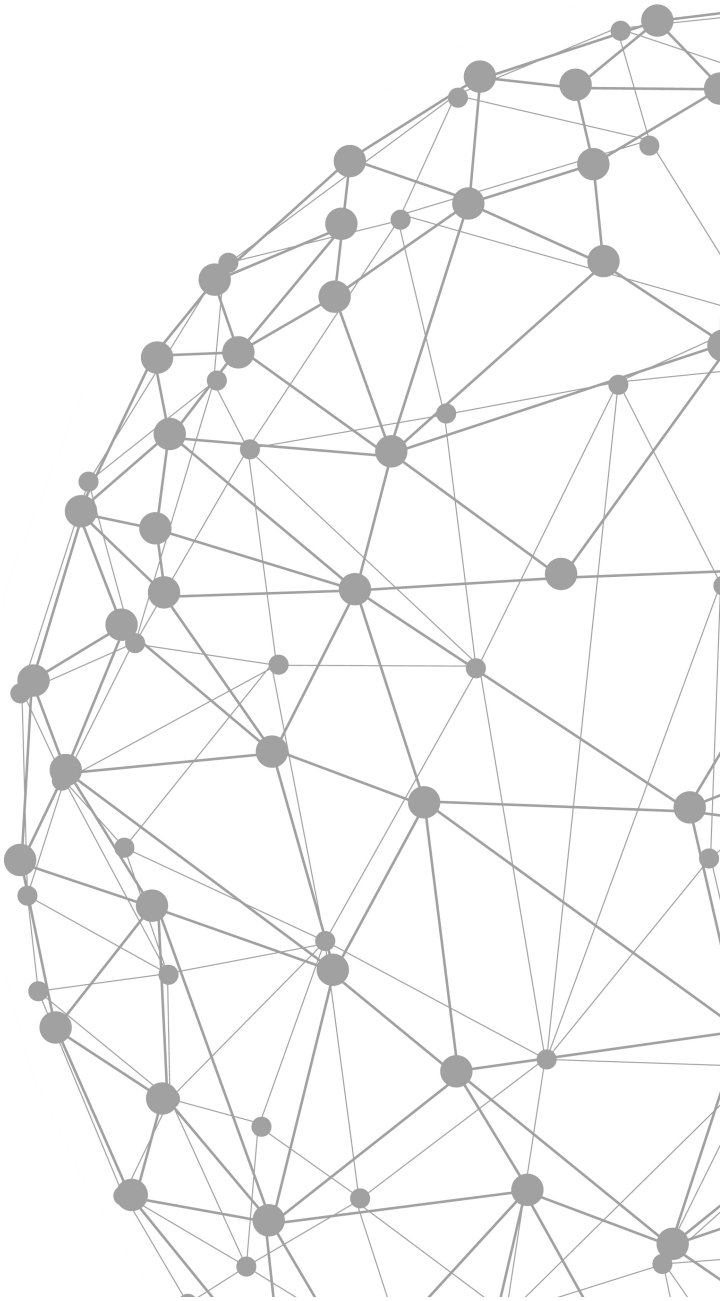
Creating safety.
With passion.

NewTec

Security Assessment Approach and Attestation Process

Doc.-Number: 11001_0099_0009_MKT092TE_PAP-Security-Assessment-Approach-and-Attestation-Process
Doc.-Version: A1



Author:
Matthias Lai
NewTec GmbH

Change History

Doc.-Version	Date	Author	Description of Modification
A1	2025-07-28	Matthias Lai	Initial Release

Release

	Name	Responsibility	Date	Signature
Creation	Matthias Lai	PM	2025-07-28	Release via SVN
Verification	Michel Junghäni	CSM	2025-07-28	Release via SVN
Approval	Stephan Strohmeier	Active CSM	2025-07-28	Release via SVN
Release	Benjamin Bisser	QS	2025-07-28	Release via SVN

Table of Contents

1 Purpose of the Document

With the increasing integration of information technology (IT) into all areas of life – especially in the domains of embedded components and the systems that incorporate them – the importance of security continues to grow. This development is driven not only by the digitalization of industrial environments and safety-critical systems, but also by the emergence of specific and sophisticated attack vectors targeting embedded components and the systems that incorporate them. These include threats to firmware, communication interfaces, fieldbus protocols, and vulnerabilities in the supply chain.

