What is PROFIsafe and how does it work?

Pete Brown
Siemens I CS
“The condition of being safe; freedom from danger, risk, or injury.”

In the UK (and Europe) this can cover many areas and industries, for example:

- Supply of Machinery (Safety) Regulations
- Electromagnetic Compatibility Regulations
- Electrical Equipment (Safety) Regulations
- Pressure Equipment Regulations
- Simple Pressure Vessels (Safety) Regulations
- Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres Regulations
- Lifts Regulations
- Medical Devices Regulations
- Gas Appliances (Safety) Regulations

Important: It is essential to have some form of risk assessment / risk analysis
e.g. HAZAN / HAZID / HAZOP / RA to ISO 12100
PROFIsafe – The Vision

Coexistence of standard and failsafe communication

F-Host/FPLC

Standard-I/O

F-I/O

Standard-Host/PLC

Profibus DP

PG/ES with secure access e.g. Firewall

TCP/IP

Engineering Tool

F-Sensor

F-Field-Device

F-Actuator

Master-Slave Assignment

Other Safety-Bus

F-Gateway

Repeater

F = Failsafe

Peter Brown / What is PROFIsafe?
Peter Brown / What is PROFIsafe?

Cyclic Communication

1:1 Communication relationship between master and slave

F-Host / FPLC

Bus cycle

Laserscanner

Standard-I/O

F-I/O

Drive with integrated Safety
"Black Channel": ASICs, Links, Cables, etc. Not safety relevant

Non safety critical functions, e.g. diagnostics

"PROFIsafe": Safety critical communications systems: Addressing, Watch Dog Timers, Sequencing, Signature, etc.

Safety relevant, Not part of the PROFIsafe: Safety I/O / Safety Control Systems
PROFIsafe – Add-on Strategy

Standard engineering tool STEP 7 + Failsafe engineering Tool Distributed Safety

Standard CPU + Failsafe Application Program

Standard Remote I/O + Failsafe I/O Modules

Standard PROFIBUS DP + PROFIsafe

Peter Brown / What is PROFIsafe?
Coexistence of standard program and safety-related program on one CPU

- Changes to the standard program have no effect on the integrity of the safety-related program section.
PROFIsafe – Coded Processing

Coded Processing

Time redundancy and diversity replace complete redundancy

Operators → A, B → Operation (AND) → C → Output

Coding → /A, /B

Diverse Operators

Comparison → D = /C → Diverse Output

Stop by D ≠ /C

Peter Brown / What is PROFIsafe?
Safety-oriented communication via PROFIsafe
First standard of communication in accordance with safety standard IEC 61508
PROFIsafe supports safe communication for the open standard PROFIBUS and PROFINET
The PROFIsafe meets possible faults like address error, delay, data loss with
- Serial numeration of PROFIsafe-telegram
- Time monitoring
- Authenticity monitoring via unique addresses
- Optimized CRC-checking

PROFIsafe supports standard- and failsafe Communication by one medium

Peter Brown / What is PROFIsafe?
Overview: Possible Errors and detection mechanism

<table>
<thead>
<tr>
<th>Failure type:</th>
<th>Remedy:</th>
<th>Consecutive Number</th>
<th>Time Out with Receipt</th>
<th>Codename for Sender and Receiver</th>
<th>Data Consistency Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repetition</td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deletion</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Insertion</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Resequencing</td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Corruption</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Delay</td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Masquerade (standard message mimics failsafe)</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Revolving memory failure within switches</td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PROFIsafe safety PDU

Standard PROFINET IO messages

<table>
<thead>
<tr>
<th>F Input/Output Data</th>
<th>Status / Control Byte</th>
<th>CRC2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>across F I/O data, Status or Control Byte, F-Parameter, and Vconsnr_h</td>
<td></td>
</tr>
<tr>
<td>Max. 12 / 123 Bytes</td>
<td>1 Byte</td>
<td>3/4 Bytes *)</td>
</tr>
</tbody>
</table>

PROFIsafe container = Safety PDU

*) 3 Bytes for a max. of 12 Byte F I/O data
4 Byte for a max. of 123 Bytes F I/O data
Extended Consecutive Number (24 Bit)

Example:

### Synchronization via "Toggle Bit"

<table>
<thead>
<tr>
<th>F Input data</th>
<th>Status Byte</th>
<th>CRC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. 12 / 123 Bytes</td>
<td>1 Byte</td>
<td>3 / 4 Bytes</td>
</tr>
</tbody>
</table>

- **Vconsnr_d**
  - (F-Device) Consecutive Number (not transmitted)
  - 0,1...0FFFFFFFFh
  - 3 Bytes

- **24/32 Bit CRC Signature**
  - Include Vconsnr_d within CRC2 calculation (see calculation details)

- **Toggle_h**
  - (Bit 5 of the Control Byte)
  - Increment

- **R_cons_nr**
  - (Bit 2 of the Control Byte)
  - Reset

- **24 Bit consecutive number**

Virtual consecutive numbering = patented
Which protocol must be supported?

- F-DI: Fail-safe digital input
- F-DO: Fail-safe digital output
- IO-C: PROFINET IO-Controller

PROFINET - PROFIBUS - PROFIsafe - Introduction
Which protocol version applies when?

Goal: 100% compatibility

- A PROFIsafe slave which supports the v2 mode must be able to replace an older version of this PROFIsafe slave which only supports the v1 mode without the need of any adaption.

