TOPICAL REPORT

SOLO™ I&C Architecture and Design Basis for Reactor Protection System (RPS)

(Non-Proprietary)

Total Pages:37

Document Number: SOLO-TR-2025-5

Revision 0

(Enclosure 4)

2026-03-01

Terra Innovatum s.r.l.

Via Matteo Trenta 117, 55100 Lucca (LU), Italy

Notes on revisions, source control and e-attachments:

Revision 0

First release.

Signatures

Role	Person	Signature
Author	Ivica Bašić	
Reviewers	Simone Di Pasquale, Chris Gosdin	
Approver	Cesare Frepoli	

Git commit

N/A

Archive Content (e-attachments)

None

Instructions

None.

ACRONYMS AND ABBREVIATIONS

Table 1 – Acronyms and Abbreviations

Term	Definition
AOO	Anticipated Operational Occurrence
DBE	Design Basis Event
HIPS	Highly Integrated Protection System
FOAK	First Of A Kind
FPGA	Field Programmable Gate Array
FW	Feed Water
I&C	Instrumentation and Control
ISG	Interim Staff Guidance
IRC	Integrated Radiological Containment
LCO	Limited Condition for Operation
MMR	Micro Modular Reactor
MS	Main Steam
NOAK	Next of A Kind
NRC	Nuclear Regulatory Commission
PSAR	Preliminary Safety Analysis Report
PDC	Principal Design Criteria
PTCS	Pressure Tubes Coolant System
RFDC	Required Functional Design Criteria
RPS	Reactor Protection System
SR	Safety-Related
SSC	Structure, System, or Component
V&V	Verification and Validation

EXECUTIVE SUMMARY

This topical report documents the Instrumentation and Control (I&C) Architecture and Design Basis for the Reactor Protection System (RPS) for the SOLO Micro Modular Reactor (MMR). The report describes the RPS objectives and safety functions, safety classification, architectural layout, functional description, voting logic, and the technical basis for the selected design approach.

Terra Innovatum hereby submits this topical report to the U.S. Nuclear Regulatory Commission (NRC) for review and approval. Upon approval, Terra Innovatum intends to reference this topical report in the Preliminary Safety Analysis Report (PSAR) and subsequent licensing applications supporting the Construction Permit and Operating License for the SOLO MMR.

The SOLO MMR RPS licensing basis follows a deterministic framework consistent with NUREG-1537 [1] [2], including the applicable acceptance criteria of Chapter 7 for non-power reactors. Risk-informed considerations are incorporated where appropriate but do not replace deterministic design requirements. Applicable standards include ANSI/ANS-15.8-1995 for quality assurance [3], IEEE 7-4.3.2 [4] guidance for digital safety systems (as incorporated through the ISG), and relevant regulatory guidance governing safety-related instrumentation and control systems. This report demonstrates how the SOLO Principal Design Criteria (PDCs), as described in SOLO-TR-2025-1 [5] , relevant to reactor protection are satisfied.

The RPS design described herein establishes the licensing design basis envelope. The conceptual design is informed by the Paragon RPS Design Description for the Terra Innovatum SOLO Reactor [6] and leverages experience from Highly Integrated Protection System (HIPS) platform implementations [7]. However, the SOLO RPS design is evaluated independently against the applicable regulatory requirements for non-power reactors [8].

The SOLO RPS is designed to satisfy the single-failure criterion, including consideration of digital common-cause failure mechanisms, such that no single credible failure prevents the accomplishment of required safety functions or results in unintended actuation inconsistent with the safety analyses. Key design principles include redundancy at the sensor, logic, actuation, and power levels, independence and isolation between safety divisions and from non-safety systems, diversity to mitigate common-cause failures and fail-safe operation, such that loss of power results in reactor shutdown.

The RPS is a digitally implemented, deterministic protection system based on Field Programmable Gate Array (FPGA) technology and deployed across two physically and electrically independent safety trains.

Monitored parameters include neutron flux, coolant temperatures and pressures, helium conditions, containment pressure, radiation levels, and key equipment status signals. Each safety-significant parameter is measured through multiple independent channels to support coincidence voting logic.

The RPS employs [[ ]] coincidence voting logic for trip determination and [[ ]] Setpoints are established using conservative methodologies [9] consistent with safety limits and analytical limits defined in the safety analysis. Upon single-channel failure, the system maintains full protective capability and reconfigures as needed to preserve reliability while minimizing spurious trips.

The RPS uses deterministic FPGA-based processing to eliminate non-deterministic operating system dependencies. The digital lifecycle is governed by structured development processes including fully specified functional requirements, independent verification and validation (V&V), robust configuration management and defined behavior under anomalous conditions. These measures align with IEEE 7-4.3.2 guidance and address potential digital common-cause failure mechanisms.

The RPS is designed to support online testing, calibration, and maintenance without compromising required protection. Independent channel testing, controlled bypass features, continuous self-diagnostics, and startup self-testing are incorporated.

Administrative and technical controls ensure that any temporary bypass conditions maintain compliance with the single-failure criterion and clearly indicate system status to operators. Bypass duration is minimized and strictly controlled.

