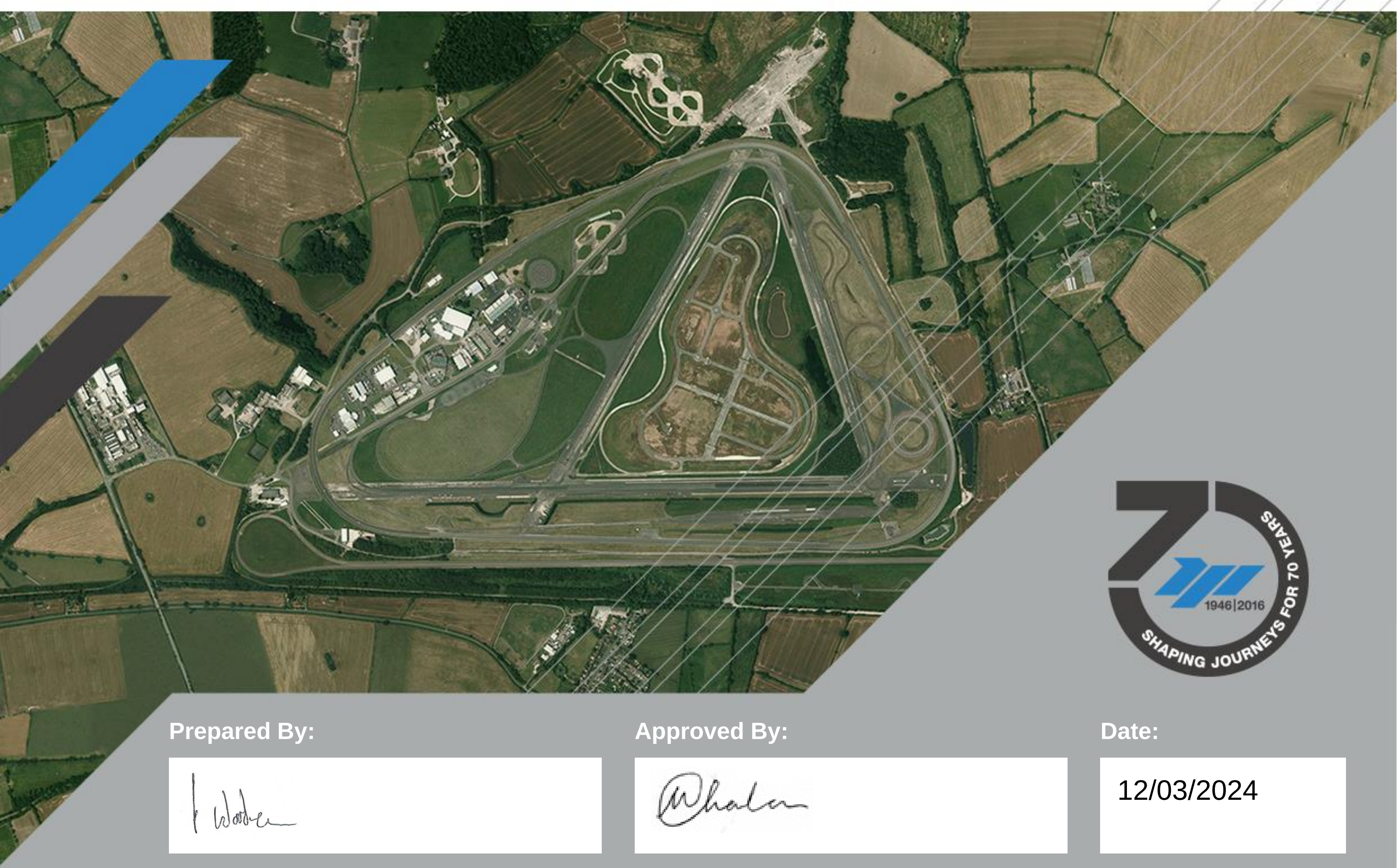
Information:

# ISO/SAE 21434 Cybersecurity Engineering Process Certification

Version 1



| | | |
|---|---|---|
| **Prepared By:** | **Approved By:** | **Date:** |
| | | 12/03/2024 |
| Paul Wooderson<br>Cybersecurity Chief Engineer | Mitesh Chauhan<br>Head of Certification | |

