Security Incident & Vulnerability Report

Version 1.0 09/2026

NBB Controls + Components GmbH
Otto-Hahn-Straße 3 – 5 · 75248 Ölbronn-Dürrn · GERMANY · T: +49 7237 999-0 · F: +49 7237 999-199 · info@nbb.de · www.nbbcontrols.com
Registergericht Mannheim HRB 500961 · Geschäftsführer: Dipl.-Ing. Thomas Burchard, Dipl.-Wirtschafts-Ing. (FH) / MBA Pierre Augstein

Cybersecurity Incident and Vulnerability Report Form

Urgent cases:
Please send the completed form to **security@nbb.de**. If there is an immediate danger to people or equipment, place the equipment in a safe state in accordance with the applicable operating and safety instructions. This form does not replace emergency measures.

Internal case number	
Date / time received	

Purpose of the form

This form enables customers, operators, integrators, security researchers, and other external parties to submit structured reports of suspected or confirmed cybersecurity vulnerabilities and security incidents related to products from NBB Controls + Components GmbH (NBB).

Security notice:
Do not submit passwords, private keys, access tokens, or other secrets. Do not send potentially harmful, confidential, or large files by email without prior arrangement; first describe them and agree on a secure transfer method with **security@nbb.de.**

Note: This form supports structured data collection and internal CRA assessment.
NBB will determine whether a statutory reporting obligation applies in the specific case.

1. Reporting person details

Name / contact person	
Company / organization	
Role / department	
Email address	
Telephone number	
Country	

Role of the reporting person:

☐ Customer / operator
☐ Dealer / distributor
☐ System integrator / service partner
☐ Security researcher
☐ Authority / CSIRT
☐ Other: _____

Preferred contact method:

☐ Email
☐ Telephone

2. Report type and urgency

Report type (select all that apply):

☐ Suspected vulnerability
☐ Confirmed vulnerability
☐ Suspected active exploitation
☐ Confirmed active exploitation
☐ Security incident
☐ Suspicious behavior / anomaly
☐ Security issue in configuration / documentation
☐ Others: _____

Urgency assessed by the reporting person:

☐ Critical
☐ High
☐ Medium
☐ Low
☐ Unknown

Reason for urgency:

In particular, describe any ongoing attacks, immediate hazards, or widespread impact.

3. Affected product

Product type (select all that apply):

☐ Transmitter ☐ Receiver

☐ Accessory ☐ Configuration or service tool

☐ Firmware / Software ☐ Others: _____

Product name / type		
Part number		
Serial number(s)		
Hardware version		
Firmware version		
Software / tool version		
Configuration status / project file		

4. Affected installation and operating environment

End customer / operator	
Location / country	
Number of affected products	
Commissioning date	

Operating status:

☐ Currently in operation ☐ Out of operation

☐ Disconnected from network / system ☐ Unknown

Operating context:

☐ Industrial machine / installation ☐ Mobile machine / vehicle

☐ Crane / lifting equipment ☐ Other application: _____

Description of the system environment:

Connected systems, networks, interfaces, relevant components, and operating conditions.

5. Timeline and discovery

Date / time discovered	
First known occurrence	
Time zone	
Method of discovery	

Chronological sequence:
Known events, observations, and actions in chronological order, including dates and times.

6. Description of the incident or vulnerability

Brief description:

Detailed description:
What happened? What behavior was expected, and what behavior was actually observed?

Affected functions / components:
For example, radio communication, CAN, authentication, updates, configuration, diagnostics, or a protection function.

7. Observed or potential impact

Security objectives / functions:

☐ Availability affected
☐ Integrity affected
☐ Confidentiality affected
☐ Authenticity affected
☐ Malware suspected / confirmed
☐ Unauthorized access suspected / confirmed
☐ Safety or protection function affected
☐ No impact identified
☐ Unknown
☐ Others: _____

Scope:

☐ One product
☐ Multiple products at one site
☐ Multiple sites / customers
☐ Scope unknown

Description of actual or potential impact:
Affected data, functions, operational interruptions, and potential risks to people, property, or the environment.

