Scully Intellitrol®2
Safety Manual

Overfill Prevention Control Unit with
Ground Verification & Vehicle Identification Options

IEC 61508 Certified
SIL 2
# Intellitrol®2 - Safety Manual

## Table of Contents

### Introduction
1.1 Terms and Abbreviations  
1.2 Acronyms  
1.3 Product Support  
1.4 Related Literature  
1.5 Reference Standards

### Designing a Safety Instrumented Function

**using a Scully Signal Company Intellitrol**

2.1 Safety Function  
2.2 Environmental limits  
2.3 Design Verification  
2.4 SIL Capability  
2.5 General Requirements

### Installation and Commissioning

3.1 Installation  
3.2 Physical Location and Placement

### Operation and Maintenance

4.1 Proof test  
4.2 Proof Test Procedure  
4.3 Repair and replacement  
4.4 Useful Life  
4.5 Scully Signal Company Notification
This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing a Scully Signal Company Intellitrol Overfill Protection System. This manual provides necessary requirements for meeting the IEC 61511 functional safety standards.

1.1 Terms and Abbreviations

- **Safety**: Freedom from unacceptable risk of harm
- **Functional Safety**: The ability of a system to carry out the actions necessary to achieve or to maintain a defined safe state for the equipment / machinery / plant / apparatus under control of the system
- **Basic Safety**: The equipment must be designed and manufactured such that it protects against risk of damage to persons by electrical shock and other hazards and against resulting fire and explosion. The protection must be effective under all conditions of the nominal operation and under single fault condition
- **Safety Assessment**: The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems
- **Fail-Safe State**: State corresponding to the device failing to detect a ground connection and/or the state where the device output relay contacts correspond to the de-energized state of the relay.
- **Fail Safe**: Failure that causes the relay contacts to go to the defined fail-safe state without a demand from the process.
- **Fail Dangerous**: Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
- **Fail Dangerous Undetected**: Failure that is dangerous and that is not being diagnosed by the device.
- **Fail Dangerous Detected**: Failure that is dangerous but is detected by the device.
- **Fail Annunciation Undetected**: Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic and is not detected by another diagnostic.
- **Fail Annunciation Detected**: Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic or false diagnostic indication.
- **Fail No Effect**: Failure of a component that is part of the safety function but that has no effect on the safety function.
- **Low Demand Mode**: Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
1.2 **Acronyms**

- **FMEDA**: Failure Modes, Effects and Diagnostic Analysis
- **HFT**: Hardware Fault Tolerance
- **MOC**: Management of Change. These are specific procedures often done when performing any work activities in compliance with government regulatory authorities.
- **PFD AVG**: Average Probability of Failure on Demand
- **SFF**: Safe Failure Fraction, the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault.
- **SIF**: Safety Instrumented Function, a set of equipment intended to reduce the risk due to a specific hazard (a safety loop).
- **SIL**: Safety Integrity Level, discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems where Safety Integrity Level 4 has the highest level of safety integrity and Safety Integrity Level 1 has the lowest.
- **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).

1.3 **Product Support**

**Product support can be obtained from:**
Scully Signal Company, 70 Industrial Way, Wilmington, Massachusetts
(617) 692-8600 / (800) 272-8559 / www.scully.com

1.4 **Related Literature**

The Technical Manual provided with the product contains information critical to the functional safety of the ST-47 Groundhog. That manual provides key specifications for the product and procedures which are pertinent to the proper installation and maintenance of the product. The options for the ground detection and enclosures are also outlined in the Technical manual.

