


# Results of the IEC 61508 Proven In Use Assessment

Project:
MPS Flammable Gas Sensor 5.0

Customer:
NevadaNano
1395 Greg Street, Suite 102
Sparks, NV 89431
USA

Contract No.: Q26/03-113
Report No.: NVN 26/03-113 R002
Version V1, Revision R3, August 12, 2026
Paddy Healy and Eric Myers

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.
© All rights reserved.

## Management Summary

The Functional Safety Assessment of the NevadaNano

MPS Flammable Gas Sensor 5.0

development project, performed by *exida* consisted of the following activities:

- *exida* assessed the systematic capability through a detailed analysis of proven-in-use data provided by NevadaNano and the creation of a detailed safety case against the proven-in-use requirements of IEC 61508.
- *exida* reviewed and assessed the random capability through a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed field failure data to ensure that the FMEDA analysis was complete.

**The MPS Flammable Gas Sensor 5.0 satisfies the Proven in Use (PIU) requirements for systematic capability up to SIL 2. However, the sensor itself has not been certified, as the supporting certification evidence (e.g., test results, safety manual, and other certification deliverables) has not been assessed independently. Assessment of these items will be performed as part of the certification of the complete transmitter and sensor system.**

## Table of Contents


Management Summary ..... 2

1 Purpose and Scope ..... 4

1.1 Tools and Methods used for the assessment ..... 4

2 Project Management ..... 5

2.1 *exida* ..... 5

2.2 Roles of the parties involved ..... 5

2.3 Standards / Literature used ..... 5

2.4 Reference documents ..... 5

2.4.1 Documentation provided by Nevada Nano ..... 5

2.4.2 Documentation generated by *exida* ..... 7

2.5 Assessment Approach ..... 7

3 Product Description ..... 9

3.1 Hardware and Software Version Numbers ..... 9

4 IEC 61508 Functional Safety Assessment Scheme ..... 9

4.1 Product Modifications ..... 9

5 Results of the IEC 61508 Proven In Use Assessment ..... 10

5.1 Lifecycle Activities and Fault Avoidance Measures ..... 10

5.1.1 Safety Lifecycle and Functional Safety Management Planning ..... 10

5.1.2 Safety Requirement Specification and System Architecture Design ..... 10

5.1.3 Change and modification management ..... 11

5.1.4 Proven In Use ..... 11

5.2 Software Design and Verification ..... 12

5.3 Safety Validation ..... 13

5.4 Hardware Design and Verification ..... 14

5.4.1 Hardware Architecture Design and Probabilistic Properties ..... 14

5.5 Safety Manual ..... 15

6 Terms and Definitions ..... 16

7 Status of the document ..... 17

7.1 Liability ..... 17

7.2 Version History ..... 17

7.3 Future enhancements ..... 17

7.4 Release signatures ..... 17

# 1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the:

- MPS Flammable Gas Sensor 5.0

by *exida* according to the accredited *exida* certification scheme which includes the requirements of IEC 61508:2010.

The purpose of the assessment was to evaluate the compliance of:

- the technical requirements of IEC 61508 parts 2 and 3 for SIL 2 and the derived product safety property requirements;

and

- the MPS Flammable Gas Sensor 5.0 development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial requirements of IEC 61508 parts 1, 2 and 3 for SIL 2;

and

- the MPS Flammable Gas Sensor 5.0 hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

The assessment has been performed based on the quality procedures and scope definitions of *exida*.

The results of this assessment provide the safety instrumentation engineer with the required failure data per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

## 1.1 Tools and Methods used for the assessment

This assessment was performed by using the *exida* Safety Case tool. The Safety Case tool contains the accredited *exida* certification scheme which includes all the relevant requirements of IEC 61508.

For the fulfillment of the objectives, expectations are defined which builds the acceptance level for the assessment. The expectations are reviewed to verify that each single requirement is covered. Because of this methodology, comparable assessments in multiple projects with different assessors are achieved. The arguments for the positive judgment of the assessor are documented within this tool and summarized within this report.

All assessment steps were continuously documented by *exida* (see [R1])

# 2 Project Management

## 2.1 *exida*

*exida* is one of the world's leading accredited Certification Bodies and knowledge companies, specializing in automation system safety and availability with over 500 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment based on 350 billion hours of field failure data.