All safety-related components are environmentally and seismically qualified consistent with design-basis conditions. Pressure boundary penetrations maintain hermetic sealing and electrical isolation.

The RPS does not depend on non-safety systems for execution of protective functions. Any data transmitted to non-safety systems is routed through qualified isolation devices, preserving independence and integrity.

This topical report demonstrates compliance with the applicable acceptance criteria of NUREG-1537 Chapter 7. Specifically, the SOLO RPS::

- Automatically initiates protective action prior to exceeding safety limits;
- Satisfies the single-failure criterion;
- Incorporates redundancy, independence, and diversity;
- Applies conservative setpoint methodology;
- Maintains fail-safe characteristics;
- Supports testing and maintenance without degrading protection;
- Implements disciplined digital lifecycle and quality assurance controls.

Based on this evaluation, the SOLO Reactor Protection System provides reasonable assurance that it will perform its intended safety functions under all analyzed operating and accident conditions. The design is consistent with regulatory expectations for non-power reactor protection systems and is suitable to support NRC review and approval for the SOLO FOAK project.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE

This topical report documents I&C Architecture and Design Basis for Reactor Protection System (RPS) for the SOLO MMR design and the basis for their selection including the RPS objectives and safety functions, safety classification, architectural layout, functional description and voting logic overview.

Terra Innovatum is submitting this topical report for NRC review and approval in support of the future Construction Permit and Operating License for the SOLO MMR.

1.2 SCOPE

This topical report documents the I&C Architecture and Design Basis for RPS for the SOLO MMR and discusses the application of NUREG-1537 "Guidelines for Preparing and Reviewing Applications for the Licensing of non-Power Reactors", [1] and [2] Chapter 7.4 RPS including relevant information as outlined in Sections 7.2.1, 7.2.2 and 7.2.3 [1] for RPS. This report establishes the licensing design basis for the SOLO RPS and describes how the applicable SOLO PDCs, as defined in SOLO-TR-2025-1 [7] are satisfied with respect to reactor protection functions. The document defines the system safety functions, classification, architecture, design principles, independence, redundancy, voting logic, and digital implementation approach.

The RPS design described herein is informed by the Paragon RPS Design Description for the Terra Innovatum SOLO Reactor [6] and leverages design experience from implementations of the HIPS platform [7] and safety evaluated for implementation in NuScale Power Reactor . However, the SOLO RPS is evaluated independently against the regulatory requirements applicable to non-power reactors under NUREG-1537.

This topical report establishes the architectural, functional, and safety design basis of the RPS. Detailed analyses of RPS operation and performance, including quantitative evaluation of scrams, runbacks, interlocks, engineered safety feature (ESF) initiators, and associated technical specifications, consistent with Section 7.2.4 of NUREG-1537 [1], are being developed in parallel with the deterministic safety analyses for Anticipated Operational Occurrences (AOOs) and Design Basis Events (DBEs) supporting PSAR Chapter 15.

Those analyses will evaluate RPS response to postulated credible accidents, transients, and other events requiring protective action using approved evaluation models, SOLO-specific analytical models, and associated computer codes. The detailed performance results are outside the scope of this topical report and will be provided in the PSAR. Such analyses will remain bounded by the RPS design basis and architectural framework described herein.

1.3 APPLICABLE REGULATIONS AND REGULATORY GUIDANCE

The SOLO MMR is intended to be licensed under Section 104(c) of the Atomic Energy Act and 10 CFR Part 50 as a non-power reactor facility. Accordingly, the licensing basis for the SOLO RPS is established consistent with the regulatory framework applicable to Class 104(c) facilities.

The NRC issued NUREG-1537 "Guidelines for Preparing and Reviewing Applications for the Licensing of non-Power Reactors", [1] and [2], to provide guidance in all aspects of licensing Class 104(c) facilities. Chapter 7 of NUREG-1537 provides acceptance criteria and review guidance for Instrumentation and Control systems, including Section 7.4 addressing Reactor Protection Systems. The SOLO RPS is designed to meet the applicable acceptance criteria identified in NUREG-1537 Sections 7.2.1, 7.2.2, 7.2.3, and 7.4.

In addition, NRC ISG supplementing Chapter 7 of NUREG-1537, including guidance applicable to digital safety systems, is considered in establishing the SOLO RPS licensing basis. Such guidance is used to inform the design, evaluation, and documentation of the digital RPS architecture, including treatment of software, hardware, independence, diversity, and common-cause failure considerations.

The licensing basis for the SOLO MMR is primarily deterministic and consistent with the guidance and acceptance criteria of NUREG-1537. Risk-informed insights may be used to support or corroborate design decisions; however, such considerations do not replace or reduce compliance with deterministic regulatory requirements applicable to non-power reactor facilities.

1.4 REQUEST FOR NRC

Terra Innovatum is requesting NRC review and approval of "I&C Architecture and Design Basis for RPS" for the SOLO Micro Modular Reactor FOAK Project as discussed in this topical report.

2 RECTOR PROTECTION SYSTEM (RPS) OVERVVIEW

The general overview provides the objectives and safety functions, safety classification, architectural layout, functional description and voting logic overview. The system proposed to provide reactor protection is the HIPS platform.