HORIBA MIRA Ltd. Registered Office: Watling Street · Nuneaton · Warwickshire · CV10 0TU · England · www.horiba-mira.com
Tel: +44 (0)24 7635 5000 · Fax: +44 (0)24 7635 8000 Registered in England No 9626352 · VAT Registration GB 100 1464 84

# Revision History

| Date | Revision No. | Raised By | Description |
|---|---|---|---|
| March 2024 | 1 | PW | Initial issue |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# 1 Introduction

For customers seeking certification against the requirements for processes against ISO/SAE 21434 Road vehicles – Cybersecurity engineering, HORIBA MIRA Certification Ltd are a Certification Body for ISO/SAE 21434:

The scope of HORIBA MIRA Certification Ltd (HMCL) activity as a Certification Body includes:

- Cybersecurity Engineering Process (CSEP) Certification – examination and certification of a process to determine if it satisfies ISO/SAE 21434 process requirements

HMCL do not currently offer Cyber Security Product assessment, however we would welcome your enquiry for this service to keep you informed should this become one of our offerings.

This document describes the services offered and an overview of the process that shall be followed.

## 1.1 Terms and definitions

For avoidance of doubt the terms described below are understood as follows in this document

- Audit – examination of a process to determine the extent to which the process objectives are achieved.
- Assessment – not used in this document
- Process – set of interrelated or interacting activities which transforms inputs into outputs
- Certification – the process of earning an official certificate following a review of the process against the prescribed requirements of the standard. Final Report  the work product resulting from a cybersecurity (CSEP) audit according to ISO/SAE 21434 Clause 5.4.7.
- Evaluation – see ISO/IEC 17065 Clause 7.4, the activities of conducting the audit and reviewing its results
- Review – see ISO/IEC 17065 Clause 7.5, the activities of an independent review of the evaluation results to ensure they have been conducted with impartiality and competence
- Certification decision – see ISO/IEC 17065 Clauses 7.6 and 7.7, the activities of making a formal decision on whether or not to issue a certificate, based on the results of the Evaluation and the Review
- Surveillance – a periodic activity to confirm that the basis of making the certification decision remains valid

# 2 Contract Review

Following an initial customer enquiry, HORIBA MIRA Certification Ltd will request for the customer to populate an application form. This will help to determine the customer requirements and ensure that their request is within our scope.

The application will be reviewed, and a quotation/proposal will then be issued to the customer clearly indicating the evaluation that will be conducted in accordance with ISO/SAE 21434.

Upon return of a signed quotation/proposal and a purchase order, the Technical Manager of HORIBA MIRA Certification Ltd shall appoint a technical member of HORIBA MIRA Certification Ltd to complete the required evaluation activities.

The activities could consider Certification against existing audits completed by HORIBA MIRA, however a review would still need to be completed to determine whether they have captured all elements and are suitable. If no audit has been completed, then HORIBA MIRA Certification Ltd will need to complete these audits prior to a Certification decision.

For ISO/SAE 21434 audits that are completed by HORIBA MIRA VRES Team and certification is required, a separate quotation/proposal will always be issued by HORIBA MIRA Certification Ltd and will consider the audit completed however it does not guarantee compliance.

**Customers should request for certification from the outset to reduce the risk of completing an audit and then requiring further assessments of the audits completed.**

# 3 Cybersecurity Process Certification

## 3.1 General

The Process Audit is the procedure whereby a Certification Body ascertains and certifies that a representative system of work satisfies the requirements of the appropriate provision within ISO/SAE 21434.

The process for Certification typically involves an initial desk-based review of the process being examined and an audit visit. The exact requirements are dependent upon whether the organisation has been audited by HORIBA MIRA and is now seeking Certification or whether they also require full audits to be completed.

Where an audit/certification is requested from the outset, HORIBA MIRA Certification Ltd will complete an initial desk-based review followed by an audit to enable a final audit report to be completed. This stage will be defined as the evaluation stage with an initial recommendation on whether certification can be recommended. As required by ISO/IEC 17065, this recommendation is subject to confirmation through a review before a certification decision is made.

