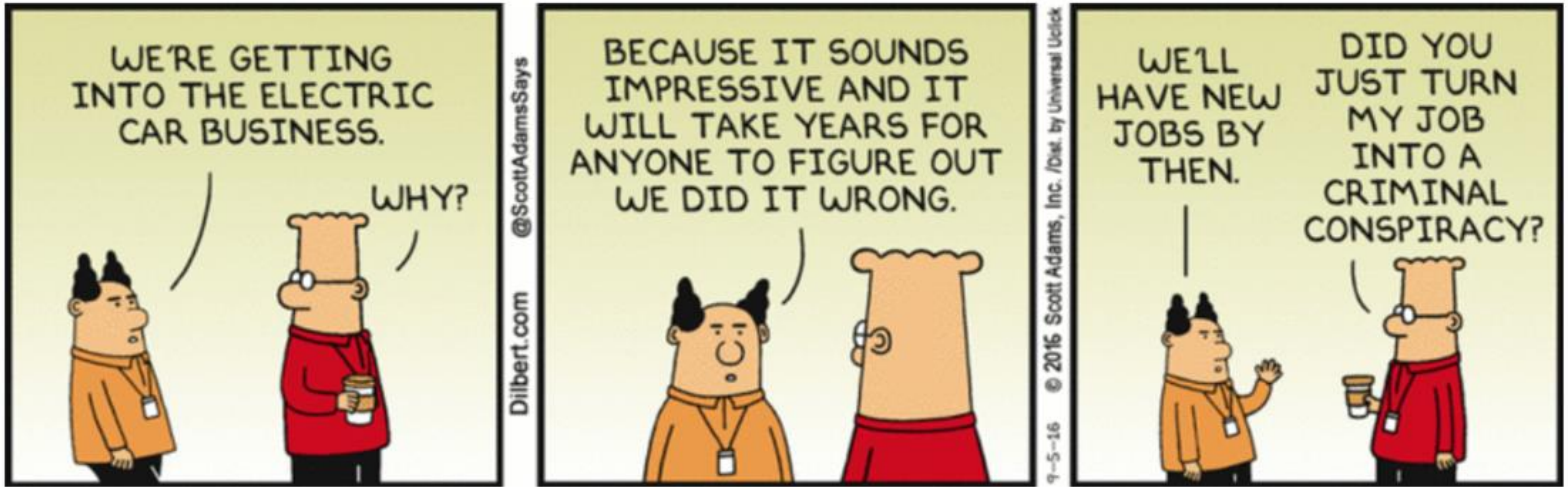
The New Rules of the Road

Meet Your Guide for Today



https://www.linkedin.com/in/vinceschira/

Humor


WE'RE GETTING INTO THE ELECTRIC CAR BUSINESS.
WHY?
@ScottAdamsSays
Dilbert.com
BECAUSE IT SOUNDS IMPRESSIVE AND IT WILL TAKE YEARS FOR ANYONE TO FIGURE OUT WE DID IT WRONG.
9-5-16 © 2016 Scott Adams, Inc. /Dist. by Universal Uclick
WE'LL HAVE NEW JOBS BY THEN.
DID YOU JUST TURN MY JOB INTO A CRIMINAL CONSPIRACY?