2.1 RPS OBJECTIVES AND SAFETY FUNCTION

The objective of the RPS is to automatically initiate protective actions to prevent exceeding established safety limits and to place and maintain the reactor in a safe, shutdown condition during AOOs and DBEs. The RPS is designed to protect the integrity of the fuel and other fission product barriers and to ensure the protection of public health and safety. The RPS protects the reactor core from transient conditions that could exceed design margins, including but not limited to operational errors, equipment failures, design basis accidents, or beyond design basis events that threaten safety barriers.

The RPS executes its protection functions by monitoring plant parameters and comparing the values against predetermined design basis setpoints. Upon detection of conditions that could challenge safety limits, the system initiates automatic scram and associated engineered safety feature actuations, triggering safety system activation.

The RPS is functionally independent from non-safety systems and does not rely on non-safety-related equipment for execution of protective functions. Inputs are received through dedicated, safety-classified instrumentation channels, and protective outputs are transmitted through safety-related actuation circuits. Electrical and communication isolation is provided to preserve independence and prevent adverse interactions.

Reactor shutdown and maintenance of subcriticality are achieved through diverse and redundant reactivity control mechanisms, including [[ ]] These actuations are designed to achieve and maintain the reactor in a safe shutdown condition under all analyzed operating and accident conditions.

2.2 RPS SAFETY CLASSIFICATION

The RPS is classified as “safety-related” as appropriate and as defined for the SOLO reactor application. The RPS performs functions necessary to meet the safety objectives established in the SOLO PDCs and the licensing basis developed under NUREG-1537.

1. For the SOLO project, “safety-related” structures, systems, and components (SSCs) are those relied upon to: Maintain the integrity of the reactor coolant pressure boundary (the reactor vessel and associated piping that circulates the reactor coolant);
2. Shut down the reactor and maintain it in a safe shutdown condition; or
3. Prevent or mitigate the consequences of AOOs and DBEs that could otherwise result in potential radiological consequences.

The RPS is relied upon to automatically initiate reactor shutdown and associated protective actions necessary to prevent exceeding safety limits and to preserve the integrity of fuel and other fission product barriers. Accordingly, the RPS, including its safety-classified sensors, logic processing equipment, actuation devices, and required support power supplies, is designated as safety-related.

The safety classification ensures that the RPS is designed, fabricated, installed, tested, and maintained in accordance with the applicable quality assurance requirements, environmental qualification requirements, seismic qualification requirements, and independence criteria consistent with its credited safety functions.

2.3 SYSTEM OPERATION

The SOLO RPS operates as an autonomous safety system that requires no human intervention for design basis protective functions. The system monitors critical plant parameters, processes instrumentation signals, and automatically initiates reactor trip functions when predetermined safety setpoints are exceeded. Figure 1 provides a simplified signal progression diagram of the SOLO RPS. The RPS is implemented using the HIPS platform architecture. Simplified HIPS Chassis Signal Progression Diagram is shown on Figure *2*.

The RPS incorporates manual reactor trip capability for the FOAK reactor, allowing licensed reactor operators to initiate protective actions independent of automatic trip logic. [[

]]

[[

]]

Figure 1:Multi-level modular RPS diagram

[[

]]

Figure 2: HIPS Chassis Signal Progression Diagram

2.3.1 RPS Voting Logic

To enhance operational reliability and avoid spurious reactor trips, the system utilizes multiple input channels for each safety related input, processed through a logical voting stage, before generating a reactor trip signal. For example, in the voting circuit figure above, the system will only generate a trip signal if [[ ]] instruments reading a particular parameter reach threshold values.

This allows the RPS to remain stable and operational in the presence of up to [[

]]

[[

]]

However, upon the failure of another channel, a limiting condition of operation (LCO) with an associated repair time will be declared. [[

]]

Figure 3 presents [[ ]] Figure 4 presents [[

]]

[[

]]

3 RPS DESIGN INPUTS AND REQUIREMENTS

The purpose of this section is to explain the licensing basis chosen for the SOLO RPS and describe the design bases thereof.

The SOLO reactor, and therefore all comprising systems, will be licensed as a Class 104(c) facility. The NRC issued NUREG-1537 “Guidelines for Preparing and Reviewing Applications for the Licensing of non-Power Reactors” to provide guidance in all aspects of licensing Class 104(c) facilities. Additionally, an ISG supplemental to Chapter 7 of NUREG-1537 specifically has been made available for further guidance.

The significance of the safety functions performed by the SOLO RPS are aligned with the description of a non-power reactor RPS given in NUREG-1537, therefore guidance from the NUREG and the associated Chapter 7 ISG will be used to create the licensing basis for the RPS. The following design criteria and bases are selected for use from the guidance.

3.1 PRINCIPAL DESIGN INPUT AND REQUIREMENTS

3.1.1 General Requirement

The RPS is designed to automatically place and maintain the reactor in a safe shutdown condition whenever established safety limits could be challenged. Protective actions are initiated prior to exceeding safety limits, consistent with the deterministic safety analyses described in PSAR Chapter 15.

Trip setpoints are conservatively derived from analytical limits established in the safety analysis to ensure that safety limits are not exceeded during AOOs or DBEs.