If an existing final audit report is available and completed by HORIBA MIRA, this will be evaluated by HORIBA MIRA Certification Ltd to make an initial recommendation on whether this evidence could be used for the purpose of Certification. In instances where elements are missing due to the approach taken, these will need to be assessed. As required by ISO/IEC 17065, any recommendation are subject to confirmation through a further review by an independent resource appointed by HORIBA MIRA Certification Ltd

## 3.2 Application

In the first instance, an application form must be populated. This will define which processes are being requested and what details are required.

If an audit has been completed prior to Certification being requested, the final audit report will need to be provided. This will be reviewed and if required, a further audit may be needed to validate the findings. Competency of the HORIBA Staff that completed the audit will be reviewed.

Competency of the HORIBA Staff that completed the audit will be reviewed.

Where an audit has not been completed by HORIBA MIRA, access to cybersecurity related process, definitions and supporting information implemented will be required.

## 3.3 Process review

The typical process review will consist of the following; however this will be further detailed in the proposal:

- Perform a gap analysis/mapping of existing artefacts and activities into the ISO/SAE 21434 requirements.
- Carry out a desk-based review and completion of the mapping.
- Examine evidence for application of the Cybersecurity Process.
- Complete an audit of the process

- Creating of a final audit report

Audit reports are only considered if they have been completed by HORIBA MIRA or HORIBA MIRA Certification. The staff that completed the audits should have the appropriate competence and expertise in the interpretation and application of the relevant standard. HORIBA MIRA Certification Ltd will in these instances still follow the process outlined above and reserve the right to request for a further audit to be completed to validate the findings should there be any concerns or areas that have not been sufficiently reviewed.

## 3.4 Evaluation and Review

A HORIBA MIRA Certification Ltd Independent Evaluator shall review the overall audit activities, summarised by the Final Audit Report and supporting information, and conclude a recommendation for certification within the Evaluation Report.

Where the audit has been completed by HORIBA MIRA Certification Ltd, the same member of staff will also populate the Evaluation Report.

The recommendation for certification will identify one of the following four outcomes:

- **Certification Recommended**: there are no identified major or minor non-conformities
- **Conditional Acceptance**: subject to the satisfactory resolution by the applicant of identified non-conformities within an agreed and appropriate timescale.
- **Certification Rejected**: the evaluation of the Cybersecurity Final Audit report identifies non-conformities and/or other findings which confirm conformity to ISO/SAE 21434 has not been achieved. Corrective actions are to be performed and the evaluation repeated.
- **Evidence Incomplete;** the information provided was not sufficient to conclude a decision. In the case of this outcome, the certification activities cannot proceed further and the evaluation has to be repeated once sufficient evidence is available.

**Note: Conditional acceptance cannot be used as a qualifying outcome for initially issuing a certificate. Conditional acceptance can only be used for the purpose of renewing a certificate, where an agreed timescale is given for closing the identified non-conformities.**

Following the Evaluation, a further independent Review as required by ISO/IEC 17065:2012 Clause 7.5 will be undertaken of the Evaluation report together with the recommendation made to determine whether the overall evaluation is accurate and the reviewer is in agreement with the process evaluated.

Upon their review, they will make one of the following outcomes:

- **Certification Recommended**: there are no identified major or minor non-conformities
- **Conditional Acceptance**: subject to the satisfactory resolution by the applicant of identified non-conformities within an agreed and appropriate timescale
- **Certification Rejected**: the Cybersecurity Evaluation report identifies non-conformities and/or other findings which confirm conformity to ISO/SAE 21434 has not been achieved. Corrective actions are to be performed and the evaluation repeated.

This will then be passed onto the Technical Manager of HORIBA MIRA Certification Ltd for a Certification decision, see Section 6 below.
In instances where the Certification is rejected, a populated report will be sent to the customer and further discussions will occur.

# 4 Competency requirements

All our auditors are suitably qualified and experienced personnel with at least several years experience with cybersecurity/Functional Safety experience in the automotive industry. Auditor competencies are carefully managed to ensure that the requires skills are matched to the specific domain subject matter being assessed. Strict procedural rules are enforced within the business to ensure the auditors have the necessary independence and impartiality.