**Guidelines/References:**
- Safety Integrity Level Selection – Systematic Methods Including Layer of Protection Analysis, ISBN 1-55617-777-1, ISA
- Safety Instrumented Systems Verification, Practical Probabilistic Calculations, ISBN 1-55617-909-9, ISA

1.5 **Reference Standards**

**Functional Safety:**
- ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.) Functional Safety – Safety Instrumented Systems for the Process Industry Sector
2.1 **Safety Function**

As part of the safety instrumented function the Intellitrol system will be configured such that when the output relay opens the Safety Instrumented Function will go to the safe state (no permit state). An Intellitrol system consists of a cabinet, Sculcon junction box, and one or more sensors. The output of the Intellitrol can be used to directly actuate a safety valve or it can be used as an input to a safety rated logic solver.

2.2 **Environmental limits**

The designer of a SIF must check that the product is rated for use within the expected environmental limits. Refer to the Intellitrol Technical Manual for environmental limits.

2.3 **Design Verification**

A detailed Failure Mode, Effects, and Analysis (FMEA) report is available from Scully Signal Company. This report details all failure rates and failure modes.

The achieved Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) design must be verified by the designer via a calculation of PFDAVG considering architecture, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements. To model multi-channel systems, a technique such as Markov modeling is recommended to properly account for common failure modes.

The failure rate data listed in the FMEA report is only valid for the useful life time of an Intellitrol module. The failure rates will increase sometime after this time period. Reliability calculations based on the data listed in the FMEA report for mission times beyond the lifetime may yield results that are too optimistic, i.e. the calculated Safety Integrity Level will not be achieved.

2.4 **SIL Capability**

2.4.1 **Systematic Integrity**

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer. A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than the statement without “prior use” justification by end user or diverse technology redundancy in the design.

2.4.2 **Random Integrity**

The Intellitrol is a Type B Device. Therefore based on the SFF between 90% and 99% the design can meet SIL 2 @ HFT=0.

2.4.3 **Safety Parameters**

For detailed failure rate information refer to the Failure Modes, Effects and Analysis Report for the Intellitrol.
2.5 General Requirements

The Intellitrol will transition from the permit state to the non permit state within 450ms of a sensor wet or fault condition when used within the specified ambient temperature range of -40 degrees to +120 degrees Fahrenheit.

All SIS components including the Intellitrol must be operational before process start-up.

Personnel performing maintenance and testing on the Intellitrol shall be competent to do so.

Results from the proof tests shall be recorded and reviewed periodically.
3.1 **Installation**  
The Intellitrol module must be installed per standard practices outlined in the Technical Manual.

The environment must be verified to not exceed the ratings.

The Intellitrol must be accessible for physical inspection.

3.2 **Physical Location and Placement**  
The Intellitrol shall be accessible with sufficient room for electrical connections and shall allow manual proof testing.

The Intellitrol shall be mounted in a low vibration environment. If excessive vibration can be expected special precautions shall be taken to ensure the integrity of the connectors or the vibration should be reduced using appropriate damping mounts.
4.1 **Proof test**

The objective of proof testing is to detect failures within a Scully Signal Company Overfill Prevention Control Monitor that are not detected by any automatic self-check diagnostics of the system. Of main concern are undetected failures that prevent the safety instrumented function from performing its intended function.

The frequency of proof testing, or the proof test interval, is to be determined in reliability calculations for the safety instrumented functions for which a Scully Signal Company Overfill Prevention Control Monitor is applied. The proof tests must be performed more frequently than or as frequently as specified in the calculation in order to maintain the required safety integrity of the safety instrumented function.

The following proof test is recommended. The results of the proof test should be recorded and any failures that are detected and that compromise functional safety should be reported to Scully Signal Company. The suggested proof test consists of:

- Sensor wire open
- Sensor wet condition
- Sensor wire shorted to ground

And for units with ground proving enabled:

- Ground open
- Ground ball / ground bolt, if jumpered, shorted to ground

And for units with deadman enabled:

- Deadman open

4.2 **Proof Test Procedure**

The suggested proof test consists of an electrical test of each monitored input. Separate proof testing is required for each plug type connected to the Intellitrol. See Table 1 to 3 for the steps to perform manual testing using a Scully rack test unit. Scully personnel will typically utilize a test unit which will automate these steps. If Vehicle Identification Proving (VIP) is enabled on the Intellitrol, the serial number of the tester must be added to the Intellitrol’s TIM list or the VIP disabled during the proof test.
### Table 1: Proof Test for Green Plug 2 or 4 J-Slot/Locking Pin (2-Wire Sensors)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Set the tester for 2-wire and all 2-wire switches in a dry/thermistor position. Place the Ground switch in the appropriate position of Resistor or Ground Bolt/Ball based on the Intellitrol ground jumper position. Connect the Intellitrol to the tester. When a deadman switch is connected confirm that the control module is indicating a permit condition (green bar illuminated) with the switch closed and a no permit (red bar illuminated) with the switch open. NOTE: If the Intellitrol is jumpered for 6 compartments, switches 1 and 2 will have no effect. This is normal operation.</td>
</tr>
<tr>
<td>2</td>
<td>If a deadman switch is connected, confirm that the control module is indicating a permit condition (green bar illuminated) with the switch closed and a nonpermit condition (red bar illuminated) with the switch open. The deadman switch must be closed in the remaining steps.</td>
</tr>
<tr>
<td>3</td>
<td>For each optic sensor switch, one at a time, move the switch to the wet position and verify the Intellitrol goes to a non-permissive state then reposition the switch to dry. Verify the Intellitrol returns to the permissive state.</td>
</tr>
<tr>
<td>4</td>
<td>Hold the SHORT switch in the SHORT position for several seconds and verify the correct Intellitrol response. If the Intellitrol is jumpered for ground proving and Ground Bolt the Intellitrol will go non-permissive and the red ground light will be illuminated while the switch is held in the SHORT position. A short will also cause a non-permissive output due to a VIP fault making it critical to verify the ground light as well as the non-permissive light bar.</td>
</tr>
<tr>
<td>5</td>
<td>Move the GROUND switch to the open position and verify the correct Intellitrol response. The Intellitrol, if jumpered for ground proving, will go non permissive and the red ground light will be illuminated.</td>
</tr>
<tr>
<td>6</td>
<td>Disconnect the Intellitrol from the tester.</td>
</tr>
</tbody>
</table>
### Table 2: Proof Test for Blue Plug 3J-Slot/Locking Pin (5-Wire Sensors)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Set the tester for 5-wire and with 5-wire switch in a dry position. Place the Ground switch in the appropriate position of Resistor or Ground Bolt/Ball based on the Intellitrol ground jumper position. Connect the Intellitrol to the tester and confirm that the control module is indicating a permit condition (green bar illuminated).</td>
</tr>
<tr>
<td>2</td>
<td>If a deadman switch is connected, confirm that the control module is indicating a permit condition (green bar illuminated) with the switch closed and a nonpermit condition (red bar illuminated) with the switch open. The deadman switch must be closed in the remaining steps.</td>
</tr>
<tr>
<td>3</td>
<td>Move the 5-wire switch to the wet position and verify the Intellitrol goes to a non-permissive state (red bar illuminated) then reposition the switch to dry. Verify the Intellitrol returns to the permissive state.</td>
</tr>
<tr>
<td>4</td>
<td>Hold the SHORT switch in the SHORT position for several seconds and verify the correct Intellitrol response. If the Intellitrol is jumpered for ground proving and Ground Bolt the Intellitrol will go non-permissive and the red ground light will be illuminated while the switch is held in the SHORT position. A short will also cause a non-permissive output due to a VIP fault making it critical to verify the ground light as well as the non-permissive light bar.</td>
</tr>
<tr>
<td>5</td>
<td>Move the GROUND switch to the open position and verify the correct Intellitrol response. The Intellitrol, if jumpered for ground proving, will go non-permissive and the red ground light will be illuminated.</td>
</tr>
<tr>
<td>6</td>
<td>Disconnect the Intellitrol from the tester.</td>
</tr>
</tbody>
</table>
### Table 3: Proof Test for 4 J-Slot/Locking Pin Black Plug (2-Wire and 5-Wire Sensors)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Set the tester for 2-wire and all 2-wire switches in a dry/thermistor position. Place the Ground switch in the appropriate position of Resistor or Ground Bolt/Ball based on the Intellitrol ground jumper position. Connect the Intellitrol to the tester and confirm that the control module is indicating a permit condition (green bar illuminated). NOTE: If the Intellitrol is jumpered for 6 compartments, switches 1 and 2 will have no effect. This is normal operation.</td>
</tr>
<tr>
<td>2</td>
<td>If a deadman switch is connected, confirm that the control module is indicating a permit condition (green bar illuminated) with the switch closed and a nonpermit condition (red bar illuminated) with the switch open. The deadman switch must be closed in the remaining steps.</td>
</tr>
<tr>
<td>3</td>
<td>For each optic sensor switch, one at a time, move the switch to the wet position and verify the Intellitrol goes to a non-permissive state (red bar illuminated) then reposition the switch to dry. Verify the Intellitrol returns to the permissive state.</td>
</tr>
<tr>
<td>4</td>
<td>Disconnect the Intellitrol from the tester, change the tester to 5-Wire mode, and reconnect the tester. Confirm that the control module is indicating a permit condition (green bar illuminated).</td>
</tr>
<tr>
<td>5</td>
<td>Move the 5-wire switch to the wet position and verify the Intellitrol goes to a non-permissive state (red bar illuminated) then reposition the switch to dry. Verify the Intellitrol returns to the permissive state.</td>
</tr>
<tr>
<td>6</td>
<td>Hold the SHORT switch in the SHORT position for several seconds and verify the correct Intellitrol response. If the Intellitrol is jumpered for ground proving and Ground Bolt the Intellitrol will go non-permissive and the red ground light will be illuminated while the switch is held in the SHORT position. A short will also cause a non-permissive output due to a VIP fault making it critical to verify the ground light as well as the non-permissive light bar.</td>
</tr>
<tr>
<td>7</td>
<td>Move the GROUND switch to the open position and verify the correct Intellitrol response. The Intellitrol, if jumpered for ground proving, will go non-permissive and the red ground light will be illuminated.</td>
</tr>
<tr>
<td>8</td>
<td>Disconnect the Intellitrol from the tester.</td>
</tr>
</tbody>
</table>