3.1.2 Safety Classification

As described in Section 2.2, the RPS is classified as safety-related. The RPS performs functions necessary to:

1. Ensure the integrity of the reactor PTCS and Integrated Radiological Containment (IRC) pressure boundaries;
2. Provide the capability to shut down the reactor and maintain it in a safe shutdown condition; or
3. Prevent or mitigate the consequences of accidents that could result in potential offsite exposures.

Accordingly, RPS components credited for safety functions are designed, fabricated, installed, tested, and maintained in accordance with safety-related requirements and the applicable quality assurance program.

3.1.3 Regulatory Basis and Licensing Framework

The SOLO reactor is intended to be licensed as a non-power utilization facility under 10 CFR Part 50, Class 104(c). The RPS licensing basis is established consistent with the following guidance and standards:

- NUREG-1537, *Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors*, including Chapter 7 review guidance [1] and [2].
- ISG associated with Chapter 7 of NUREG-1537 [1] and [2].
- ANSI/ANS-15.8-1995, *Quality Assurance Program Requirements for Research Reactors* [3].

- IEEE 7-4.3.2, as incorporated through the Chapter 7 ISG at a level appropriate for a non-power reactor [4]
- Regulatory Guide 2.5 (Quality Assurance Program Requirements for Research Reactors) [10]
- Applicable portions of IEEE 497-2016 [11] and Regulatory Guide 1.97 [12] (as evaluated for safety significance and operating license commitments).

The RPS is developed and implemented under a quality assurance program consistent with ANSI/ANS-15.8-1995 and applicable provisions of 10 CFR Part 50. The licensing basis is deterministic. Risk insights may be used to support design decisions but do not replace deterministic compliance with regulatory requirements.

3.1.4 Functional Requirements

Automatic Protective Actions

The RPS shall:

1. Automatically initiate a reactor scram upon detection of monitored parameters meeting or exceeding predefined trip criteria.
2. Clearly define input, processing, and output criteria for each protective function.
3. Complete protective actions once initiated; consistent with safety analysis assumptions.
4. Perform credited safety functions without requiring operator intervention.
5. Prevent control room operator actions from defeating automatic safety functions.

These requirements are consistent with NUREG-1537 guidance for non-power reactor protection systems.

Manual Protective Actions

The RPS shall include manual reactor trip capability located in the main control room (FOAK configuration). Manual trip:

- Overrides automatic logic and voting circuitry;
- Directly actuates all required protective functions;
- Provides diverse means of achieving reactor shutdown.

[[ ]]

Safe State Definition

The RPS shall drive the plant to a known, defined, and verifiable safe shutdown state during any abnormal or failure condition. Safe states are defined in terms of reactor subcriticality and maintenance of safety barrier integrity.

Trip Reset Logic

Once a reactor trip is initiated:

- Manual operator action is required to reset trip logic.

- Predefined reset conditions must be satisfied..
- Reactor restart is prevented until protective conditions are verified.

This requirement provides a deliberate human verification step prior to re-criticality.

<u>Redundancy and Single-Failure Criterion</u>

The RPS is designed to meet the single-failure criterion consistent with NUREG-1537 Chapter 7 guidance.

Redundancy provided as follows:

- [[.]]
- [[ ]]
- [[ ]]
- [[ ]]
- Two independent architectural trains capable of performing required safety functions.
- At least two independent power supplies, each capable of supporting full RPS load.

No single credible failure, including one channel out of service, prevents accomplishment of required safety functions or results in unintended protective action inconsistent with safety analyses.

<u>Channel Independence and Isolation</u>

The RPS is designed with sufficient independence such that:

- Failure in one channel does not impair the safety function of another.
- Channels are physically and electrically separated.
- The RPS is independent of non-safety systems.
- Isolation devices between safety and non-safety systems are qualified as safety-related.

Instrumentation routing, power supplies, logic processing, and actuation circuits are arranged such that no credible single event disables the protective function.

<u>Equipment and Performance Requirements</u>

The RPS shall:

- Measure safety-significant parameters using redundant, safety-grade instrumentation.
- Employ deterministic logic processing.

- Meet system response times assumed in Chapter 15 analyses of AOOs and DBEs.
- Verify completion status of protective action sequences.
- Operate autonomously under design-basis conditions.

Power supplies are independent and designed such that loss of power results in a safe-state actuation (fail-safe behavior).

3.1.5 Maintenance, Testing, and Bypass Requirements

Online Testing and Surveillance

The RPS is designed to allow:

- Periodic testing, calibration, and inspection during reactor operation;
- Independent channel testing;
- Testing that duplicates, as closely as practical, the performance required of automatic and manual circuitry.

During testing or maintenance, the remaining RPS channels shall continue to satisfy the single-failure criterion or demonstrate acceptable reliability. RPS is capable of performing on-line continuous self-diagnostics for early identification of inoperable or faulted equipment. Self-diagnostics is included during system start-up and continuously while the system is operating.

Bypass Controls

Operational and maintenance bypasses:

- Are permitted only under defined permissive conditions;
- Shall not compromise scram capability of remaining channels;
- Are clearly indicated in the control room;
- Are automatically removed when plant operating conditions require protection;
- Include physical or administrative controls to prevent unauthorized use.