## 2.2 Roles of the parties involved

| | |
|---|---|
| NevadaNano | Manufacturer of the MPS Flammable Gas Sensor 5.0 |
| *exida* | Performed the hardware assessment [R3] |
| *exida* | Performed the Functional Safety Assessment [R1] per the accredited *exida* certification scheme. |

NevadaNano contracted *exida* with the IEC 61508 Proven In Use Assessment of the above mentioned devices.

## 2.3 Standards / Literature used

The services delivered by *exida* were performed based on the following standards / literature.

| | | |
|---|---|---|
| [N1] | IEC 61508:2010 (Parts 1 – 3): | Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Normative Parts |
| [N2] | IEC 61508:2010 (Parts 4 – 7): | Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Informative Parts |

## 2.4 Reference documents

### 2.4.1 Documentation provided by NevadaNano

| Doc ID | Customer Reference | Rev | Date | Description |
|---|---|---|---|---|
| [D1] | QA-PL-0001-08 | Rev 8 | 15-Jul-2024 | Business Quality Management System Manual |
| [D2] | MPS – Configuration Management Plan | Rev 1f | 28-Jan-2024 | Configuration Management Plan |
| [D3] | QA-FM-0033-02 | None | None | RMA Request Form |
| [D4] | QA-OP-001 | Rev 04 | None | Document Control Procedure |
| [D5] | Flam 5.0.0.0 Jira Report | None | 07-Mar-2024 | Corrective Action Tracking |
| [D6] | Shipments and Returns E-mail | None | 26-Jun-2026 | Shipments and Returns |

| Doc ID | Customer Reference | Rev | Date | Description |
|---|---|---|---|---|
| [D7] | ISO 9001:2015, Registration 19.8213 | None | Exp. 16-Jul-2028 | ISO 9001:2015 |
| [D8] | MPS - Product Requirements Specification | Rev 1e | 14-Feb-2024 | Product Requirements Specification |
| [D9] | MPS - Software Requirements Specification | Rev 1n | 15-Feb-2024 | Software Requirements Specification |
| [D10] | MPS - FRS to Design Traceability Matrix | Rev 1o | 17-Feb-2024 | FRS to Design Traceability Matrix |
| [D11] | MPS – Architecture and Design Specification | Rev 3.2 | 29-May-2024 | System Architecture Design Specification |
| [D12] | MPS - Software Development Process | Rev 1e | 15-Oct-2025 | Software Development Process |
| [D13] | Project Overview | None | None | 628MP-F31NN Project Overview |
| [D14] | MPS – Source Code Review | Rev 1h | 29-Jan-2024 | Code Review |
| [D15] | QA-FM-0002-03 | None | None | Change Request Form |
| [D16] | MPS – Coding Standard | Rev 1d | 23-Jan-2024 | Coding Standard |
| [D17] | MPS – Software Analysis | Rev 1e | 7-Mar-2024 | Static Code Analysis |
| [D18] | MPS – Test Cases | Rev 1o | 17-Feb-2024 | Integration Test Plan |
| [D19] | MPS – Test Cases Report | Rev 1g | 27-Jun-2024 | Integration Test Results |
| [D20] | MPS – Software Validation Plan | Rev 1f | 16-Feb-2024 | Software Validation Plan |
| [D21] | Environmental Robustness Test Plan | Rev 06 | 01-Dec-2023 | Environmental Test Plan |
| [D22] | SM-UM-0010-09 | N/A | 27-Apr-2026 | MPS Flammable Gas Sensor 5.0 User Manual |
| [D23] | SM-DS-0012-11 | N/A | 27-Apr-2026 | MPS Flammable Gas Sensor 5.0 Data Sheet |
| [D24] | MPS – Tool Analysis Report | Rev 1i | 15-Oct-2023 | Tool Qualification Report |
| [D25] | MPS – Impact Analysis | Rev 1e | 31-Oct-2024 | Impact Analysis Record |
| [D26] | SM-RN-0005-01 | None | None | SW Release Notes (5.0.0.0) |
| [D27] | Flam5.0.0.0.Alpha-GA | V8 | 22-Jun-2024 | Firmware & Chemometrics |