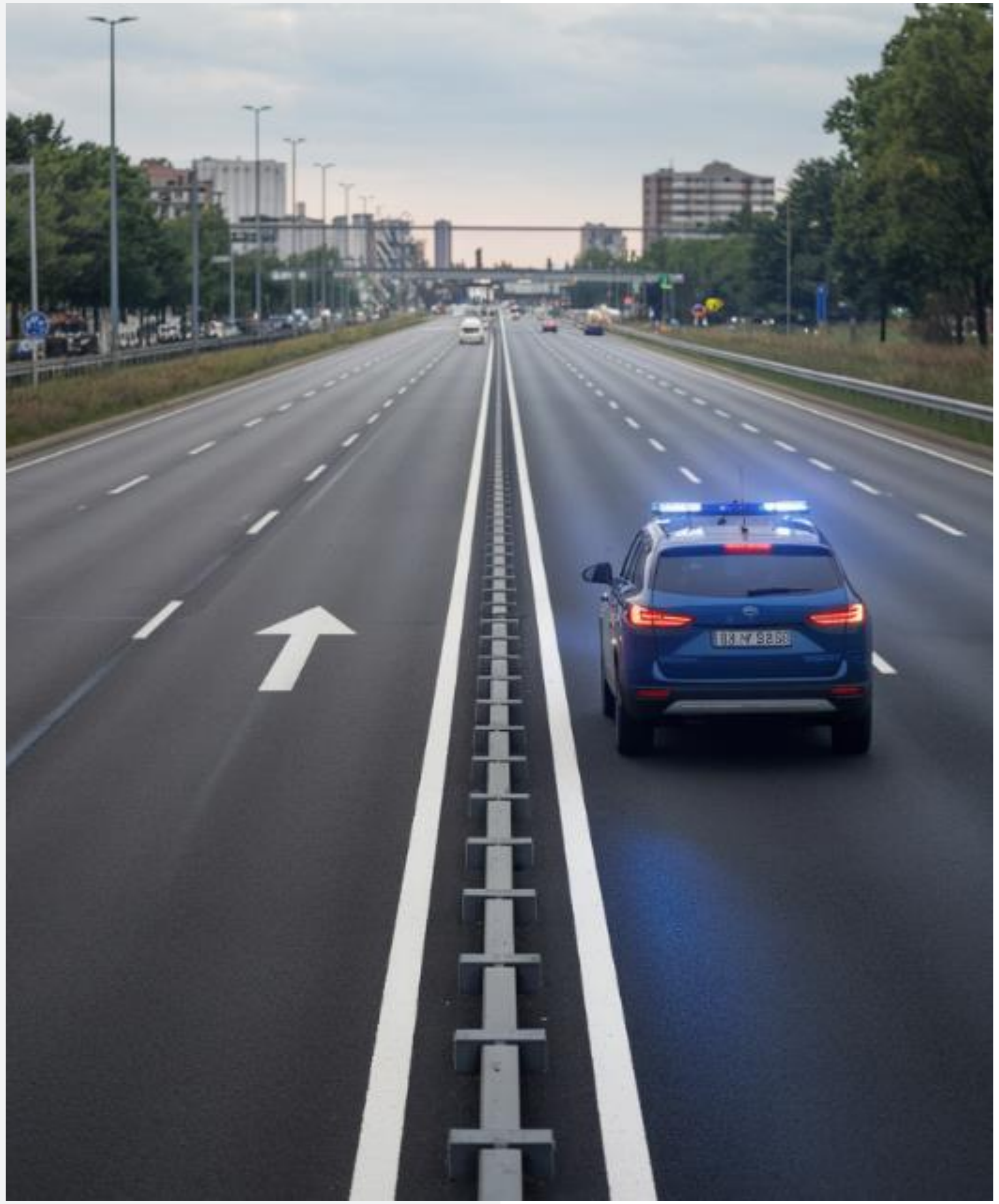
Agenda

- Industry landscape
- History
- Compliance path with UL Solutions
- Maintenance considerations
- Reflections / lessons learned

Industry Landscape

United Nations (UN) R155

- Vehicle cybersecurity regulation for manufacturers
  - Promote economic integration and cooperation
- Cybersecurity management system (CSMS) approval
  - Demonstrate processes for handling vehicle related cyber risks throughout vehicle lifecycle
- Vehicle type approval
  - Specific evidence proving reasonable mitigation measures for cyber risks related to their products
- Spreading as industry standard
  - Implementation/mandate varies
  - EU, UK, South Korea, Japan



United Nations (UN) R155

- Through the CSMS the regulation requires processes and evidence in:
  - Software and systems development
  - Architecture design
  - Software updates
  - Risk assessment
  - Cybersecurity incident management
  - Personal data protection

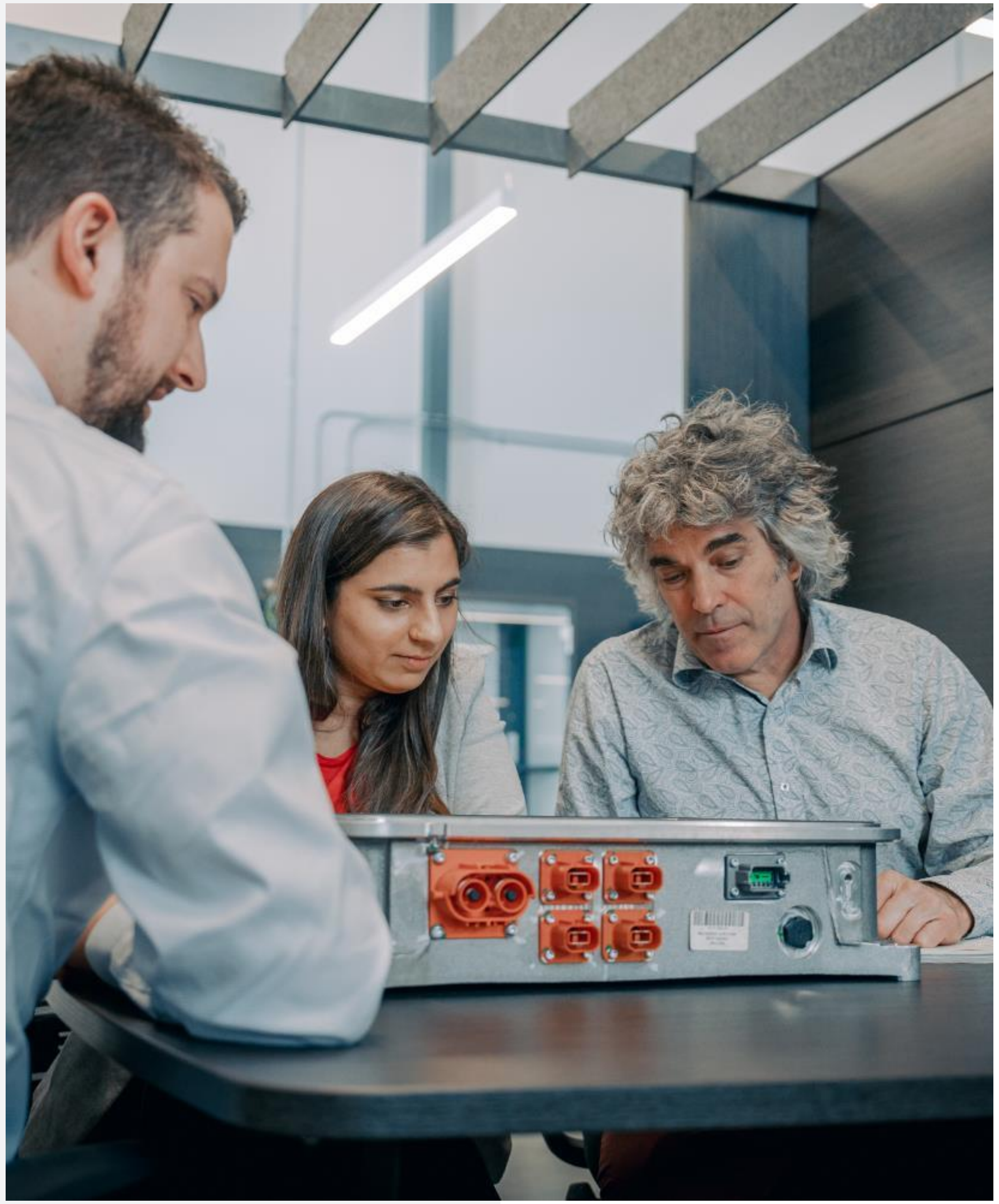
- Risk focus areas manufactures must consider
  - Back-end servers
  - Communications channels
  - Update procedures
  - Human error
  - External connectivity
  - Data or code error/modification
  - Hardening against vulnerabilities