Bypass duration is minimized and controlled in accordance with administrative procedures.

3.1.6 Software Quality Assurance and Configuration Management

Given the digital implementation of the RPS, requirements include:

- Safety-related software shall be developed using structured processes that incorporate disciplined specification and implementation of design requirements throughout the software lifecycle.
- The development process shall ensure that software requirements specifications are functionally characterized with accuracy requirements stated numerically with appropriate physical units and error bounds.
- Software functionality shall be specified in terms of inputs to functions, transformations carried out by functions, and outputs generated by functions.

- Requirements specifications shall fully define software behavior in the presence of unexpected, incorrect, anomalous, or improper input, hardware behavior, or software behavior.
- Software requirements specifications shall be complete, describing all actions required of the computer system for all operating modes and all possible values of input variables, and describing actions the software is prohibited from executing.
- Verification and validation processes shall provide objective assessment of software products and processes throughout the software lifecycle. These processes shall demonstrate whether system requirements and software requirements are correct, complete, accurate, consistent, and testable.
- Verification and validation shall determine whether development products conform to requirements of each activity and whether the system performs according to its intended use and user needs.
- The verification and validation effort shall maintain required levels of technical independence, managerial independence, and financial independence.
- A configuration management program shall be implemented that emphasizes design process for software including criteria for administrative control, design documentation, design interface control, design change control, document control, identification and control of parts and components, and control and retrieval of qualification information.
- Configuration management shall control the substantial design process information and intermediate design outputs associated with final software design output.
- Robust change management processes shall address the frequency of software engineering changes.
- Identification and control of product versions shall be maintained throughout the software lifecycle.
- Predeveloped software and commercial off-the-shelf software shall be qualified for reliably performing required safety functions.
- Software critical characteristics essential for performance of safety functions shall be validated and qualified to ensure no unanalyzed failure modes are introduced.
- The applicability of specific products to safety applications shall be demonstrated through qualification.
- Software treated as a component in programmable devices shall meet all criteria applicable to safety-related software including quality requirements, verification and validation, and documentation.

These controls are consistent with IEEE 7-4.3.2 guidance as incorporated through NUREG-1537 Chapter 7 ISG and ANSI/ANS-15.8-1995 quality program requirements.

3.1.7 Security Requirements

The RPS incorporates cybersecurity and physical protection measures consistent with applicable NRC guidance for digital safety systems. These include:

- Access control (dedicated maintenance equipment restricted to secure areas).
- Cyber security interface (logical and physical protection or disabling of unused communication ports).
- Logical isolation of safety networks.
- Restricted and controlled maintenance interfaces.
- Protection of communication pathways.
- Administrative and technical controls preventing unauthorized modification.

Cybersecurity provisions are consistent with applicable NRC guidance for digital safety systems and planned operating license commitments.

3.1.8 Environmental and Human Factors Requirements

The RPS design shall:

- Ensure seismic design and protection against external and internal hazards;
- Ensure environmental qualification for pressure boundary penetrations and safety-related components;
- Ensure protection against electromagnetic and radio frequency interferences;
- Provide clear indication of system status, bypassed channels, and inoperable conditions.
- Locate equipment to facilitate inspection, maintenance, and calibration;
- Incorporate ALARA considerations for occupational exposure

[[

]]

3.2 SUMMARY OF DESIGN COMPLIANCE

The design inputs and requirements described above ensure that the SOLO RPS:

- Automatically initiates protective action prior to exceeding safety limits;
- Satisfies the single-failure criterion;
- Maintains independence and redundancy;
- Supports safe testing and maintenance without compromising protection;
- Implements disciplined digital system lifecycle controls;

- Complies with applicable guidance of NUREG-1537 Chapter 7, associated ISG, and ANSI/ANS-15.8-1995.

These design inputs form the basis for the detailed system description provided in Section 4 below and demonstrate reasonable assurance that the RPS will perform its intended safety functions under all analyzed operating and accident conditions.

4 RPS DESCRIPTION

The RPS is a safety-related, autonomous instrumentation and control system designed to automatically initiate reactor shutdown and maintain the reactor in a safe shutdown condition whenever monitored parameters approach or exceed predetermined safety limits.

The RPS performs three fundamental functions:

1. **Continuous Monitoring** – Receives and processes real-time signals from safety-related field instrumentation associated with core reactivity, heat removal capability, coolant system integrity, and radiological conditions.
2. **Trip Determination** – Evaluates plant parameters against predefined safety setpoints using deterministic logic processing consistent with the single-failure criterion.
3. **Protective Actuation** – Issues scram and safety system activation signals when trip criteria are satisfied.

The system continuously monitors selected plant parameters, compares measured values to established limiting safety system settings (LSSSs. When trip criteria are met, the RPS automatically initiates protective actions within the response times assumed in the safety analysis. The RPS performs its safety functions without reliance on non-safety systems and without requiring operator intervention.

