MARQUARDT
CYBERSECURITY POLICY

We develop cybersecurity related products for our customers. These must comply with international standards for cybersecurity according to ISO 21434. If specialized cybersecurity standards exist then these need to be taken into account, i.e. UNECE-Regulations for Automotive Cybersecurity or SAE (Society of Automotive Engineers). Our top objective is to fulfill the requirements of these standards.

According to the defined cybersecurity requirements, certain measures, methods, principles must be considered and carried out in compliance with standards from technical point of view, as well as from process view for the respective product during the cybersecurity lifecycle.

To guarantee this we implement the following responsibilities for the Marquardt Group:

1. In projects:

The respective development departments take the responsibility for the implementation of the requirements of the respective product sufficient practice in relation to the applicable standard. The resulting measures are set out in the Cybersecurity Plan and further technical documents.

The Central Quality Management implements the role of the Cybersecurity Quality Manager (CSQM) as an independent administrative department with overall responsibility for cybersecurity. This includes:

- Responsibility for independent confirmation activities within the projects (e.g. Audit, Assessment, Completeness).
- Creation and continuous improvement of the process for cybersecurity.
- Supervision of information in regard to cybersecurity products in the field.

The Development Department implements the role of the Cybersecurity Engineer (CSE) which defines and supervises measures for cybersecurity within the project. This includes in particular:

- Responsibility for fulfillment of the cybersecurity life-cycle (e.g. tailoring of process, set up technical cybersecurity concept, selection and implementation of cybersecurity analyses ...)

In the context of tailoring, at the project start it will be decided, depending upon characteristic of the project, and under certain circumstances together with the customer, which procedures and measures need to be implemented in the project.

The CSQM has complete authority as well as the right to veto all decisions which concern cybersecurity. The CSE has direct reporting and escalation authority to the CSQM.

The heads of the Development Department and the Central Quality Management accompanied by the CSQM provide series-production approvals for cybersecurity related systems or restricted releases for intermediate release-levels.

2. In the Development Process:

The Development Departments ensure, in the context of the process definition and improvement, and thus in cooperation with the Central Quality Management, that the implemented procedures and measures are further developed to guarantee the completeness and efficiency of the cybersecurity process.

The CSQM is responsible for the definition and development of the cybersecurity process within the Marquardt Group.

MARQUARDT
CYBERSECURITY POLICY

3. **Regarding the Implementation:**

   The CSE ensures that the project specific cybersecurity goals are comprehensibly anchored within the general targets of the project. The development departments qualify all project staff in cybersecurity related projects on the ability to implement the agreed measures in the project work effectively.

4. **Regarding Monitoring and Escalation:**

   The CSQM presents the status of cybersecurity to the Management of the Marquardt Group regularly, with reports about progress and deviations with appropriate measures for cybersecurity within the project.

5. Incident Response Management is managed globally by the Cooperated Information Security Officer (CISO), the Cybersecurity Manager (CSM) and the Cybersecurity Quality Manager (CSQM).

Together with the CSQM, the heads of the Development Department and the Central Quality Management check the implementation of this guideline regularly and present the status to the Management of Marquardt Group.

The Management
Rietheim-Weilheim, January 2022