Relationship of UN R155 to ISO/SAE 21434

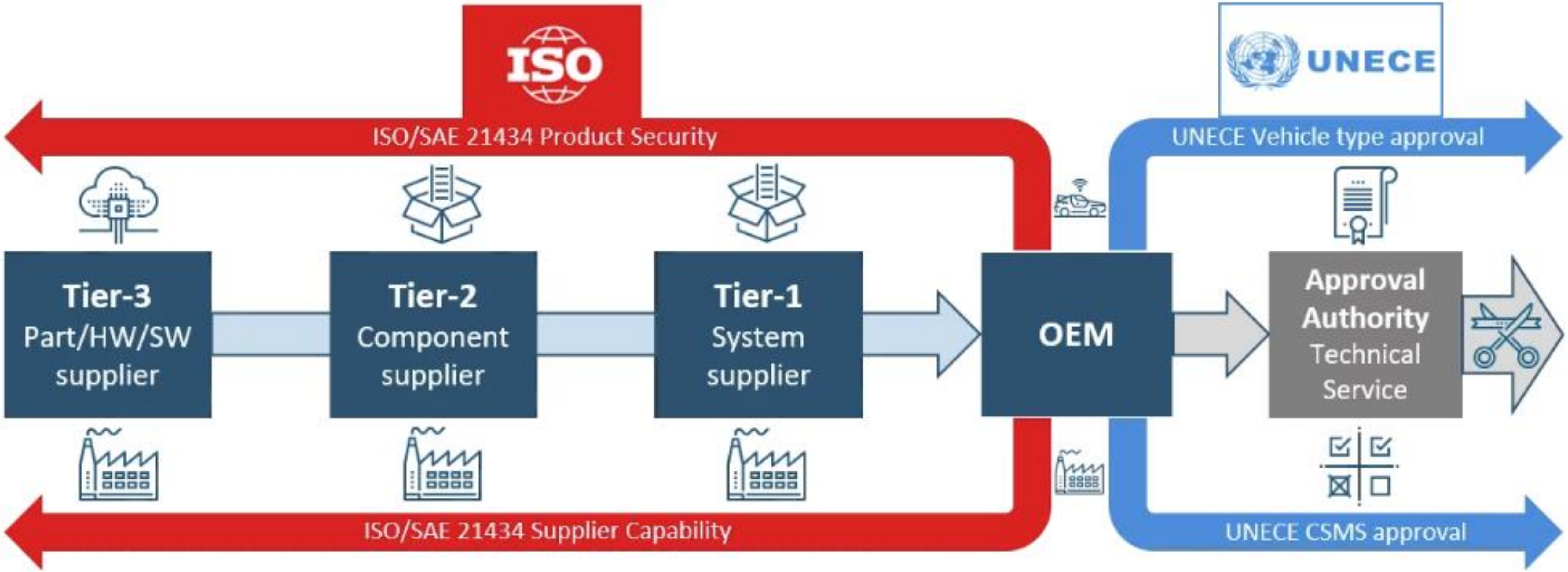
- Suppliers are widely involved in the OEMs cybersecurity ecosystem