### 2.4.2 Documentation generated by *exida*

| | | |
|---|---|---|
| [R1] | NVN Q26-03-113 W001 V1R1 MPS 5_0 Sensor SafetyCase | SafetyCase file for MPS Flammable Gas Sensor 5.0 |
| [R2] | NVN Q26-03-113 W002 R2 MPS 5_0 Sensor FFA | Field Failure Analysis for MPS Flammable Gas Sensor 5.0 |
| [R3] | NVN Q26-03-113 R002 V1R2 MPS 5_0 Sensor PIU Assessment Report | IEC 61508 Functional Safety PIU Assessment for MPS Flammable Gas Sensor 5.0 (This document) |
| [R4] | NeN 628MP-F31 V1R2.OEMx | FMEDA for MPS Flammable Gas Sensor 5.0 |

## 2.5 Assessment Approach

The proven-in-use audit was closely driven by requirements of the accredited *exida* certification scheme which includes subsets filtered from IEC 61508. The assessment was planned by *exida* and agreed with NevadaNano.

For designs that have been in service for several years and have demonstrated themselves in a variety of applications and conditions, consideration of a proven in use assessment may be used as a substitute if a product didn't follow a fully compliant IEC 61508 design process. The partial functional safety assessment includes an assessment of all fault avoidance and fault control measures during any hardware and software modifications needed to achieve SIL 2 capability for the MPS Flammable Gas Sensor 5.0. Other product development aspects prior to these modifications were assessed according to Proven-In-Use (PIU) requirements (see section 5.1.5).

The assessment considers the SIL 2 Proven In Use requirements of IEC 61508. Any requirements that have been deemed not applicable have been marked as such in the full Safety Case report, e.g. software development requirements for a product with no software.

As part of the IEC 61508 functional safety assessment for the MPS Flammable Gas Sensor 5.0, the following evidence aspects have been reviewed:

- FMEDA
- SRS or product specification
- Instruction manual
- PIU data collection procedures and operational excellence calculation/report (evidence that the equipment is proven-in-use; analysis of field failure rates to ensure that no systematic faults exist in the product)

No ASICs are used in this product and No safety related communications are used in this product.

Proven-In-Use (PIU) assessment provides for the prevention of systematic failures for pre-existing devices with a proven history of successful operation. As part of the PIU assessment for the MPS Flammable Gas Sensor 5.0, a number of IEC 61508 functional safety assessment requirements are satisfied without further documented evidence:

- FSM Plan
- Validation test plan
- Development process

Note that validation test plans, system architecture designs, and integration test plans must be assessed at the device + sensor level.

The project teams, not individuals, were audited.

# 3 Product Description

Molecular Property Spectrometer™(MPS™) Flammable Gas Sensor 5.0 is a multi-Gas sensor with a real-time k-factor multiplier. It will default to the safe state if Gas detection is compromised for an extended period but will alert that measurements are diminished. The MPS carries out a self-check every 2 seconds, any failures or status alerts are communicated. The MPS uses a digital output or a customized analog output.

## 3.1 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of MPS Flammable Gas Sensor 5.0:

| MPS Flammable Gas Sensor 5.0: | |
|---|---|
| Hardware | MPSF02 |
| Software/Firmware | 5.0.0.0.GA |

# 4 IEC 61508 Functional Safety Assessment Scheme

The assessment was executed using the accredited *exida* certification scheme which includes subsets of the IEC 61508 requirements tailored to the work scope of the development team. The assessment was performed based on the information received from NevadaNano [section 2.4.1] and is documented in the safety case [R1].

## 4.1 Product Modifications

The modification process has not yet been assessed and audited as part of this assessment, so modifications are not currently covered by this assessment. No modifications are permitted to the assessed versions of the MPS Flammable Gas Sensor 5.0 without reassessment.

# 5 Results of the IEC 61508 Proven In Use Assessment

*exida* assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) [R4] of the MPS Flammable Gas Sensor 5.0 to document the hardware architecture and failure behavior. The FMEDA [R4] and the Safety Case [R1] created for the S4 MPS 5.0 documents this assessment.

*exida* assessed failure history of the MPS Flammable Gas Sensor 5.0 [D030] and performed a detailed analysis of the data provided [R2]. This PIU assessment is done in place of a detailed functional safety assessment for systematic failures. The Safety Case created for the S4 MPS 5.0 documents this assessment.