# 5 Transfer of Certification services

When a customer requests transfer from one Certification Body to another, the process described in section 3 will be applied. An audit by HORIBA MIRA Certification Ltd will still be required due to the complexity of the assessment and unknown technical competency of other organisations that may have completed the audit.

# 6 Certification

Where the HORIBA MIRA Certification Ltd Technical Manager receives a positive recommendation from the Reviewer and a review of the supporting evidence (in the form of the Cybersecurity Evaluation and  Review reports) supports the positive recommendation, the HORIBA MIRA Certification Ltd Technical Manager will issue a uniquely numbered and dated Cybersecurity Process Compliance Certificate

The Cybersecurity Process Compliance Certificate will be sent to the applicant and copies held along with the Technical details provided.

Initial and Recertification Certificates will be valid for a period of 3 years, but subject to surveillance audits, see Section 7 below. HORIBA MIRA Certification Ltd will need to carry out periodic surveillance visits to ensure the applicant continues to fulfil their obligations for compliance.

# 7 Routine Surveillance& Recertification

The Certification Body shall carry out periodic surveillance checks for maintenance of issued certificates. The frequency of the surveillance activity shall be such that surveillance will typically occur every 12 months, but a full re-certification shall be carried out every 3 years.

Specifically, the surveillance activity shall review any changes undertaken against the original evaluation.

A surveillance application will be issued to the applicant every year requesting for details of changes made to the audited process or product. Depending upon the details contained within, a formal surveillance audit/assessment may be completed.

The format of the surveillance activity will follow the same process to that of initial certification, however the level, scope and depth of the evaluation and review may be reduced to focus on any changes made and contain a spot check of areas previously evaluated.

For re-certification, a formal audit/assessment shall be completed even if there are no changes.

There may be a random surveillance visits undertaken and the applicant should ensure they have the required personnel to assist with the audit. In instances where random surveillance visits are required, contact will be establish and a visit will be planned typically within a few days.

# 8 Modification

Where a modification is made to the item/s assessed to a certified process, the applicant must inform the Certification Body of these changes. The HORIBA MIRA Certification Ltd Technical Manager will arrange for the modification to be reviewed and this could be subject to an audit visit and the associated processes result in a surveillance audit.

While it is the responsibility of the customer to notify HORIBA MIRA Certification Limited of these changes, HORIBA MIRA Certification Limited reserves the right to send an annual surveillance application to confirm the product is unchanged.

# 9 Withdrawal of Certificate

If it is necessary to withdraw a Cybersecurity Engineering Process Compliance Certificate then HORIBA MIRA Certification Ltd will inform the applicant of the reasons for the withdrawal.

A copy of the withdrawal letter and any associated documentation shall be retained with the certificate.

# 10 Fees

All Certification decisions will be made by HORIBA MIRA Certification Ltd (07530871), here on after referred to as HORIBA MIRA Certification – A separate legal entity of HORIBA MIRA Ltd. The organisation is supported financially through the income of Certification Body activities and is not reliant on the number of audits completed.

Impartiality of staff undertaking the evaluation, review and certification decision is guaranteed and their remuneration does not depend on the number of audits and approvals carried out, nor the results of such audits or approvals.

Fees for the certification and associated activities will depend upon the size of the organisation, the number of audits, locations to audit and can be provided upon request following initial discussions on the customer’s requirements.

# 11 Customers’ requirements/restrictions

Prior to any work being completed, HORIBA MIRA Certification Ltd will issue a proposal/quotation which will detail the deliverables and task to be undertaken. Each proposal/quotation details a series of ISO/IEC 17065 requirements that will need to be agreed by the customer. This includes the use of the certification body's name and certification mark and on the ways of referring to the certification granted.

# 12 Complaints

Should for any reason, the service offered under the quotation/procedure provided is deemed by the client to be unsatisfactory and it cannot be resolved through discussion with the Head of Certification directly (contactable via Certification@horiba-mira.com), an official compliant can be raised by sending an email describing the issue to Enquiries@horiba-mira.com. The same process applies to appeals.

The complaint/appeal will be logged and reported to customer services and processed through our internal systems. This will result in actions being allocated to appropriate management and where necessary a full review will take place before a formal response is made to the customer. The customer shall be given 28 days in which to respond to the formal response before the item is closed internally.