- Suppliers do not need their own UN R155 compliance approvals. **They must demonstrate to manufacturers that cybersecurity requirements (a CSMS) have been implemented**

- **If ISO/SAE 21434 is met, a supplier should be able to support UN R155**



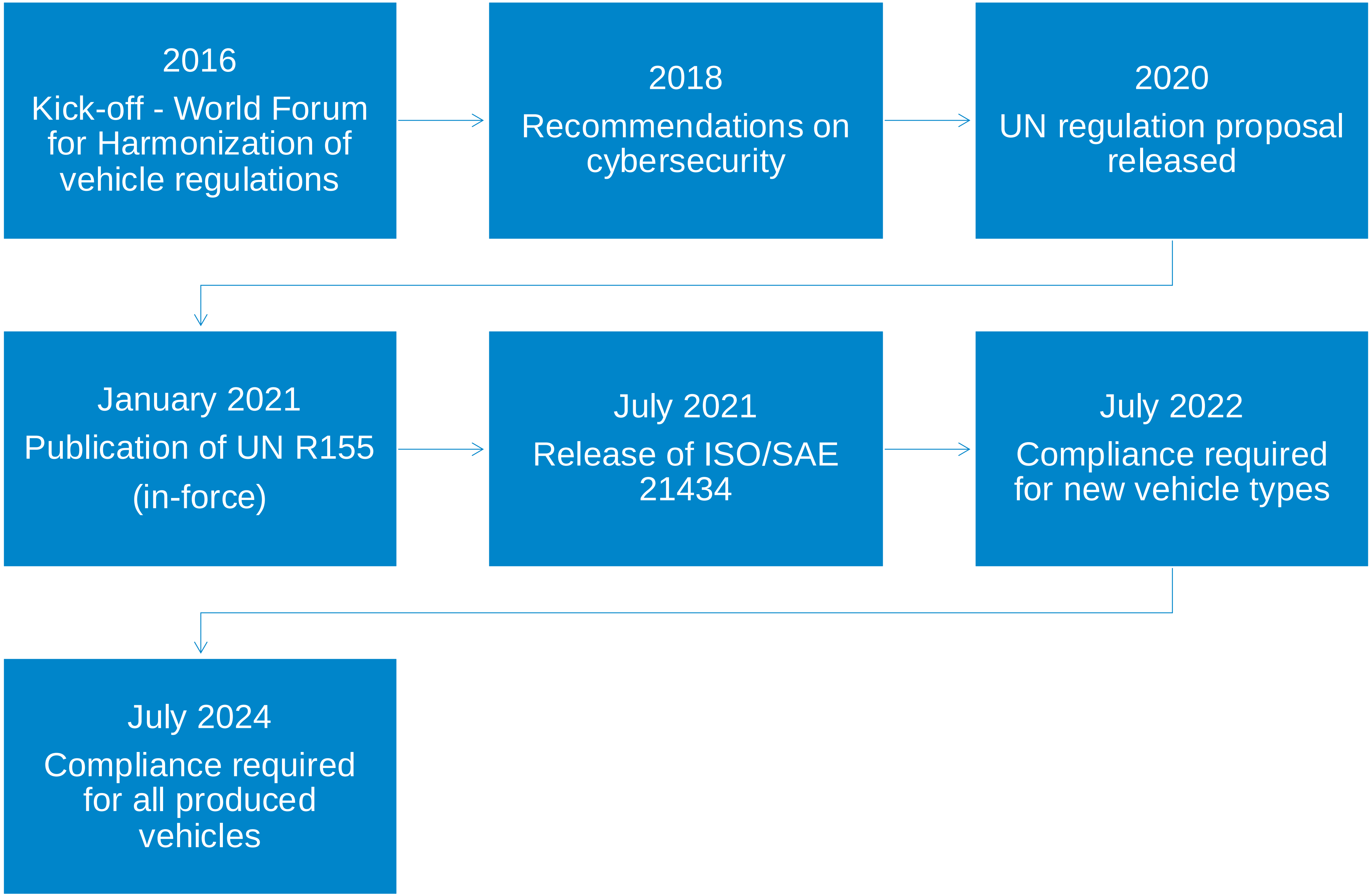
Relationship of UN R155 to ISO/SAE 21434



Source: https://certx.com/automotive/cyber-security-for-road-vehicles-ep-1/

History

UN R155 Timeline



2016
Kick-off - World Forum for Harmonization of vehicle regulations

2018
Recommendations on cybersecurity

2020
UN regulation proposal released

January 2021
Publication of UN R155 (in-force)