## 5.1 Lifecycle Activities and Fault Avoidance Measures

This functional safety assessment evaluated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the product development. The assessment was executed using subsets of the IEC 61508 requirements tailored to the SIL 2 work scope of the development team and supported by PIU analysis.

### 5.1.1 Safety Lifecycle and Functional Safety Management Planning

**Assessment**

FSM Plan

A Business Quality Management Plan [D1] exists to document key areas of functional safety management (Page 5) and act as guidance for future modifications. It identifies the responsibilities of personnel, key safety activities and measures to be used, and software tools.

Documentation and Version Control

All documents are under version control as required by [D1] and [D4]. A documented procedure exists to ensure that only approved items are delivered to customers. Master copies of the software and all associated documentation are kept during the operational lifetime of the released software.

**Conclusion**

The objectives of the standard are fulfilled by the NevadaNano internal management system, internal organizational procedures, product change management processes, and safety lifecycle processes and supported by PIU analysis. This can be used as supporting evidence when the MPS 5.0 is integrated into the final SIS.

### 5.1.2 Safety Requirement Specification and System Architecture Design

**Objectives**

- Specify the requirements for each E/E/PE system, in terms of the required safety functions and the required safety integrity, in order to achieve the required functional safety.
- Specify the system architecture design.
- Specify traceability for safety requirements

**Assessment**

Nevada Nano has Product [D8] and Software Safety [D9] requirements. The throughput and response time performance of the safety function is documented. The flowchart in section 2.1.4 of [D22] indicates the fault annunciation and fault response time. Diagnostic Test Interval is specified. This is the worst-case time that it will take for the diagnostics to detect a dangerous failure, and it is approximately 5 seconds. Specific requirements for start-up and restart procedures are specified. The product only has one mode of operation.

**Conclusion**

The objectives of the standard are fulfilled by the NevadaNano functional safety management system and use of requirements management tools (JIRA and Confluence) and supported by PIU analysis. This can be used as supporting evidence when the MPS 5.0 is integrated into the final SIS.

### 5.1.3 Change and modification management

**Objectives**

- Ensure that the required safety integrity is maintained after corrections, enhancements or adaptations to the E/E/PE safety-related systems.

**Assessment**

No modifications are permitted to the certified versions of the MPS Flammable Gas Sensor 5.0 without reassessment.

### 5.1.4 Proven In Use

In addition to the Design Fault avoidance techniques listed above, a Proven in Use evaluation was performed on the MPS Flammable Gas Sensor 5.0. Shipment records were used to determine that the MPS Flammable Gas Sensor 5.0 has greater than 23 million operating hours and has demonstrated a field failure rate less than the predicted failure rates indicated in the FMEDA reports. All components considered in the FMEDA are standard components with greater than 400 billion operating hours, and diagnostic coverage is shown to be greater than 60% (see [R4]). This provides justification for using a Route 2H approach. The exida PIU analysis workbook shows that the failure rate based on field returns within the warranty period is lower than the expected failure rate as defined in the FMEDA. The environmental specifications and the function of the product are the same as the fielded version. It also shows that the number of hours achieved meets the minimum amount required for the given SIL per the exida scheme.

Software must have same operational profile for all field installations that were used to calculate PIU hours. This means:

- Software must run on same hardware
- Software must have simple flow control and data flow
- Control flow and data flow must have minimal dependencies on configuration parameters or physical parameters such as temperature
- Any applications or variants of the product that do not conform to this operational profile must be explicitly excluded in the safety manual.

The MPS 5.0 is preconfigured for the customers' end application, there is no user configurable element so there are no variations to the product other than the preconfigured gas that it is set up to measure.

The product has been shipping for 30 months without any significant revisions or changes (NOTE: Based on the assumption that installation takes six months. Significant changes include any change in design structure or new features that interrelate with existing features.). This is supported by the shipping records and the PIU analysis.

**Conclusion**

The objectives of the standard for Proven In Use for SIL 2 are fulfilled by the NevadaNano field history and return procedures and supported by PIU analysis. This can be used as supporting evidence when the MPS 5.0 is integrated into the final SIS.

