(ISO 21434)

Automotive Cybersecurity – Cybersecurity Operations and Maintenance Process (Clause 13)

- JBM Electric Vehicle Pvt. Ltd.

Document Version 1.0 b

DOCUMENT INFORMATION

Version	Release date	Description of change	Prepared by	Approved by
V1.0a	05.06.2024	Original Issue		
V1.0b	17.06.2024	Updated JBM Logo		

CONTENT

1. PURPOSE

The purpose behind the operations and maintenance clause is to explain how JBM determines and implements remedial actions for cybersecurity incidents along with maintaining cybersecurity process and guidelines throughout production, also with postproduction (includes during and after performing updates to the items or components) until the end of cybersecurity support.

2. SCOPE

This document's scope is focused on the incident response procedure and includes information on updates performed to the items or components in the field during production and postproduction.

3. RESPONSIBILITY

Top Management

a) Analyze the capital and resource availability required to meet the process requirements for efficient cybersecurity initiatives.

Cybersecurity Leader

a) The cybersecurity leader should manage cybersecurity team's operations and maintenance.

Cybersecurity Team

a) The cybersecurity team should develop a cybersecurity incident response plan and perform the tasks required for supporting operations and maintenance, including security incident investigation, communication, and remediation.

Incident Response Team leader

a) The Incident Response Team Leader is responsible for initiating and coordinating incident response activities, as well as updating the incident response process based on emerging threats, changes in technology, or organizational requirements.

4. TERMS

Asset

Object that has value or contributes to value.

Attack Feasibility

Attribute of an attack path describing the ease of successfully conducting the corresponding set of actions

Component

Part that is logically and technically separable

Cybersecurity

(Road vehicle cybersecurity) condition in which assets are sufficiently protected against threat scenarios to items of road vehicles, their functions and their electrical or electronic components.

Cybersecurity Event

Cybersecurity information that is relevant for an item or component

Cybersecurity Incident

Situation in the field that can involve vulnerability exploitation.

Cybersecurity Information

Information regarding cybersecurity for which relevance is not yet determined.

Cybersecurity property

Attribute that can be worth protecting

Risk

Cybersecurity risk (effect of uncertainty on road vehicle cybersecurity expressed in terms of attack feasibility and impact)

Risk management.

Coordinated activities to direct and control an organization regarding risk.

Vulnerability

Weakness that can be exploited as part of an attack path.

5. ABBREVIATION

Sr. No	Term	Abbreviation
1	IR	Incident Response
2	IRT	Incident Response Team
3	ISO	International Organization for Standardization
4	IT	Information Technology
5	RQ-XX-XX	Requirement-Clause number of ISO/SAE 21434:2021 standard Clause wise serial number of Requirement
6	SAE	Society of Automotive Engineers
7	SIEM	Security Information and Event Management
8	TARA	Threat Analysis and Risk Assessment
9	JBM	JBM Electric Vehicle Pvt. Ltd.

6. OPERATION AND MAINTAINANCE

Response to cybersecurity incidents and field-based updates to components or objects. Response to security incidents as a component of vulnerability management. Updates are changes made to JBM products or JBM components after they have been developed, and they may contain additional information like technical specifications, integration guidelines, and user manuals. JBM might make updates to address vulnerabilities, address security issues, or enhance functionality. Update-related work products are documented similarly to other work products from ISO/SAE 21434:2021-compliant clauses.

6.1. Inputs

To support its operations and maintenance-related work product, which is primarily JBM's cybersecurity incident response plan, JBM should take into consideration a vulnerability analysis report as well as any cybersecurity incident-related information, if already accessible

6.1.1. Remedial Actions

Remedial actions include details about how vulnerabilities are managed. These actions specify how cybersecurity risks for each vulnerability are identified. A threat analysis and risk assessment activity conducted prior to gathering vulnerabilities helps to manage them accordingly. Remedial action also specifies how the vulnerability is eliminated by using appropriate remediation technique.

6.1.2. Communication Plan

Internal stakeholders such as marketing or public relations, product development teams, legal, customer relations, quality management, and purchasing may be involved in the communication plan making activity. Identification of internal and external communication partners and development of specific content for various audiences can all be part of a communication plan. *(JBM_Communication Matrix v1.0a.docx)*

6.1.3. Incident handling checklist

The incident handline checklist to be followed which involves detection and analysis, containment and recovery and post-incident activity.

6.1.4. Incident monitoring

Our cybersecurity incident monitoring process focuses on critical components like software platforms and network infrastructure. We categorize incidents by type (e.g., unauthorized access, data breaches) and identify affected cybersecurity attributes (confidentiality, integrity, availability) for impact assessment. We utilize robust logging systems such as SIEM tools and ensure continuous monitoring with real-time alerts. Stakeholders are promptly notified via email or SMS, and we maintain defined response times for incident resolution.