July 2021
Release of ISO/SAE 21434

July 2022
Compliance required for new vehicle types

July 2024
Compliance required for all produced vehicles

Compliance Path

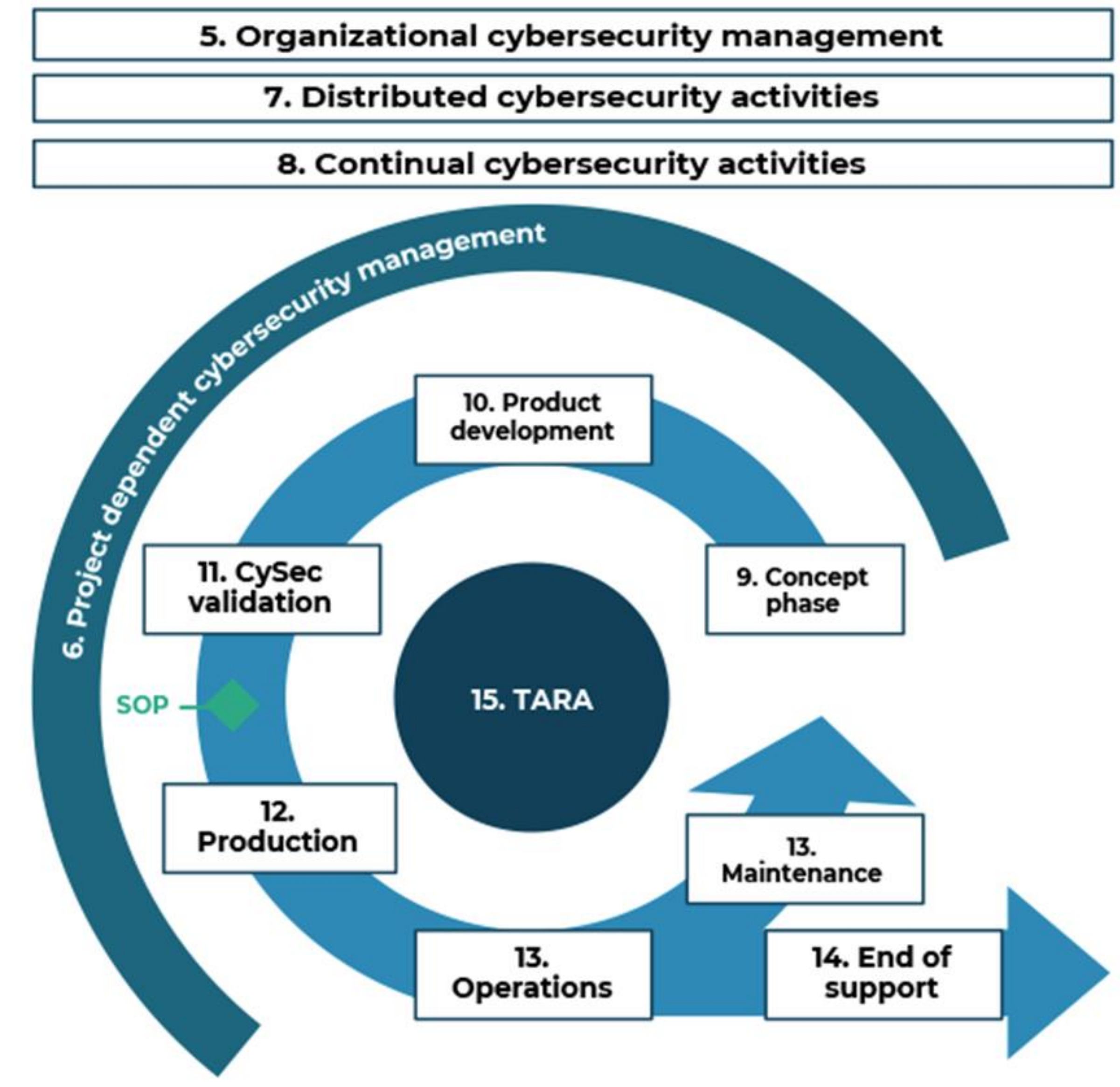
Disclaimer

- The applicability of lessons learned are highly dependent on the specifics of your organization’s culture and products.

ISO/SAE 21434

- Implementation of a CSMS for product cybersecurity

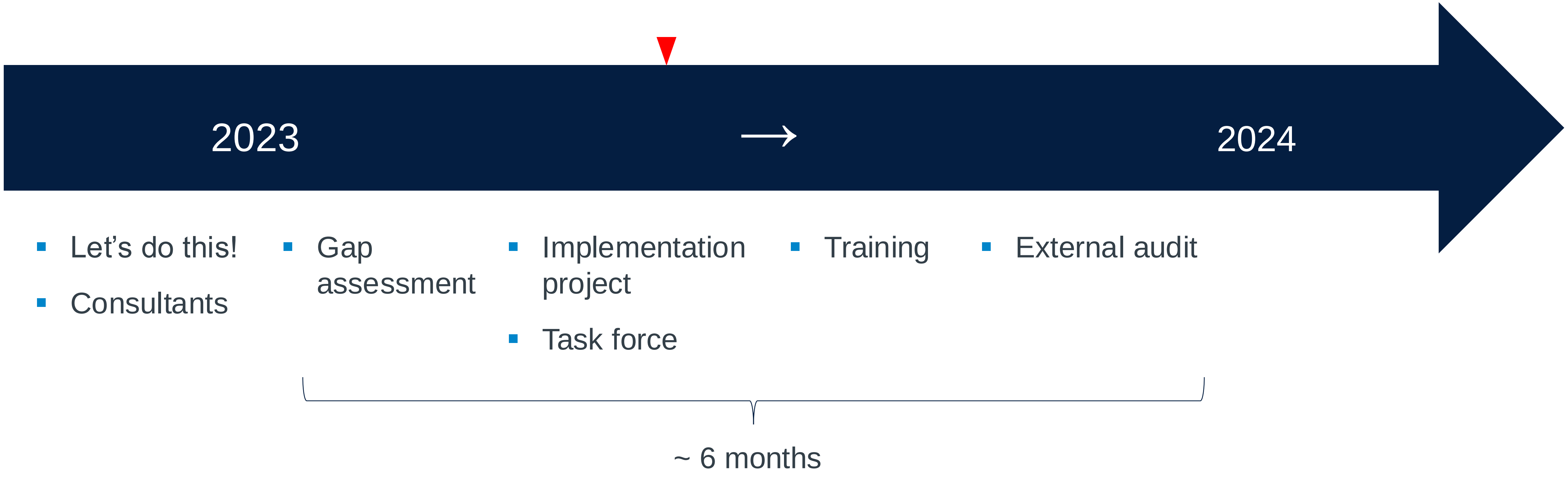
- Similar to ISO 26262, ISO/SAE 21434 looks at the entire development process and product lifecycle
  - Organizational cybersecurity management
  - Project dependent cybersecurity management
  - Product development
    - Threat analysis and risk assessment methods
  - Distributed cybersecurity activities
  - Continual cybersecurity activities
  - Cybersecurity validation
  - Production
  - Operations and maintenance
  - End of cybersecurity support and decommissioning



5. Organizational cybersecurity management
7. Distributed cybersecurity activities
8. Continual cybersecurity activities
6. Project dependent cybersecurity management
10. Product development
11. CySec validation
9. Concept phase
15. TARA
SOP
12. Production
13. Maintenance
13. Operations
14. End of support

Source: https://www.cyres-consulting.com/official-publication-of-iso-sae-21434-first-edition-overview/

Timeline



2023 → 2024

- Let’s do this!
- Consultants

- Gap assessment

- Implementation project
- Task force

- Training

- External audit

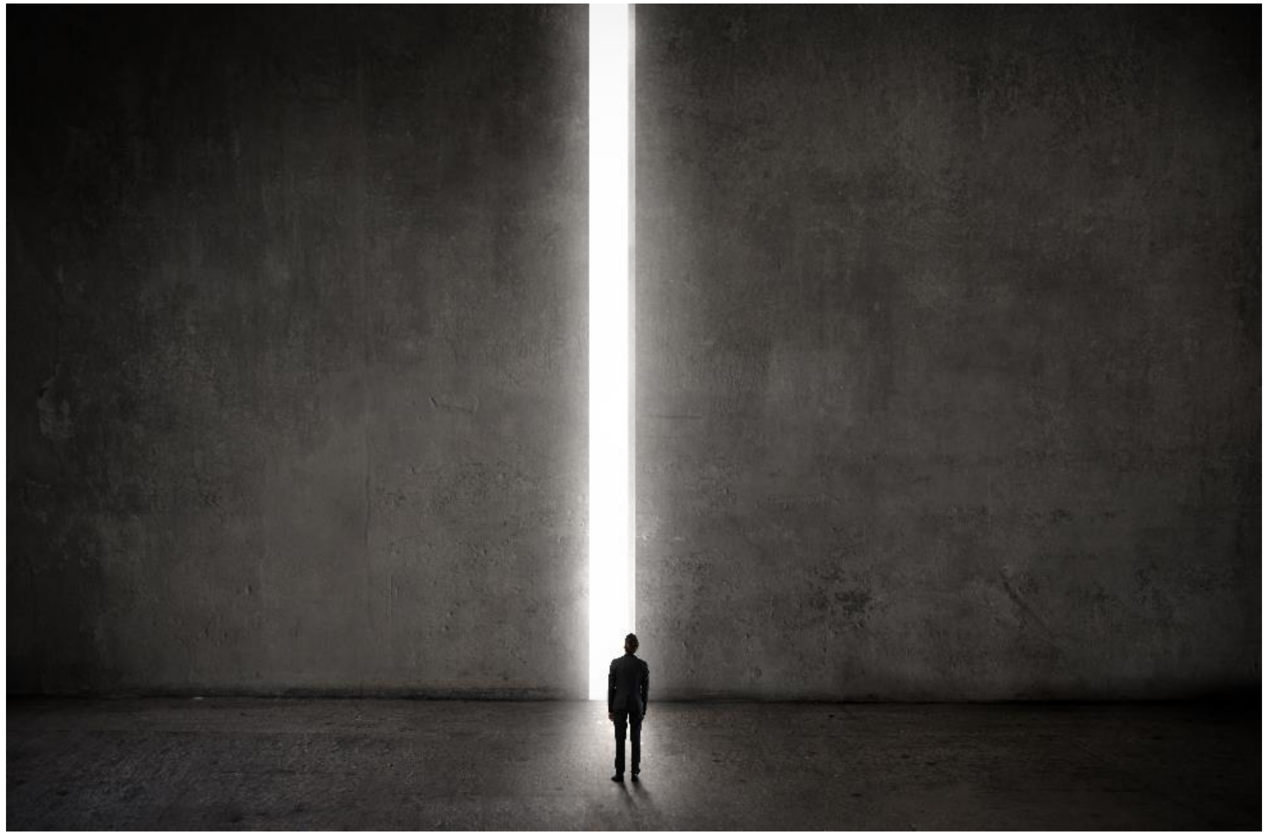
~ 6 months

Consultants

2023 → 2024

- **Let’s do this!**
- **Consultants**
- Gap assessment
- Implementation project
- Training
- External audit