Customers and partners—as well as **regulatory authorities (e.g., FDA, EU Notified Bodies)**—are placing increasing demands on the transparency and verifiability of product and service security. In response, NewTec GmbH conducts structured, context-aware security assessments and issues security assessment certificates confirming that, based on the defined scope and applied methods, no critical vulnerabilities were identified.

This document outlines the principles and procedures that NewTec applies in such assessments and describes the content and structure of the resulting security assessment report.

2 NewTec Security Certificate – Statement of Purpose

NewTec GmbH issues a **Security Certificate** upon the successful completion of a structured security assessment. This certificate confirms that the **Product Under Consideration (PUC)** has been evaluated in accordance with NewTec's established security assessment methodology and that **no critical vulnerabilities were identified** during the evaluation.

The Security Certificate serves the following purposes:

- **Formal Assurance**: It provides formal assurance regarding the PUC's security posture to customers, partners, and **regulatory authorities** (e.g., **FDA**, **EU Notified Bodies**) as part of compliance and product approval processes.
- **Independent Evaluation**: It demonstrates that an impartial and systematic security assessment has been conducted by NewTec.
- **Transparency and Traceability**: It supports accountability and clarity within the PUC's security lifecycle by documenting scope, methodology, and findings in a concise, accessible format.

NewTec's methodology, while distinct from formal accreditation schemes, is based on international standards (such as IEC 62443, ISO/IEC 21434, and IEC 81001-5-1) and incorporates best practices for threat modeling, risk assessment, testing, and analysis.

The security certificate is supported by a detailed **technical report** ("Testat"), which provides:

- A structured summary of the security posture of the PUC
- Concrete insights into identified risks, attack paths, and protective mechanisms
- Actionable recommendations for improving the system's resilience

This makes the certificate and technical report highly useful in:

- Supporting internal development processes
- Demonstrating security due diligence to customers or partners
- Preparing for later formal certifications

3 Fundamental Approach

NewTec's Security Assessment methodology is rooted in the belief that reliable security assessments require realistic, application-oriented testing by an independent, technically competent entity. The goal is not only to detect vulnerabilities but also to clearly communicate the security properties of a system or product in a way that supports risk-informed decisions.

NewTec assessments are:

- Context-driven: tailored to the specific environment and use case
- Risk-based: guided by realistic threat models and potential impact
- Standards-aligned: inspired by IEC 62443, ISO/IEC 21434, and IEC 81001-5-1

The assessment aims to deliver practical insight into whether a product shows security-critical weaknesses in its intended context of use.

4 Scope and Evaluation Principles

NewTec evaluations are based on fundamental security objectives that also contribute to safety through security:

- **Confidentiality**: Ensuring data is only accessible to authorized parties
- **Integrity**: Protecting the accuracy and completeness of information
- **Availability**: Ensuring timely and reliable access to systems and data
- **Authenticity**: Verifying the origin and integrity of data and components

These objectives form the foundation for secure system behavior and indirectly support functional safety by reducing the likelihood of security-induced safety failures.

Evaluation Authority

All evaluations are performed by NewTec GmbH's Security Assessment Team. The team is independent of the product development organization and adheres to internal quality and confidentiality guidelines.

Product Under Consideration (PUC)

The PUC defines the exact scope of the assessment. The resulting certificate applies only to the specific version and configuration submitted for evaluation. Significant modifications to the PUC may necessitate a re-assessment.