6.1.5. Assigned responsibilities for the remedial actions.

Assigned responsibilities are JBM personnel who may have good knowledge of the items or components, organizational knowledge, and decision-making authority.

6.1.6. Recording new cybersecurity information relevant to cybersecurity incident

This procedure involves information on affected components, associated incidents and vulnerabilities, forensic data such as data logs, crash sensor data, and/or end-user complaints, that can be gathered in line

with cybersecurity monitoring activity.

6.1.7. Method for determining progress.

The percentage of impacted items or components that have been remediated, as well as the percentage of items or components that have been affected by remedial activities, are used as indicators of progress.

6.1.8. Criteria for closure of the cybersecurity incident response

A decision regarding closure of an incident depends on its severity as well as remediation option chosen as part of either TARA activity or an independent assessment.

6.1.9. Actions for the closure

A rationale for how a cybersecurity event is managed is closure action. This could also include categorizing each incident based on the chosen course of action.

6.1.10. Work Product

Incident response plan

6.2. Incidence response plan

For each cybersecurity incident, a cybersecurity incident response plan is going to be created that includes:

- remedial actions

  Document specific steps and procedures to remediate the cybersecurity incident effectively. This may include isolating affected systems, restoring backups, applying security patches, and implementing measures to prevent similar incidents in the future.

  NOTE 1 Remedial action are determined by vulnerability management.

  (Refer ISO/SAE 21434:2021 clause 8.6)

- a communication plan.

  Define a communication plan outlining how information about the cybersecurity incident will be communicated internally and externally. Specify communication channels, key stakeholders, escalation paths, and messaging protocols to ensure timely and accurate dissemination of information.

  NOTE 2 The creation of a communication plan can involve internal interested parties, e.g., or public relations, product development teams, legal, customer relations, quality management, purchasing.

  NOTE 3 A communication plan can include identification of internal and external communication partners (e.g., development, researchers, the public, authorities) and development of specific information for these audiences.

- assigned responsibilities for the remedial actions.

  Assign clear roles and responsibilities to individuals or teams responsible for conducting remedial actions. Ensure that responsibilities are aligned with each person's expertise and authority, facilitating swift and coordinated response efforts.

  NOTE 4 Those responsible can have:

- *expertise in affected items or components, including legacy items and components.*
- *organizational knowledge (e.g., business processes, communications, purchasing, legal); and/or*
- *decision authority.*

- a procedure for recording new cybersecurity information relevant to the cybersecurity incident.

  Establish a standardized procedure for recording new cybersecurity information relevant to the incident, such as incident details, investigative findings, mitigation strategies, and lessons learned. This ensures that all pertinent information is documented accurately for future reference and analysis.

- a method for determining progress.

  Define criteria and metrics for measuring progress in addressing the cybersecurity incident. This may include milestones achieved, impact mitigation, containment efforts, and restoration of normal operations. Regularly track and assess progress against these metrics to gauge the effectiveness of response efforts.

- criteria for closure of the cybersecurity incident response.

  Identify specific criteria that must be met for the cybersecurity incident response to be considered resolved and closed. This may include confirmation of successful remediation, verification of system integrity, cessation of malicious activity, and restoration of services to pre-incident levels.

- actions for the closure.

  Outline the final steps and actions to be taken to formally close the cybersecurity incident response process. This may include conducting post-incident reviews, documenting lessons learned, updating security controls and policies, and communicating closure to relevant stakeholders.

  A cybersecurity incident response plan is a 4-Step procedure that helps JBM incident response team to efficiently and effectively react when an incident happens on JBM owned product.

