R155 Items: Failure Conditions

Description

The following is taken from the R155 interpretation document. It enumerates the explicit reasons for considering individual R155 requirements as unfulfilled.

Note: The requirement is considered **unfulfilled** if any of the items listed are true.

7.2.2.2(a) Cybersecurity Management

1. Processes are absent or incomplete.
2. Processes are not applied universally or consistently.
3. Processes are often or routinely circumvented to achieve business objectives.
4. The vehicle manufacturer's security governance and risk management approach have no bearing on its processes.
5. System security is totally reliant on users' careful and consistent application of manual security processes.
6. Processes have not been reviewed in response to major changes (e.g., technology or regulatory framework), or within a suitable period.
7. Processes are not readily available to staff, too detailed to remember, or too hard to understand.

7.2.2.2(b) Risk Identification

1. Risk identification is not based on a clearly defined set of assumptions.
2. Risk identification for vehicle types is a "one-off" activity (or not done at all).
3. Vehicle types are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g., interactions between IT and OT environments).

7.2.2.2(c) Risk Assessment / Treatment

1. Risk assessment outputs are too complex or unwieldy to be consumed by decision- makers and are not effectively communicated in a clear and timely manner.
2. Security requirements and mitigation techniques are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of vehicle types.
3. Only certain domains or types of assets are documented and understood. Dependencies between assets are not understood (such as the dependencies between IT and OT).
4. Inventories of assets relevant to vehicle types are incomplete, non-existent, or inadequately detailed.
5. Asset inventories are neglected and out of date.
6. Systems are assessed in isolation, without consideration of dependencies and interactions with other systems (e.g., interactions between IT and OT environments).
7. Risk assessments are not based on a clearly defined set of assumptions.
8. Risk assessments for vehicle types are a "one-off" activity (or not done at all).

7.2.2.2(d) Verification of Risk Management

1. The security elements of projects or programs are solely dependent on the completion of a risk management assessment without any regard to the outcomes.
2. There is no systemic process in place to ensure that identified security risks are managed effectively.
3. Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve.

7.2.2.2(e) Cybersecurity Testing

1. A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value.
2. Assurance methods are applied without appreciation of their strengths and limitations, such as the risks of penetration testing in operational environments.
3. Assurance is assumed because there have been no known problems to date.

7.2.2.2(f) Risk Assessment Kept Current

1. No processes are in place which require the risk assessment to be updated.

7.2.2.2(g) Adaptable Monitoring / Response

1. The vehicle manufacturer has no sources of threat intelligence.
2. The vehicle manufacturer does not apply updates in a timely way, after receiving them.
3. The vehicle manufacturer does not evaluate the usefulness of its threat intelligence or share feedback with providers, authorized aftermarket service providers or other users.
4. There are no staff who perform a monitoring function.
5. Monitoring staff do not have the correct specialist skills.
6. Monitoring staff are not capable of reporting against governance requirements.
7. Security alerts relating to vehicle types are not prioritised.

7.2.2.5 Supplier Deficiency Management

1. Relevant contracts with suppliers and service providers do not have cyber security requirements.