4.1 DESCRIPTION OF SYSTEM, SUBSYSTEMS AND MAJOR COMPONENTS

The principal safety functions of the RPS are:

1. Continuous Monitoring – Acquisition and processing of signals from redundant, safety-related field instrumentation associated with core reactivity, coolant system parameters, and radiological conditions;
2. Trip Determination – Deterministic evaluation of monitored parameters against established Limiting Safety System Settings (LSSSs);
3. Coincidence Logic Processing – Application of redundant coincidence voting logic [[

   ]] to determine trip conditions while satisfying the single-failure criterion;
4. Protective Actuation – Generation of reactor scram signals and associated safety system actuation commands through redundant actuation pathways;
5. Actuation Verification – Confirmation of successful completion of protective action sequences and annunciation of system status to operators.

4.1.1 System Architecture

The RPS is implemented using the HIPS platform. The platform consists of cabinet-based chassis assemblies and modular components performing:

- Analog and digital signal acquisition;
- Signal conditioning;

- Setpoint comparison;
- Coincidence voting;
- Protective actuation output generation.

The architecture consists of two physically and electrically independent safety divisions (trains). Each train is capable of independently performing required protection functions. Figure 5 presents SOLO RPS basic architecture and interfacing components.

[[

]]

Figure 5: RPS architecture and interfacing components

RPS satisfies basic safety engineering design incorporating:

<u>Redundancy</u>

Redundancy is incorporated at multiple levels:

- Multiple independent instrument channels per safety-significant parameter;
- Redundant signal conditioning and comparator channels;

- [[ ]] voting logic for trip determination;
- [[ ]] actuation logic for protection device actuation;
- Two independent architectural trains;
- At least two independent power supplies, each capable of supplying full RPS load.

The system is designed to meet the single-failure criterion such that no single failure prevents accomplishment of the required protective function.

Diversity

To reduce susceptibility to common-cause failure, the RPS incorporates design diversity including:

- Use of different FPGA technologies between the two safety trains (e.g., flash/OTP-based and SRAM-based architectures);
- Diverse protective actuation mechanisms [[ ]]
- Manual trip capability independent of automatic voting logic.

Diversity complements redundancy to enhance overall system reliability.

Independence and Isolation

The RPS is physically and electrically independent:

- Between safety divisions;
- From non-safety-related systems;
- From the Distributed Control System and other plant monitoring systems.

The RPS does not require input from non-safety systems to perform its safety functions. Where information is provided to non-safety systems for display or data recording, it is transmitted through qualified isolation devices.

Instrumentation channels, logic processing, and actuation circuits are arranged such that failure in one channel does not impair the function of another channel.

4.1.2 Field Instrumentation

Monitored Parameters

The RPS receives inputs from safety-related field instrumentation that monitors parameters necessary to protect reactor safety limits. These parameters include: [[

[[

]]

Figure 6: Principle Scheme of Instrumentation in PTCS and IRC

[[

]]

Figure 7: Principal Scheme of Instrumentation in Secondary Side

Table 1: SOLO RPS Plant parameters

[[

]]

Process of RPS setpoint validation and verification through PSAR 15 deterministic analyses is presented on Figure 8. Methodologies for the determination of RPS setpoints will be in accordance with ISA RP67.04.02-2020 [6].

Instrumentation Characteristics

Instrumentation features include:

- Electrical and physical separation between channels;
- Safety-grade qualification as required;
- Routing through qualified pressure-boundary penetrations;
- Environmental and seismic qualification consistent with design-basis conditions.

Signal routing and installation are arranged such that no expected event renders protective action ineffective.

4.1.3 Actuation Devices

Protective actuation is achieved through diverse, fail-safe mechanisms: [[

]]

4.1.4 System Boundaries and Interfaces

The RPS system boundary extends from:

- Safety-related instrumentation inputs;
  to
- Outputs to shutdown and safety actuation mechanisms.

The RPS is not connected to non-safety systems for execution of safety functions. It may interface with:

- The Main Control Room (in the case of FOAK) for display and indication;
- A dedicated Maintenance Workstation for diagnostics and controlled configuration activities.

No non-safety input is required for protective function execution.

4.1.5 Pressure Boundary Penetrations

Safety-related signals originating within the PTCS or IRC are transmitted through qualified electrical penetration assemblies.

These penetrations:

- Maintain pressure boundary integrity;
- Provide hermetic sealing and electrical isolation;
- Are environmentally and seismically qualified;
- Conform to applicable ASME and IEEE qualification standards.

Penetration assemblies establish the physical interface between in-containment instrumentation and external RPS equipment.

4.1.6 Power Supplies

Each RPS train is supplied by an independent power supply. Either power supply is capable of supporting full system operation. Table presents estimated power consumption for 4 channel HIPS platforms with NMS channels included.

The RPS is designed such that loss of electrical power results in a safe-state actuation. Power supplies are electrically isolated from non-safety systems.

[[

]]

4.1.7 Maintenance and Diagnostics

The RPS includes:

- Continuous online self-diagnostics;

- Startup self-testing;
- Dedicated maintenance workstation;
- Controlled module isolation procedures;
- Capability for online calibration and testing.

During maintenance or testing, remaining channels retain protective capability consistent with the single-failure criterion.

System status, bypassed channels, and inoperable conditions are clearly indicated in the control room (for FOAK) or remote display.