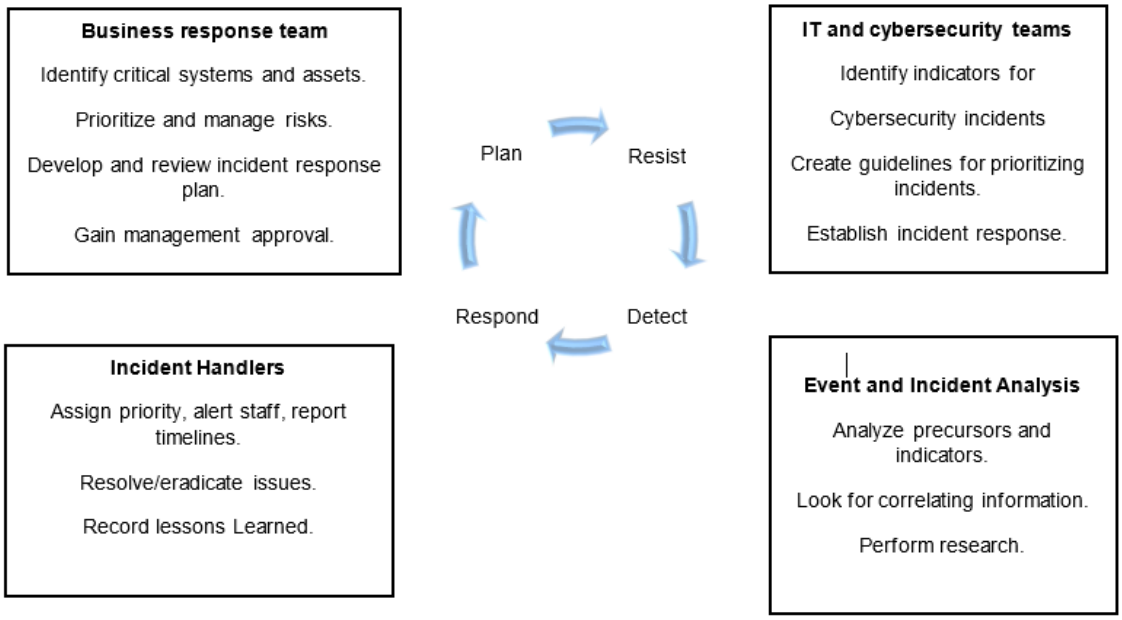


fig 01 Software structural Design

6.2.1. Plan

The success of an incident response plan is determined on how well it is planned. The plan phase comprises creating a well-defined strategy that directs the incident response team to perform all the actions correctly during an incident. JBM product owner will perform annual evaluations and drills to prepare the team in the case of an active cyber incident. As part of the Plan phase, the following steps are conducted:

- Referring to the existing incidents: The IRT leader oversees informing the core team and starting the IR process at this point. It is highly recommended to look for similar historical instances and gather information. This would aid in determining failure mechanisms or mitigations that were overlooked. In the resist phase, referring to the corresponding TARA might assist to comprehend the severity level and threat vector identifications.

- Forming the incident response team: Required team is identified to start the incident investigation process.

Recording the incident: In this step, incidents are appropriately recorded and tracked. If the IR plan is not required, an incident is just documented and closed throughout this step.

6.2.2. Resist

The resist step's goal is to confirm the incident, implement appropriate containment measures, determine the cause, and escalate, as necessary. The IR team leader is responsible for working with the first reporting team and collecting the appropriate evidence because the incident source can come from various sources. Following the discovery of the incident, the team's focus switches to fixing the vulnerability that caused the incident. During the Resist phase, the following procedures are conducted:

- Validate the Incident Occurrence: This step is completed to ensure the incident reported is from a reliable source. The team decides whether there are sufficient details to evaluate the incident. If this data is insufficient, the group will use testing strategies to attempts to recreate the failure.

- Acquire the evidence: Appropriate logs are collected and saved as evidence.

- Confirm the Incident occurrence: Details collected in validating and acquiring evidence steps will help to get a final confirmation about the incident.

- Assess the severity of the occurrence: The severity level of the occurrence is established based on the evidence gathered. Prioritization and issue handling are based on the severity level calculated. Severity levels are described in section 5 of this document.

- Activate the required IR team: Internal stakeholders affected across the organization should be informed, and the responsible personnel should be brought into the team. A product cybersecurity incidence response call sheet is maintained that includes instructions on who to contact, what information to offer, when to contact them, and how to contact them.

- Containment: One of the most essential elements in the Incident Response plan is containment. This prevents the incident effects from spreading throughout the JBM-owned system or causing damage to any JBM products.

- Root cause analysis: The team refers to the analysis to find the root cause if the identified attack was covered in the completed component TARA. If this is not the case, the team starts a new TARA as needed.

- Identify the affected products: The determination of the damaged product line is aided by determining the root cause. This phase is conducted to identify all products that were not included in the initial

report. For any newly recognized products, the containment methods are followed.

- Adjust the severity of the occurrence: Throughout the incident, the severity score is observed and recorded. With the newly discovered details, the team calculates severity. To compute the new risk level, TARA's risk matrix from ISO/SAE 21434:2021 is used. A risk matrix is a representation of the relationship between levels of impact and attack feasibility on certain scales and risk values. To calculate Impact/Attack feasibility levels, refer to the "Threat analysis and Risk assessment procedure."

