Safety PLC Programming Validation Document

Document ID: PDR-SPLC-2023-V1.2

Effective Date: January 15, 2024

Last Review: December 28, 2023

Document Owner: Automation Safety Control Systems Department

Classification: CONFIDENTIAL

1. Purpose and Scope

1. This document establishes the validation requirements and procedures for safety Programmable Logic Controller (PLC) programming used in Polar Dynamics Robotics, Inc.'s ("Company") autonomous mobile robot systems, specifically the IceNav(TM) platform and associated safety control systems.

2. This validation protocol applies to all safety-critical PLC programming implemented in the Company's cold-environment autonomous mobile robots operating in temperature ranges from -40 C to +25 C.

2. Referenced Standards and Regulations

1. IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems

2. ISO 13849-1: Safety of machinery - Safety-related parts of control systems

3. ANSI/RIA R15.06-2012: Industrial Robots and Robot Systems - Safety Requirements

4. 21 CFR Part 11: Electronic Records; Electronic Signatures (where applicable for pharmaceutical environments)

3. Validation Requirements

1. Safety PLC Program Architecture

- 3.1.1. Dual-channel safety architecture with independent processing
- 3.1.2. Redundant sensor input validation
- 3.1.3. Cross-monitoring of safety functions
- 3.1.4. Fail-safe state definition and implementation

- 3.1.5. Emergency stop functionality verification

2. Critical Safety Functions

- 3.2.1. Motion control safety limits
- 3.2.2. Collision avoidance parameters
- 3.2.3. Temperature monitoring and thermal protection
- 3.2.4. Battery safety management
- 3.2.5. Load stability monitoring
- 3.2.6. Human-robot interaction safety protocols

4. Validation Procedure

1. Documentation Review

- 4.1.1. Safety requirement specifications
- 4.1.2. Risk assessment documentation
- 4.1.3. PLC program architecture diagrams
- 4.1.4. Safety function descriptions
- 4.1.5. Test case specifications

2. Static Analysis

- 4.2.1. Code review by qualified safety engineer
- 4.2.2. Verification of safety programming guidelines compliance
- 4.2.3. Assessment of program structure and modularity
- 4.2.4. Review of variable declarations and data types
- 4.2.5. Evaluation of comment completeness and accuracy

3. Dynamic Testing

- 4.3.1. Functional testing of all safety routines
- 4.3.2. Boundary condition testing
- 4.3.3. Response time verification
- 4.3.4. Fault injection testing
- 4.3.5. Environmental condition simulation

5. Validation Documentation

1. Required Records

- 5.1.1. Test results and data logs
- 5.1.2. Validation summary report
- 5.1.3. Non-conformance reports and resolutions
- 5.1.4. Change control documentation
- 5.1.5. Approval signatures and dates

2. Document Control

- 5.2.1. Version control procedures
- 5.2.2. Document retention requirements
- 5.2.3. Access control protocols
- 5.2.4. Audit trail maintenance

6. Responsibilities

1. Safety Systems Engineer

- 6.1.1. Execution of validation procedures
- 6.1.2. Documentation of test results
- 6.1.3. Non-conformance reporting

2. Quality Assurance Manager

- 6.2.1. Review of validation documentation
- 6.2.2. Approval of validation results
- 6.2.3. Maintenance of validation records

3. Chief Robotics Officer

- 6.3.1. Final approval of validation
- 6.3.2. Authorization for production release
- 6.3.3. Oversight of safety system modifications

7. Validation Approval

The undersigned certify that the safety PLC programming has been validated according to this document and meets all specified requirements:

Safety Systems Engineer: Date:

Quality Assurance Manager: Date:

Chief Robotics Officer: Date:

8. Legal Disclaimer

This document contains confidential and proprietary information of Polar Dynamics Robotics, Inc. Any unauthorized use, reproduction, or distribution is strictly prohibited. While the Company has made every effort to ensure the accuracy and completeness of this validation protocol, it assumes no liability for any errors or omissions. This document shall be governed by and construed in accordance with the laws of the State of Delaware.

Document End.