Evaluation Principles

Each assessment adheres to the principle of proportionality: the depth of analysis must match the risk level and application context of the PUC. The evaluation:

- Verifies the presence and robustness of relevant security functions
- Tests whether these functions behave correctly under realistic conditions
- Investigates whether they offer effective protection in the PUC's environment

Evaluation Depth

The evaluation typically includes:

- Architecture and interface review
- Threat modeling and risk analysis
- Vulnerability scanning and exploit attempts

- White-box and/or black-box testing

The specific methods and depth are agreed upon with the customer in advance and documented in the test plan.

Result Dissemination

NewTec issues a **certificate** upon successful completion of the evaluation. A **technical test report (Testat)** will be shared, detailing vulnerabilities found (if any), risk context, and suggested mitigations. The customer controls the confidentiality level of the report.

5 Security Assessment Process

The security assessment follows a structured, multi-phase approach that is aligned with established standards such as IEC 81001-5-1 AD01_IEC62443-4-1 and ISO/IEC 21434. The objective is to identify potential vulnerabilities in the product, understand their context, and derive appropriate mitigation measures.

The following activities were carried out:

1. **Vulnerability Analysis**
   In this phase, all relevant technical and contextual information about the product under consideration is collected and documented. This includes product details, architecture, communication interfaces, and publicly available information. Based on this data, known vulnerabilities/weaknesses from sources such as CVE databases or scientific publications are identified. Additionally, all identified assets are mapped to applicable use cases. Unlinked assets are critically reviewed and, if applicable, marked as potential attack surfaces.
2. **Assessment of Attack Potential (Part of the Vulnerability Analysis)**
   As part of the vulnerability analysis, the attack potential is evaluated. The evlauation is done based the attack potential approach defined in ISO/IEC 18045. This method is widely adopted in different industries such as automotive cybersecurity (e.g., ISO/SAE 21434) and relies on five core parameters:
   - Elapsed time (time required to execute the attack),
   - Specialist expertise (attacker's skill level),
   - Knowledge of the system (familiarity with the target),
   - Window of opportunity (availability of access to the system), and
   - Equipment (tools/resources needed)

   This evaluation helps to realistically assess the criticality of a vulnerability in the system context and serves as the basis for defining the depth of subsequent test phases.
3. **Vulnerability Testing**
   In a practical test phase, further findings are uncovered through technical testing. The goal is to identify possible weaknesses and vulnerabilites that were not identified during the analysis. Various testing methods may be used (white/grey/black box), depending on the available information and system access.
4. **Attack Path Analysis**
   Based on the prior analysis, potential attack paths are documented to assess the exploitability of identified findings. These paths model realistic scenarios in which an attacker could compromise critical assets or functions, accounting for:
   - Intermediate steps (e.g., lateral movement, privilege escalation), and
   - Dependencies (e.g., system interactions, prerequisites for exploitation).

   This analysis supports rating of findings and the definition of mitigation strategies.

5. **Penetration Testing**
   In this phase, identified vulnerabilities are actively exploited to verify their exploitability. The goal is to obtain a realistic assessment of what an attacker could achieve by exploiting a given vulnerability—such as data theft, manipulation, or system control
6. **Documentation and Evaluation**
   All findings are documented, evaluated, and linked to the relevant use cases and assets. This evaluation forms the basis for deriving concrete recommendations for risk mitigation.

5.1 Findings

During the assessment, all identified findings were systematically evaluated and classified as follows:

1. **Vulnerability**
   Confirmed exploitable flaws where a threat scenario could be realized.
2. **Weakness**
   Applicable findings that lack a practical attack vector but indicate structural or procedural deficiencies. These may elevate risk if combined with other factors.
3. **Note**
   Observations that do not pose an immediate risk but represent best-practice deviations, minor improvements, or informational insights.
4. **Not Applicable**
   Findings not relevant to the target system's environment, configuration, or scope were documented here for transparency.