  (Refer JBM_Threat Analysis and Risk Assessment V1.0a.docx)

- Escalate: Team notifies the leadership group to the situation, describes how severe it is, and asks for assistance. Information on the recently determined severity level with impact data, impacted products, and legal communication guidelines will all be used for leadership evaluation.

6.2.3. Detect/Fix

After the problem has been identified and contained, the team's attention turns to patching the weakness that led to the occurrence. The team works to identify the problem, explore potential solutions, and closely coordinate to manage the field update procedure. The developed mitigation plan includes specific implementation milestone dates as well as a range of solution options. Previous incidents with a similar and the associated activities will be taken into consideration while developing mitigation methods. Potential mitigations are analyzed and tested for efficacy before being pushed onto the product. As part of the detect phase, the following activities are performed:

- Defining corrective action and implementing the remedy: The team collaborates closely with appropriate internal product groups to assess viable solutions to the problem. Before choosing a solution, the responsible system owners are identified and an approval from experts is confirmed.

- Implement and test the solution: The team creates a strategy that includes a time schedule for each step of the solution implementation. There are pre-defined milestones for each step as well. To help align technical and corporate response actions, solution strategy is reviewed accordingly.

- Activate the update process: Appropriate updates are deployed and executed. Logs are collected and tracked.

6.2.4. Respond and Optimize

This step focuses on evaluating the response process to determine whether any improvements are required. JBM incident response team considers the procedures used to document lessons learnt, new threats discovered, and new tool adaptations. The following steps are executed as part of Respond phase:

- Re-evaluate severity matrix: It is critical to reevaluate the severity matrix now that the remedies are in place to determine the risk level with mitigations accordingly.

- Debriefing: JBM conducts a debriefing review to get comments from the members of the Incident Response Team. The evaluation of the feedback is recorded in the tracker as comments or as a separate report. Lessons learned are fed back into the plan changes during the preparation process. Cybersecurity audit is conducted as needed.

- Completion and closing: Before closing the event from the database, logs are captured with the feedback and improvements. Summary and learnings are distributed across the teams.

6.2.5. Severity levels

Incident severity Level 5: An incident of this magnitude has a significant impact on JBM products and may affect a single item, or numerous items. It can lead to the following:

- Unauthorized access or updates, which can lead to safety hazards, including life-threatening injuries.
- The vehicle is inoperable.
    - Access to sensitive/property data from multiple vehicles without authorization
    - Can result in significant financial losses.
        - It is not possible to mitigate the problem with a software update, and a part. replacement is required.
        - Having an impact on the survival of a firm Incident severity Level 4: An incident of this magnitude has a significant impact on JBM products and may affect a single or numerous items. It can lead to the following:
    - Unauthorized access or update resulting in:
        - safety hazards resulting in serious injuries (but not life threatening)
        - Regulatory/compliance difficulties
    - Some vehicle functions are lost.
        - Unauthorized access to sensitive/property data can lead to significant financial losses.
        - Cannot be minimized through software updates, part replacement is required.
        -

Incident severity Level 4: An incident of this magnitude has a limited impact on JBM products and can affect a single or numerous products. It can lead to:

- Unauthorized access or updates, which can lead to:
    - Safety hazards, which can lead to moderate injuries.
    - Regulatory/compliance issues may arise.
- Some vehicle functions are lost.
    - Unauthorized access to sensitive/property data can result in financial losses, but these can be recovered.
    - Software updates can be used to mitigate the problem.

Incident severity Level 3: An incident of this magnitude has a major impact on JBM products and could affect a single or numerous items. It can lead to:

- Unauthorized access or updates, which can lead to:
    - Safety hazards, which can lead to moderate injuries.
    - Regulatory/compliance issues may arise.
- Some vehicle functions are lost.
    - Unauthorized access to sensitive/property data can result in financial losses, but these can be recovered.
    - Software updates can be used to mitigate the problem.

Incident severity Level 2: An incident of this magnitude has a minor impact on JBM products and could affect a single or numerous items. It can lead to:

- Unauthorized access or updates, which can cause the operator inconvenience.
- It can be mitigated with a software update.

Incident severity Level 1/none: JBM products are mostly unaffected by such incidents. However, it can lead to:

- Unauthorized access or updates that cause minor safety, financial, or privacy problems.