The person(s) performing the proof test of an Intellitrol unit should be trained in SIS operations, including bypass procedures, and Intellitrol maintenance. No special tools, other than the rack tester, are required.
4.3 Repair and replacement
Repair procedures in the Intellitrol Technical Manual must be followed.

4.4 Useful Life
The useful life of the Intellitrol is 10 years.

4.5 Scully Signal Company Notification
Any failures that are detected and that compromise functional safety should be reported to Scully Signal Company. Please contact Scully Signal Company customer service.
Overfill Prevention Control Unit (with Ground Verification & Vehicle Identification Option)

Notes:
For over seventy-five years Scully has been engineering and building products to the highest safety and reliability standards. We design and manufacture all of our systems under one roof to ensure complete quality control over our manufacturing and testing operations. Scully is ISO certified and all of our products are 100% made in the U.S.A. In addition, we back up our products with the best service in the industry. We have direct sales and service personnel in the U.S.A., The United Kingdom, and Europe and are represented in over 50 countries.

For more information and 24 hour technical assistance, call Scully Signal Company at 1-800-2SCULLY (1-800-272-8559).

Scully Headquarters in Wilmington, MA U.S.A.

Copyright © 2014 Scully Signal Company. MaxSafety, Sculcon and Scully are registered trademarks of Scully Signal Company. The names and logos of other companies mentioned herein may be trademarks of their respective owners. This document is for informational purposes only. Scully makes no warranties, expressed or implied, in this document. All Rights Reserved. Specifications are subject to change without notice.