4.2 RPS ACTUATION PARAMETERS AND LOGIC

4.2.1 Signal Progression

Signal progression within the HIPS platform follows a defined sequence:

1. Input acquisition;
2. Signal conditioning;
3. Setpoint comparison;
4. Coincidence voting logic evaluation;
5. Actuation command generation.

The digital logic is implemented using deterministic FPGA-based processing, ensuring bounded execution time and predictable system behavior.

The list of SOLO RPS parameters is presented in Table 1 above.

4.2.2 Voting Logic

To enhance reliability and reduce spurious trips, the RPS employs coincidence voting logic. For example:

- [[

s.]]

Principle voting logics were presented in Figure 3 and Figure 4, above.

4.2.3 Validation and verification of chosen RPS actuation setpoints

RPS Setpoints for FOAK PSAR are chosen based on realistically steady state parameters for normal operation taking into account presumed set-point uncertainties and signal delays as shown in Table 1.

Process of validation and verification by BE TH analyses, which will be covered in Chapter 15 of PSAR, is shown on Figure 8.

[[

]]

Figure 8: Principle Scheme of RPS setpoint V&V

4.3 SUMMARY OF SYSTEM DESCRIPTION

The SOLO Reactor Protection System is a digitally implemented, deterministic, redundant, and diverse safety system designed to:

- Automatically detect conditions approaching safety limits;
- Initiate rapid reactor shutdown;
- Maintain the reactor in a defined safe state;
- Satisfy the single-failure criterion;
- Maintain independence from non-safety systems;
- Support online testing and maintenance without compromising protection.

The system architecture, instrumentation, logic processing, actuation mechanisms, and interfaces provide reasonable assurance that the RPS will perform its intended safety functions under all analyzed operating and accident conditions.

5 SUMMARY AND CONCLUSIONS

5.1 RPS EVALUATION SUMMARY

This section evaluates the RPS against the applicable acceptance criteria of NUREG-1537, Chapter 7. The evaluation provides reasonable assurance that the SOLO RPS design provides reasonable assurance that it will perform its intended safety functions under all analyzed operating and accident conditions described in Chapter 15.

The evaluation addresses:

- Safety function adequacy
- Compliance with the single-failure criterion
- Redundancy, independence, and diversity
- Setpoint methodology
- Environmental and seismic qualification
- Software and digital system controls
- Testing, surveillance, and maintainability
- Fail-safe characteristics

5.1.1 Safety Function Adequacy

NUREG-1537 requires that reactor protection systems automatically detect abnormal conditions and initiate protective action prior to exceeding established Safety Limits.

The SOLO RPS:

- Continuously monitors safety-significant parameters;
- Compares values to limiting safety system settings derived from accident analyses;
- Automatically initiates reactor shutdown when trip criteria are satisfied;
- Ensures protective actions proceed to completion consistent with safety analysis assumptions;
- Requires manual reset before restart.

Trip setpoints are conservatively established to ensure protective action occurs before Safety Limits are exceeded during AOOs and DBEs. Therefore, the RPS meets the functional adequacy expectations of NUREG-1537 for non-power reactor protection systems.

5.1.2 Compliance with the Single-Failure Criterion

NUREG-1537 Chapter 7 specifies that safety systems credited for accident mitigation should meet the single-failure criterion unless otherwise justified.

The SOLO RPS satisfies this criterion through:

- Multiple independent instrument channels per safety parameter;

- [[

]]

- Two independent safety trains;
- Redundant, independent power supplies.

No single credible failure of a sensor, logic channel, actuation circuit, or power source prevents the RPS from performing its required safety function. Where maintenance or testing necessitates temporary channel bypass, administrative controls and technical specifications ensure that required reliability is maintained.

5.1.3 Redundancy, Independence, and Diversity

Redundancy: The RPS incorporates redundancy at the sensor, logic, actuation, and power supply levels. This redundancy supports continued operability during single-channel failure and reduces spurious trip susceptibility.

Independence: Acceptance criteria require physical and electrical separation of redundant channels.

The RPS design provides:

- Electrical isolation between channels;
- Physical separation of safety divisions;
- Qualified isolation devices between safety and non-safety systems;
- No reliance on non-safety systems for protective actuation.

Failure in one channel or division does not impair the capability of the remaining channels to perform required safety functions.

Diversity: To address potential common-cause failures, including digital failure modes, the RPS incorporates:

- Diverse FPGA technologies between safety trains;
- Diverse actuation mechanisms [[ ]] ;
- Manual scram capability independent of automatic logic.

The combination of redundancy and diversity provides additional defense-in-depth consistent with NUREG-1537 guidance.

5.1.4 Setpoint Methodology

NUREG-1537 requires that LSSSs be conservatively derived and account for instrument uncertainties.

The SOLO RPS setpoint methodology:

- Derives analytical limits from Chapter 15 accident analyses;

- Accounts for total loop uncertainty (sensor accuracy, drift, environmental effects, processing error, response time);
- Establishes trip setpoints with margin to analytical limits;
- Provides additional administrative margin in technical specifications.

This methodology ensures automatic protective action occurs before safety limits are exceeded and meets acceptance criteria for setpoint determination. Process of RPS setpoint validation and verification through PSAR 15 deterministic analyses is presented on Figure 8. Methodologies for the determination of RPS setpoints will be in accordance with ISA RP67.04.02-2020 [9].