7. UPDATES

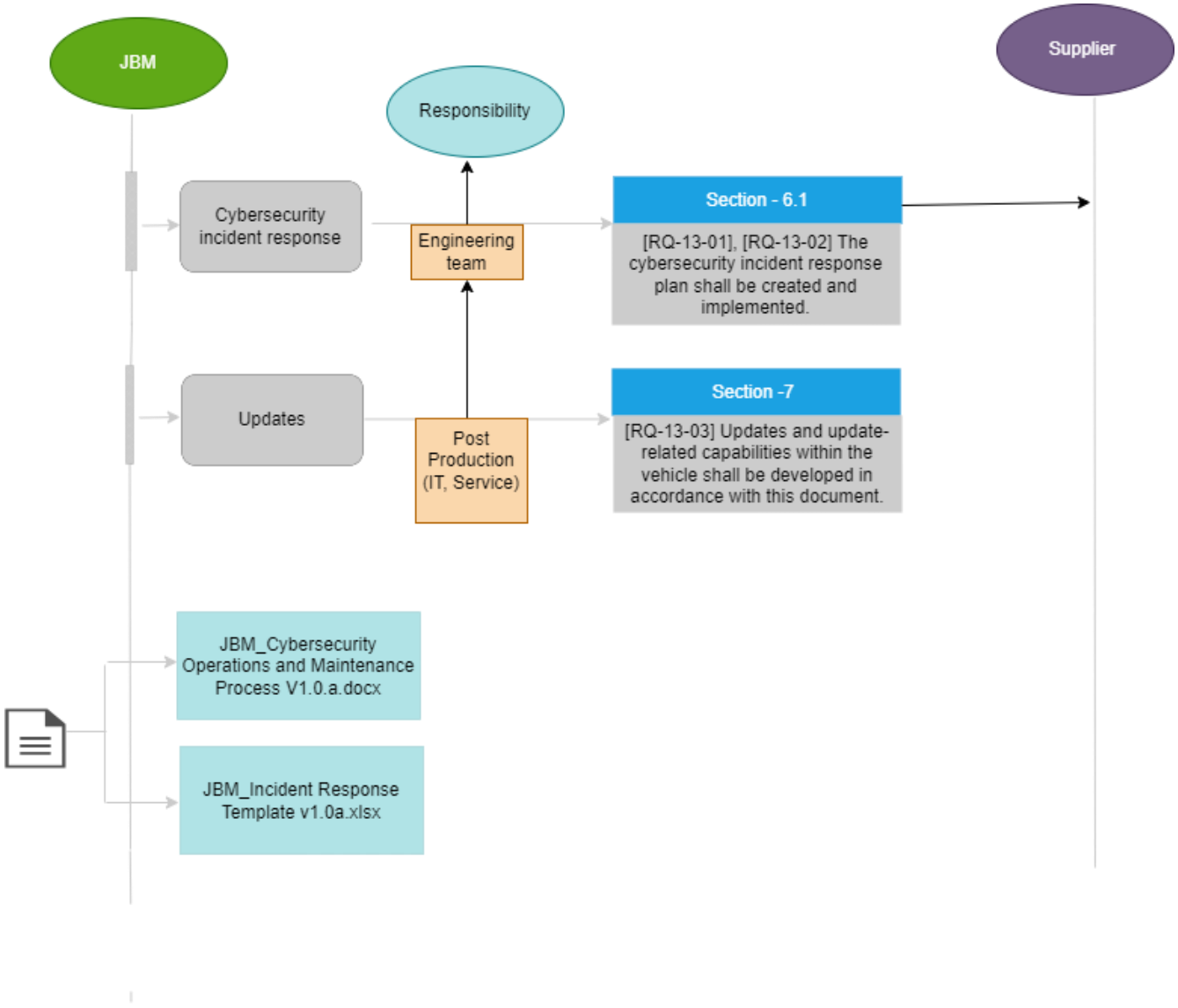
Updates are changes and modifications made to the items or components because of a cybersecurity event as part of operations and maintenance. Throughout the development phase, post-development phase, and up until the end of cybersecurity support for the item/component under consideration, updates are maintained by JBM.

7.1. Inputs

An active JBM post-development report that is currently available is taken into consideration when making updates.

The incident response plan can also be used to keep track of all the information needed for an update that reflects more information or the reasoning behind a certain update.
If necessary, these could also specify changes to the requirements.

8. PROCESS FLOWCHART



9. LIST OF RECORDS

Sr. No.	Record Title	Format No.	Retention Period	Location / custody
1	Incident response template	-	-	-

10. REFERENCE

Sr.No.	Document Descriptions	Document No.
1	Road vehicles — Cybersecurity engineering	ISO/SAE 21434:2021
2	Road vehicles — Software update engineering	ISO 24089
4	Cyber security and cyber security management system	UNR155
5	Cyber Security management systems (CSMS) [M, N and T] category	AIS189
6	Information Security Management System	ISO 27001
7	JBM_Cybersecurity Operations and Maintenance Process V1.0a	

END OF PROCESS