## 5.2 Software Design and Verification

**Assessment**

The software design was not assessed other than through the PIU analysis and the Field Failure comparison to the FMEDA assessment. Exida did examine the coding standard [D16] used and the assessment of the development tools. The System Architecture Design does clearly identify all safety critical interfaces. Code protection is considered where needed. While the design employs safety critical digital communications, they are over a bus using fixed connectors between subsystems of the product, and are carried over distances shorter than 1 meter, and therefore a safety communications analysis is not required.

Communication to and from the MPS Flammable Gas Sensor 5.0 is made up of "packets." The communication paradigm is that of "request" and "reply."

An external host sends a "request" packet to the sensor. The sensor returns a "reply" packet to the external host. A packet consists of a fixed size "header" and a variable length "payload." It is possible for a packet to have no payload (length of zero) where a packet contains only a header. The payload, if any, typically consists of "parameters" for a request or "result" for a reply. Even when a reply does not contain any result, a reply is still sent with the header as an acknowledgement of the request.

**Conclusion**

The objectives of the standard are fulfilled by the NevadaNano functional safety management system, internal organizational procedures, software development process, and new product development processes and supported by PIU analysis. This can be used as supporting evidence when the MPS 5.0 is integrated into the final SIS.

## 5.3 Safety Validation

### Objectives

- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.
- Plan the validation of the safety of the E/E/PE safety-related systems.
- Validate that the E/E/PE safety-related systems meet, in all respects, the requirements for safety in terms of the required safety functions and the safety integrity.
- Ensure that the integrated system complies with the specified requirements for software safety at the intended safety integrity level.
- Validate that the E/E/PE safety-related systems have been tested to comply with EMC immunity standards[1].

### Assessment

The product is subject to EMI Susceptibility testing up to its maximum specification while being functionally tested. IEC 61508-2 specifies conformance to IEC 61326-3-1 but the testing was done to the IEC 61326-1 standard because this is a suitable standard for this type of device, it specifies Electromagnetic Compatibility (EMC) requirements for electrical equipment used in measurement, control, and laboratory environments. The levels used in the testing are the same as those called out in IEC 61326-3-1 at SIL2.

Datasheet mentions:

- Compliant to IEC 60079-29-1 Edition 2.1 Annex A
- Electrostatic Discharge Immunity (Std: JEDEC JS001-2017) Human Body Model, passed at 2 kV
- EMC: Radio Frequency Electromagnetic Field Immunity (Std: EN 61326-1:2020) Test Method EN 61000-4-3:2013 80 MHz to 6 GHz at 10 V/m, horizontal & vertical polarities. Class A
- EMC: Power Frequency Magnetic Field Immunity (Std: EN 61326-1:2020) Test Method EN 61000-4-8:2010 30 A/m, 3 axes, 50 Hz and 60 Hz
- EMC: Radio Frequency Disturbance Characteristics (Std: EN 61326-1:2020) Test Method EN 55011:2010 30 MHz to 1 GHz. Class A

The product also already has a certificate for EN50271 - Electrical apparatus for the detection and measurement of combustible gases, toxic gases or oxygen - Requirements and tests for apparatus using software and/or digital technologies.

The product meets the criteria for Proven in Use (PIU), and the product has a single safety function which is simple, such that it can be confirmed that the functions are working correctly based on the PIU evidence. It can be assumed that the safety function not working properly would be obvious to the customer and would likely be reported as a failure. VTP-7 (EMI Susceptibility) sufficiently covers the requirements for validation test planning under Proven In Use criteria. This requirement is therefore not applicable.

[1] IEC 61000-6-2, Electromagnetic compatibility, Generic standards – Immunity for industrial environments
IEC 61326-3-1, Electrical equipment for measurement, control and laboratory use – EMC requirements

### Conclusion

The objectives of the standard are fulfilled by the NevadaNano functional safety management system, internal organizational procedures, software development process, and new product development processes and supported by PIU analysis. This can be used as supporting evidence when the MPS 5.0 is integrated into the final SIS.

## 5.4 Hardware Design and Verification

### Objectives

The main objectives of the related IEC 61508 requirements are to:

- Create E/E/PE safety-related systems conforming to the specification for the E/E/PE safety requirements (comprising the specification for the E/E/PE safety functions requirements and the specification for the E/E/PE safety integrity requirements).
- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.
- Demonstrate, for each phase of the overall, E/E/PE and software safety lifecycles (by review, analysis and/or tests), that the outputs meet in all respects the objectives and requirements specified for the phase.
- Test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase.
- Integrate and test the E/E/PE safety-related systems.