Gap Assessment



2023 → 2024

- Let’s do this!
- Consultants
- **Gap assessment**
- Implementation project
- Training
- External audit

Implementation

2023 → 2024

- Let’s do this!
- Consultants

- Gap assessment

- **Implementation project**

- Training

- External audit

Audit

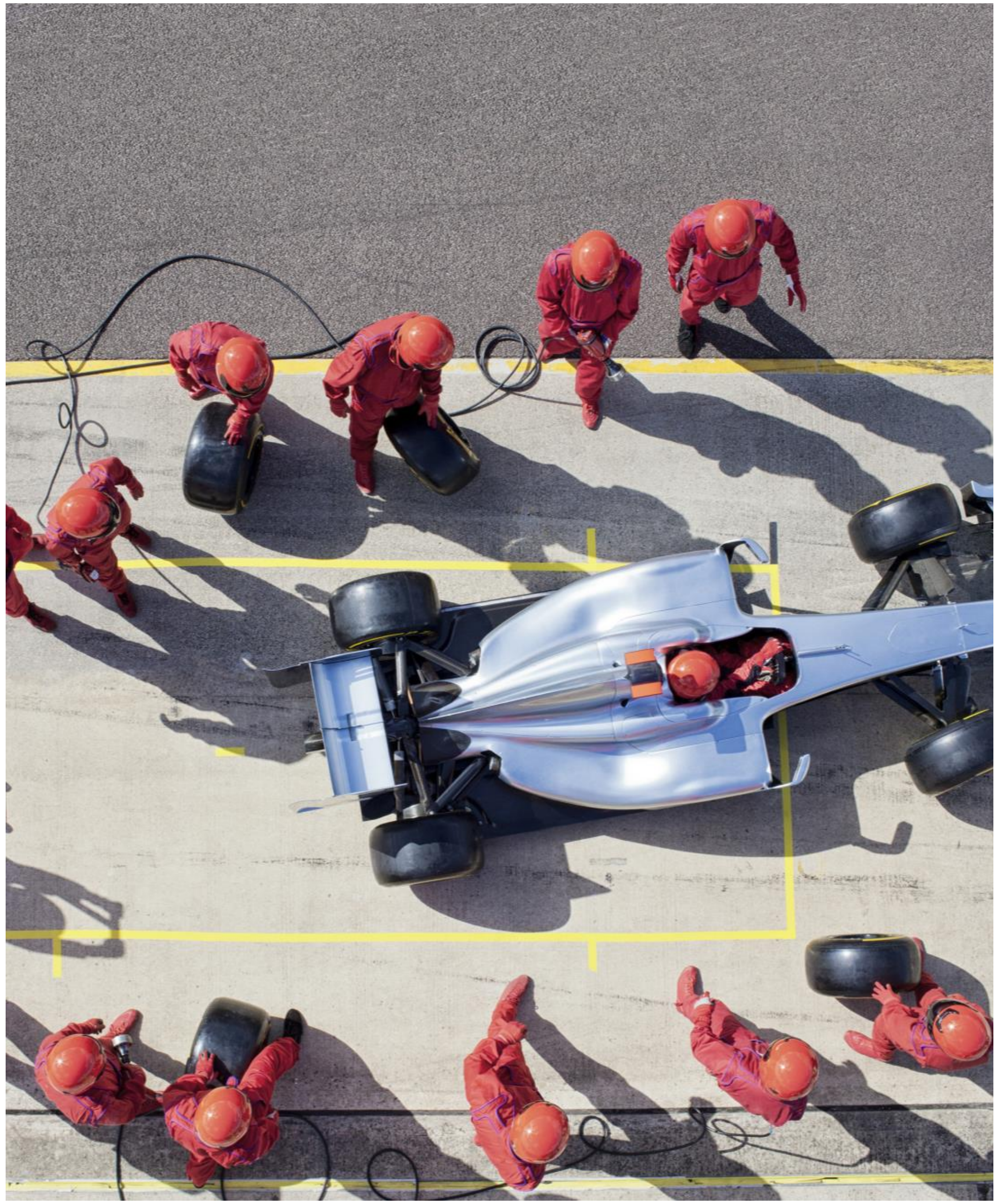
2023 → 2024

- Let’s do this!
- Consultants
- Gap assessment
- Implementation project
- Training
- **External audit**