5.1.5 Digital System Evaluation and Software Controls

NUREG-1537 and its associated Chapter 7 ISG incorporate relevant principles from IEEE 7-4.3.2 for digital safety systems.

The SOLO RPS digital implementation:

- Uses deterministic FPGA-based logic;
- Avoids non-deterministic operating system dependencies;
- Employs structured development processes;
- Implements independent verification and validation (V&V);
- Maintains configuration management and version control of programmable logic;
- Defines software behavior under anomalous or improper inputs.

These controls address potential digital common-cause failures and ensure that programmable logic performs its safety functions as intended.

5.1.6 Environmental and Seismic Qualification

NUREG-1537 requires that safety-related instrumentation and control equipment remain functional under design-basis environmental and seismic conditions.

The RPS:

- Utilizes environmentally and seismically qualified instrumentation;
- Employs qualified pressure-boundary penetration assemblies;
- Locates equipment to minimize radiation exposure consistent with ALARA;
- Ensures cabinets and modules meet applicable environmental design conditions.

Pressure boundary penetrations maintain hermetic sealing and electrical isolation under design-basis service conditions. Equipment location and design incorporate ALARA principles for occupational exposure.

5.1.7 Fail-Safe Characteristics

Acceptance criteria require that protective systems fail in a safe direction where practicable.

The RPS design incorporates fail-safe principles:

- Loss of power results in de-energization and reactor trip;
- [[ ]] to absorbing configurations upon loss of power or signal;
- Protective actions proceed to completion once initiated;
- Manual reset is required prior to restart.

These features ensure that credible power or control failures result in a safe reactor condition.

5.1.8 Testing, Surveillance, and Maintainability

NUREG-1537 requires that safety systems be testable and maintainable without compromising required protection.

The RPS:

- Permits periodic online testing and calibration;
- Allows independent channel testing;
- Incorporates controlled bypass features with clear indication;
- Maintains protective capability during maintenance consistent with the single-failure criterion;
- Includes continuous self-diagnostics and startup self-testing.

Bypass features are administratively controlled and automatically removed when required by operating conditions.

5.1.9 Interfaces and System Boundaries

The RPS boundary extends from safety-related instrumentation inputs to actuation outputs.

The system:

- Does not depend on non-safety systems for protective functions;
- Provides status indication to the control room through isolated interfaces;
- Uses qualified isolation devices for any data transmission to non-safety systems.

This configuration satisfies NUREG-1537 expectations for independence and interface control.

5.2 OVERALL EVALUATION CONCLUSION

Based on the evaluation above, the SOLO Reactor Protection System:

- Provides automatic and reliable reactor shutdown capability;
- Meets the single-failure criterion;
- Incorporates redundancy, independence, and diversity;

- Employs conservative setpoint methodology;
- Implements robust digital lifecycle controls;
- Maintains fail-safe characteristics;
- Supports surveillance and maintenance without compromising protection;
- Meets applicable guidance of NUREG-1537 Chapter 7 and associated ISG.

Accordingly, the SOLO RPS design provides reasonable assurance that it will perform its intended safety functions under all analyzed operating and accident conditions, consistent with regulatory expectations for non-power reactor protection systems. Terra Innovatum requests NRC review and approval of this topical report for incorporation by reference in the SOLO PSAR and subsequent licensing applications.

6 REFERENCES

[1] "NUREG-1537, Part 1 - Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors Format and Content," U.S.NRC, 1996.

[2] "NUREG-1537, Part 2: Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors — Standard Review Plan and Acceptance Criteria," U.S.NRC, 1996.

[3] "ANSI/ANS-15.8-1995, Quality Assurance Program Requirements for Research Reactors," American Nuclear Society (ANS), La Grange Park, Illinois, 1995.

[4] "IEEE Std 7-4.3.2-2016 – IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers (IEEE) (IEEE Standards Association), New York, NY, 2016.

[5] "SOLO-TR-2025-1 - SOLO™ Micro Modular Nuclear Reactor Principal Design Criteria," Terra Innovatum, 2025.

[6] "Paragon RPS Design Description for TINN SOLO Reactor, 2026," Terra Innovatum, 2026.

[7] "NuScale Topical Report TR-1015-18653-NP-A, "Design of the Highly Integrated Protection System Platform Topical Report," Revision 2," NuScale Power, LLC, 2017.

[8] "Safety Evaluation of the NuScale Power, LLC Topical Report TR-0815-16497-P, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 1," U.S.NRC, 2017.

[9] "ANSI/ISA-67.04.02-2010, Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation," ISA, 2010.

[10] "U.S.NRC REGULATORY GUIDE 2.5 QUALITY ASSURANCE PROGRAM REQUIREMENTS FOR RESEARCH AND TEST REACTORS," U.S. Nuclear Regulatory Commission (NRC), Office of Nuclear Regulatory Research, 2010.

[11] "IEEE Std 497-2016 – IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," 2016, Institute of Electrical and Electronics Engineers (IEEE), IEEE 497-2016.

[12] "Regulatory Guide 1.97, Revision 4: Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," U.S.NRC, 2006.