### 5.4.1 Hardware Architecture Design and Probabilistic Properties

### Assessment

The System Architecture Design [D11] clearly identifies all safety critical interfaces. Hardware architecture design has been partitioned into subsystems, and interfaces between subsystems are defined and documented. Non-interference is not applicable as there are no functions that are not covered by the PIU assessment. To evaluate the hardware design of the S4 MPS 5.0, a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) was performed by *exida* for each component in the system. This is documented in [R4].

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration. The FMEDA is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design.

From the FMEDA, failure rates are derived for each important failure category.

### Conclusion

The objectives of the standard are fulfilled by the NevadaNano functional safety management system, FMEDA quantitative analysis, and hardware development guidelines and practices and supported by PIU analysis. This can be used as supporting evidence when the MPS 5.0 is integrated into the final SIS.

## 5.5 Safety Manual

### Objectives

- Develop procedures to ensure that the required functional safety of the E/E/PE safety-related systems is maintained during operation and maintenance.

### Assessment

The User Manual is provided [D22] and identifies and describes the functions of the product (Section 1). The functions are clearly described, including a description of the input and output interfaces (Section 2). When internal faults are detected, their effect on the device output is clearly described (Section 2 & 5). Sufficient information shall be provided to facilitate the development of an external diagnostics capability (Section 2.4).

The User Manual identifies the hardware and software configuration (Section 2.1.6.9) of the product (Section 3.1.) in order to provide the device user with information about exactly what device to use in a safety function.

The User Manual doesn't directly state the diagnostic test interval of the product (Section 2.1.4) but this is clearly indicated on the product datasheet - it is 2 seconds. The User Manual gives guidance on recommended periodic (offline) proof test activities for the product, including listing any tools necessary for proof testing. Procedures for maintaining tools and test equipment are listed. This is detailed in Section 4.1.1 and 4.1.2.

The User Manual identifies all communications methods and protocols that are implemented, due to the MPS being integrated into a larger product, a safety comms analysis is not required as they will be integrated on to the same PCB.

Each software release is accompanied by release notes [D26].

The User Manual includes valuable information for the user of the device or system regarding safe operation and avoidance of hazards. This document considers user/maintenance friendliness, limited operation modes, and protection against operator mistakes.

### Conclusion

The objectives of the standard are fulfilled by the NevadaNano the safety manual and can be used as supporting evidence when the MPS 5.0 is integrated into the final SIS.

# 6 Terms and Definitions

| | |
|---|---|
| E/E/PE | Electric/Electronic/Programmable Electronic safety-related system |
| Fault tolerance | Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3) |
| FIT | Failure In Time ($1x10^{-9}$ failures per hour) |
| FMEDA | Failure Mode Effect and Diagnostic Analysis |
| HFT | Hardware Fault Tolerance |
| $PFD_{AVG}$ | Average Probability of Failure on Demand |
| PFH | Probability of dangerous Failure per Hour |
| PIU | Proven-In-Use |
| SFF | Safe Failure Fraction - Summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action. |
| SIF | Safety Instrumented Function |
| SIL | Safety Integrity Level |
| SIS | Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s). |

# 7 Status of the document

## 7.1 Liability

*exida* prepares reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

## 7.2 Version History

| Contract Number | Report Number | Revision Notes |
|---|---|---|
| Q26/03-113 | NVN 26-03-113 V1 R0 | Initial release, PWH 27-Jul-2026 |
| Q26/03-113 | NVN 26-03-113 V1 R1 | Updated release at request of customer, PWH. 29th July 2026 |
| Q26/03-113 | NVN 26-03-113 V1 R2 | Updated release at request of customer, PWH, 8th Aug 2026 |
| Q26/03-113 | NVN 26-03-113 V1 R3 | Updated release at request of customer, PWH, 8th Aug 2026 |

Reviewer: Valerie Motto, exida, 28 July 2026
Status: Released, 08 Aug 2026

## 7.3 Future enhancements

At request of client.

## 7.4 Release signatures

Paddy Healy, Senior Safety Engineer

Valerie Motto, CFSP, Senior Safety Engineer

END OF DOCUMENT