8. Evidence of active exploitation

Is there evidence of active exploitation?

☐ Yes, confirmed
☐ Yes, suspected
☐ No
☐ Unknown

Indicators / rationale:
For example, unusual access, manipulation, malicious code, recurring patterns, or external reports.

Known affected organizations / systems	
Known public disclosure?	
Source / reference / CVE	

9. Technical information

Possible access or attack vector:

☐ Radio connection
☐ Ethernet / network
☐ Service / debug interface
☐ Update mechanism
☐ Physical access
☐ Others: _____
☐ CAN / fieldbus
☐ USB / local connection
☐ Configuration / project file
☐ Supply chain / third-party component
☐ Unknown

Technical symptoms, error codes, and additional information (e.g., trace or log):

Suspected cause or attack method:

Device identifiers, addresses, or relevant timestamps:
Provide only information necessary for the investigation that you are authorized to disclose.

10. Reproducibility

Can the behavior be reproduced?

☐ Yes, reliably ☐ Yes, intermittently ☐ No

☐ Not attempted ☐ Unknown

Prerequisites for reproduction:

Steps to reproduce:

Please number the steps. Do not enter credentials or secrets.

Observed result / success indicator:

11. Actions already taken

☐ Product / equipment taken out of service
☐ Network or system connection disconnected
☐ Credentials changed / revoked
☐ Firmware / software updated
☐ Configuration changed
☐ Product restarted / reset
☐ Product replaced
☐ Evidence preserved / logs created
☐ Customers / operators informed
☐ Authority / CSIRT informed
☐ No action taken
☐ Others: _____

Description of actions and outcome:
Date/time, responsible persons, and observed effect.

Remaining risk or limitation:

12. Evidence and attachments

☐ Screenshots / photos
☐ Log files
☐ Configuration files
☐ Network or radio captures
☐ Video
☐ Diagnostic report
☐ Proof of concept / reproduction script
☐ Other documents

List and brief description of attachments:

Secure transfer
Do not submit unnecessary personal data or secrets. For confidential, large, or potentially harmful attachments, first agree on an appropriate transfer method with **security@nbb.de**.

13. Coordinated disclosure and communication

Disclosure status:

☐ Not yet disclosed ☐ Disclosure planned

☐ Already disclosed ☐ Unknown

Planned / actual date	
Location / reference	

Contact and attribution:

☐ Available for follow-up questions ☐ Contact only through organization

☐ Attribution as the reporting person requested ☐ No public attribution requested

Confidentiality or communication requirements:

14. Declaration and data protection

I confirm that, to the best of my knowledge, the information provided is complete and accurate and that I am authorized to submit the information and attachments provided.

☐ Notice on handling confidential information read

☐ NBB may contact me regarding this report

Place, date	
Name	
Signature	

Submission:
Please send the completed form to **security@nbb.de.**

Recommended subject line:

Security Report - [Product] - [Brief description].

A. For internal processing by NBB only

Internal section:
Not to be completed by the external reporting person. This section supports triage, tracking, and the documented decision regarding reporting and information obligations.

Incident-ID / Ticket	
Owner / Incident Manager	
Reporting channel	
Time awareness was established	
Affected product family / versions	
Linked tickets / CI IDs	

Initial classification:

☐ Vulnerability
☐ Actively exploited vulnerability
☐ Security incident
☐ Serious security incident
☐ Not a cybersecurity case
☐ Assessment pending

Reason for classification:

CRA-reporting obligation reviewed by / on	
24h-target deadline	
72h-target deadline	
Final report / target deadline	
Reporting authority / reference number	

Required internal involvement:

☐ Incident Response / PSIRT
☐ Product Development
☐ Systems Engineering
☐ Safety / Compliance
☐ Quality management
☐ Data protection
☐ Executive management
☐ Communications / sales
☐ Legal review
☐ External partners / suppliers

Immediate actions / containment:

Corrective action and customer communication:

Final decision / Lessons Learned:
