Interview Protocol

Sec.1 Foreword.

Thank you for taking the time to participate in this interview. We are a research team from xxx, currently conducting research on automotive cybersecurity regulations.

Specifically, this interview aims to achieve the following three objectives:

- Investigate the implementation of current automotive cybersecurity regulations within the industry to identify possible challenges and gaps.
- Evaluate the quality of existing regulations based on your experience and expertise (e.g., TARA in ISO 21434 and the threat catalog in WP29 R155e).
- Reveal the limitations of current regulations and discuss how to improve them.

Please allow me to record the audio and screen capture video of this interview. Personal information (including your name, employer company, etc.) will be properly anonymized. The recorded material will only be used for research purposes and will not be disclosed in any form.

Since we will discuss multiple regulations from various aspects (i.e., testing, TARA, and management), we may encounter some questions that go beyond your area of expertise or job responsibilities. Therefore, if you are not familiar with a specific topic or unsure about the answer to some questions, you may not answer and state that you don't know, and we will skip that part and proceed.

Sec.2 Basic Information Collection.

Q2.1: How long have you been working in the fields of software security and automotive security?

Q2.2: Is your current employer company 1) a first-party manufacturer, or 2) a third-party supplier?

Q2.3: Please describe your job content and responsibilities: is it 1) security testing, 2) TARA analysis, or 3) project management? Please describe in as much detail as possible.

Sec.3 Investigation Security Implementations.

Q3.1: How do existing regulations relate to your specific job content (e.g., TARA, testing, or management)? For example:

- Have you referred to specific threat scenarios in WP29 R155e or GB/T series to guide security testing or risk assessments?
- Have you referred to the TARA method in ISO 21434 to guide risk assessments?
- Have you referred to other specific provisions in ISO 21434 (e.g., standards for development processes, long-term risk management) to assist your work?

Q3.2: How do you implement the content of existing regulations to ensure product cybersecurity? Specifically:

- How do you reference specific threat scenarios in WP29 R155e or GB/T series to guide security testing or risk assessments?
- How do you interpret and translate the TARA method in ISO 21434 to guide risk assessments?
- How do you implement other high-level requirements in the ISO 21434 clauses?

Q3.3: Automotive systems are becoming increasingly complex in terms of external communication and internal architecture. In this challenging context, how does your team ensure that products meet the security baseline specified by current regulations?

Q3.4: How does your team ensure supply chain security? What are the specific challenges? Specifically:

- As a first-party OEM, how do you ensure that products purchased from the supply chain meet security requirements?
- As a third-party supplier, how do you ensure that the products provided meet security requirements?

Q3.5: Ensuring the cybersecurity of complex automotive systems requires the efforts of various teams besides the security team. How do you promote this cross-team collaboration, and what are the specific challenges? Specifically:

- How does your team collaborate with other teams within the company (e.g., development teams, other security teams, and sales teams)?
- How does your team collaborate with external teams (e.g., first-party OEMs, third-party suppliers, certification and consulting agencies related to regulations)?

Q3.6: What are the specific challenges that hinder your team from carrying out cybersecurity activities? For example:

- Insufficient budget for cybersecurity activities.
- Other teams not placing enough importance on security activities.
- Other challenges.

Q3.7: How does your team effectively integrate the latest knowledge in the field of automotive cybersecurity? For example:

- Obtaining information from the latest security reports.
- Gaining insights from recent research papers.
- Communicating with other teams or companies.
- Other methods.

Q3.8: What challenges have you encountered in the process of acquiring the latest knowledge (i.e., obtaining the latest knowledge)? For example:

- Difficulty in correlating acquired knowledge with specific vehicular systems.
- Inconsistent quality of materials.
- Limited access to information.
- Other challenges.

Q3.9: In your work process, do you often encounter problems with information synchronization between security and non-security teams, such as understanding of a specific threat?

Q3.10: (Open-ended question) Has your team encountered any other challenges while conducting cybersecurity activities?

Sec.4 Investigating TARA for Automotive Systems

ISO 21434 proposes a Threat Analysis & Risk Assessment (TARA) consisting of 7 components: asset identification, threat scenario identification, impact rating, attack path analysis, attack feasibility analysis, risk value determination, and risk treatment decision-making.

Q4.1: How do you rate the quality of the text describing this TARA framework in ISO 21434? For example:

- Are there any possible misunderstandings of the concepts involved?
- For each TARA module, do you think the corresponding functions and methods are clearly presented?
- Do you think the examples given in ISO 21434 Appendix clearly demonstrate the operation of its TARA?

Q4.2: How does your team implement or modify this TARA method to adapt to your specific work? Specifically:

- Does your team find all 7 components useful, or are some components of lesser importance?
- Has your team merged any analysis modules?
- Has your team identified any other important analysis modules not covered by the current TARA?

Q4.3: For the specific 7 analysis modules (asset identification, threat scenario identification, impact rating, attack path analysis, attack feasibility analysis, risk value determination, and risk treatment decision-making):

- What specific challenges have been encountered during implementation?
- How much manual effort is required for this analysis?
- Are there currently automated methods to implement these analyses?

Q4.4: Overall, regarding the current TARA guidelines:

- What do you think are the main limitations?
- What are your expectations for the standard TARA proposal?
- How can this TARA be improved?

Sec.5 Investigating Existing Threat Cases

Q5.1: How do you rate the quality of the text describing specific threats in WP29 R155e and GB/T series? Are there any possible misunderstandings of the concepts involved? Specifically, please evaluate the existing threats from the following indicators:

- Existing threats clearly identify the affected assets in automotive systems.
- Existing threats clearly describe how an attacker can exploit a specific threat (e.g., specific attack methods, attack vectors, and attack impacts).
- Existing threats present clear root causes, explaining why these threats exist.
- Existing threats are paired with explicit security testing methods to identify the mentioned threats.
- Existing threats are paired with explicit mitigation measures to protect automotive systems from the mentioned threats.

For each of the above statements, please give your rating based on the following criteria:
(1. Strongly disagree; 2. Disagree; 3. Neutral; 4. Agree; 5. Strongly agree)

Q5.2: Based on the initial threat database we sent you in advance:

- Which parts of the threats involved are most relevant to your expertise (e.g., IVI functions, OTA)? Or are you particularly familiar with or interested in?
- Can you provide specific and practical threats to supplement the existing content?
- Have you identified any important categories not covered by the current database?

Q5.3: (Open-ended question) Please openly discuss your impressions of the existing threats in the current regulations. Specifically:

- How do you qualitatively and quantitatively evaluate their quality?
- What are your expectations for the threats listed in the regulations?

Sec.6 Discussing Potential Limitations on Current Regulations

Q6.1: What assessment results would you give for the quantity and quality of threats given in existing standards and regulations? Have you identified any obvious limitations in quantity or quality?

Q6.2: Do you believe that current regulations provide practical and effective specific threats for automotive systems? Or do you think these threats are still largely copied from threats in other domains (e.g., mobile security, server security)?

Q6.3: Do you believe that a lack of objective and unified assessment criteria leads to inconsistencies in security implementation?

Q6.4: Do you think there is a lack of prioritization for specific threats, making it difficult for manufacturers to determine which threats are more severe and should be prioritized?

Q6.5: Do you think the current threat descriptions are clear enough to help you understand the threats in a specific context (e.g., attack paths shown in ISO 21434)?

Q6.6: Do you think current regulations provide effective guidance for security testing?

Q6.7: Do you think the mitigation measures in existing regulations are more like remediation measures after an attack? Would you expect some advanced security solutions to be adopted at the early development stage?

Q6.8: Do you think current threats and testing methods focus more on black-box and gray-box scenarios? Would you find it helpful if more specific guidance was provided for white-box scenarios (e.g., when manufacturers have access to the source code of ECUs)?

Q6.9: Do you think the threats given in current regulations are up-to-date? Or do you think they have not been able to keep up with the rapid development of the industry?

Q6.10: Have you identified a gap between cybersecurity testing and functional safety testing? Do you think establishing effective safety testing standards is more challenging than security testing?

Q6.11: Do you think the testing methods in current regulations can be practically applied to real products? Or do you think they are too idealized and cannot meet the implementation needs of various vehicle models?

Q6.12: Have you found that the impact scope description of specific threats is insufficient? For example, various ECUs are connected via buses in IVN topology, and a threat on one ECU may lead to another threat on a specific ECU.

Sec.7 Outro

Thank you very much for taking the time to participate in this interview.

Is there anything we didn't cover during the interview that you would like to discuss?

Do you have any suggestions on how we can improve this interview process?

Do you know any other experts who could be invited to participate in our interviews?

If you have any further additions to the content of today's interview, please feel free to contact me. Thank you again!