Maintenance Considerations

Maintaining the CSMS

- Who’s responsible?
  - Executive
  - Tactical
  - Feedback loop
- Centralized / decentralized / hybrid
- Continuous improvement
  - Internal audit
  - Project assessment
  - Weaknesses / vulnerabilities



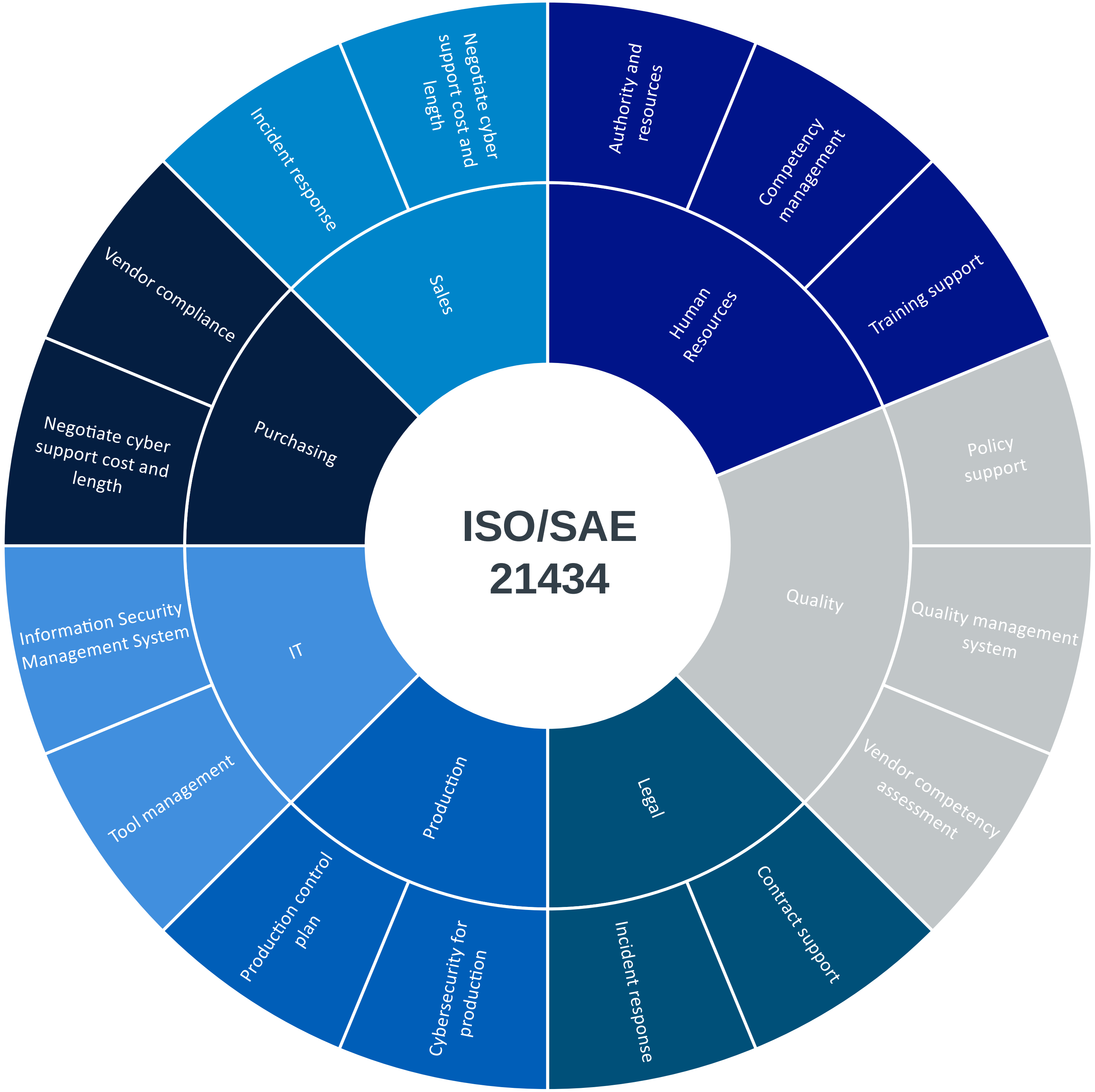
Maintaining the CSMS

- Competence management
- Culture
- Tool management
  - IT security touchpoint

Reflections and Lessons Learned

Lessons Learned

- Project manager
  - –Organizational level



Supply Chain

- Capability of your purchasing / supplier development

- Capability evaluation
- Provide a record of capability
- Align responsibilities
- Include in RFQ

- Software bill of material (SBOM)

Lessons Learned

- Plan ahead
  - Proper resourcing
  - Dedicated support
- Plan for the addition of software embedded products / services

Benefits

- New business / competitive advantage
- Competency / capability evaluation
- Serving one master
- Standard security offering
- Lower risk = lower costs
  - Productivity
  - Response
  - Replacement
  - Fines and judgements
- Unprepared for incidents, information sharing
- Cybersecurity cost not included / unknown

Questions?

https://www.linkedin.com/in/vinceschira/