<table>
<thead>
<tr>
<th>PROFIsafe V2 Slave used in</th>
<th>Protocol with 8Bit-Counter (= PROFIsafe V1 mode)</th>
<th>Protocol with 24Bit-Counter (= PROFIsafe V2 mode)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROFIBUS network only</td>
<td>mandatory</td>
<td>mandatory</td>
</tr>
<tr>
<td>PROFINET network only</td>
<td>-</td>
<td>mandatory</td>
</tr>
<tr>
<td>PROFIBUS / PROFINET network</td>
<td>mandatory</td>
<td>mandatory</td>
</tr>
</tbody>
</table>
PROFIsafe - Introduction

Which protocol version applies when?

PROFINET – PROFIsafe V2

PROFIBUS – PROFIsafe V1 or V2

V1 = PROFIsafe Profil V1
V2 = PROFIsafe Profil V2

Peter Brown / What is PROFIsafe?
Handling
Functional
Safety

Modern Requirements and Best Practice
‘Drivers’ for Safety

- **Legislation:** “I need to do something……but what?”

- **Fear:** “What are my responsibilities and am I doing enough…. Or too much?”

- **Compliance:** “Can I prove I have done as much as is reasonably practicable”

- **Operational Efficiency:** “Can I produce products safely with maximum efficiency?”

- **Cost:** “Am I getting the best return on my investment” *(FFI)*

- **Support:** “I want advice based on solutions not products”
What is Functional Safety?

Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs. Functional safety is achieved when every specified safety function is carried out and the level of performance required of each safety function is met.

Functional safety relies on **active systems**.

Safety achieved by measures that rely on **passive systems** is not functional safety.
Systematic Failures

Definition of a systematic failure:

*failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors*

Examples of systematic failures include human error in:

- The safety requirement specification;
- The design, manufacture, installation or operation of the hardware;
- The design and / or implementation of the software.
Focus: Product Manufacture

IEC 61508

Focus: Integration

IEC 61511
IEC 62061
ISO 13849

Relevant good practice

Harmonized standards

Process Industry
Manufacturing Industry

EN 954 (until 2011)
Basic Lifecycle Concept

Functional Safety

Control of dangerous failures during operation through *Robust Design*

Control and avoidance of systematic failures through *Robust Processes*

Safety Lifecycle Requirement

Engineering / Design
System Architecture
Failure Probability

Planning / Processes
Safety Management
Verification / Responsibilities
Verification and Validation

**Verification (in general) =**
“Are you making it right?”
Verification is the process used to evaluate whether or not a system complies with regulations / specifications / conditions imposed at the start of a phase.

**Validation (in general) =**
"Are you making the right thing?“
Validation is the process of establishing evidence (including functional testing) that provides a high degree of assurance that a system accomplishes its intended requirements (Fit for purpose).
Simplified Safety Lifecycle

- Hazard and Risk Assessment
- Design and Engineering
- Installation, Validation and Start-up
- Operation and Maintenance
- Modernisation and Upgrade
Security for Industrial Automation

Considering the PROFINET Security Guideline
**Industrial IT Security**

- **Plant Security**
  - **Physical Security**
    - Physical access to facilities and equipment
  - **Policies & Procedures**
    - Security management processes
    - Operational Guidelines
    - Business Continuity Management & Disaster Recovery

- **Network Security**
  - **Security Zones & DMZ**
    - Secure architecture based on network segmentation
  - **Firewalls and VPN**
    - Implementation of Firewalls as the only access point to a security cell

- **System Integrity**
  - **System Hardening**
    - Adapting system to be secure by default
  - **User Account Management**
    - Access control based on user rights and privileges
  - **Patch Management**
    - Regular implementation of patches and updates
  - **Malware Detection and Prevention**
    - Anti Virus and Whitelisting

*DCS: Distributed Control System
SCADA: Supervisory Control and Data Acquisition*
What is IT Security? (Cyber/Network)

- Protection of computers and networks from intrusion and disruption
- With so many systems relying on networks this is critical
- The internet allows global connectivity and all its advantages
- These advantages lead to vulnerability
Why do I need IT Security?

- Intrusion can be malicious or accidental
- Governments are concerned by terrorist acts
- Business is concerned by industrial espionage and theft
- Ex employees may have a grudge
- Current employees can be careless
- Computer viruses can attack PLCs
- Network intrusions are on the increase – The damage can be catastrophic
How do I implement IT Security?

- CPNI recommendations
- Risk analysis and policies
- Industrial grade equipment
- PROFINET / PROFINET Security Guideline
- (ICS CERT recommendations)

Industrial Security Homepage:
The PROFINET Security Concept
From the PROFINET Security Guideline

- Network Architecture – Security Zones
- Trust Concept – within Zones
- Perimeter Defence – Firewall/VPN
- Provision of Confidentiality and Integrity
- Transparent Integration of Firewalls
Secure Automation Cells (Zones)

Complete plant security

Secure automation cells

Peter Brown / IT Security for Industrial Automation
Security issues and vulnerabilities need to be addressed

There are many methods

How can we address these vulnerabilities using these techniques:

- **Firewall**
  - Protect against unauthorized access

- **VLAN (Virtual Local Area Network)**
  - Logical network that operates on the basis of a physical network

- **DMZ (De-Militarized Zone)**
  - Exchange data with external partners via safe areas

- **VPN (Virtual Private Network)**
  - Secure tunnel between authenticated users
‘to literally have everything imaginable connected to a network so that information from all these “things” can be stored, transferred, analysed and acted upon in new, and usually automated ways via network connections with everything else’.

- The hazards and risk aren’t changing
- Monitoring of safety actions / events
- Analysing of trends (OEMs)
- Distributed systems and controls (smaller)
- More inter-connected devices
- Mechatronics
- 100% security?
- ‘Independence’ of functional safety systems