PROFI safe: Functional Safety with PROFI BUS and PROFI NET

Jayanthreddy Donthireddy
Outline

- What is PROFIsafe
- Why Do We Need Functional Safety in Automation?
- Dichotomy of Standard and Functional Safety Automation
- Motivation and Objectives for PROFI BUS and PROFI NET
- PROFI safe, the Solution
- Beyond Functional Safety Communication
Outline

- What is PROFIsafe
- Why Do We Need Functional Safety in Automation?
- Dichotomy of Standard and Functional Safety Automation
- Motivation and Objectives for PROFI BUS and PROFI NET
- PROFIsafe, the Solution
- Beyond Functional Safety Communication
What is PROFI safe

- It is an integrated safety technology for use in all sectors of discrete manufacturing and process automation. It is independent of the communication method and provides cost-effective and flexible functional safety.

- With 4.1 Million installed nodes the PROFI safe technology has established itself in the market in a leading position in fieldbus-based safe communication systems.
Outline

- What is PROFIsafe
- Why Do We Need Functional Safety in Automation?
- Dichotomy of Standard and Functional Safety Automation
- Motivation and Objectives for PROFIBUS and PROFINET
- PROFI safe, the Solution
- Beyond Functional Safety Communication
Why Do We Need Functional Safety in Automation?

- Any active industrial process is more or less associated with the risk of
  1. Injuring or killing people
  2. Destroying nature
  3. Damaging investments

- With most of the processes, it is quite easy to avoid risk without special requirements imposed on automation systems. However, there are typical applications associated with high risk

- That means the failure, or error rate, of the standard automation technology under normal circumstances is acceptable for normal modes of operations, but not sufficient for the safety critical applications.
Outline

- What is PROFI safe
- Why Do We Need Functional Safety in Automation?
- **Dichotomy of Standard and Functional Safety Automation**
- Motivation and Objectives for PROFIBUS and PROFINET
- PROFI safe, the Solution
- Beyond Functional Safety Communication
Dichotomy of Standard and Functional Safety Automation

- In the past decades, microcontrollers, software, personal computers, and communication networks have dramatically influenced the automation area, leading to cost reduction, higher flexibility, and availability.

- But adding classical safety to modern automation solutions leads to increased cost due to additional wiring and need for engineering, to less flexibility and availability than expected, and to other disadvantages.

- Microcontrollers and software have been in a widespread use in diverse industrial automation applications. The preconditions for their use in safety applications were introduced in the international standard IEC 61508, with its different safety integrity levels, from SIL1 to SIL4.
Outline

- What is PROFI safe
- Why Do We Need Functional Safety in Automation?
- Dichotomy of Standard and Functional Safety Automation
- Motivation and Objectives for PROFI BUS and PROFI NET
- PROFI safe, the Solution
- Beyond Functional Safety Communication
Motivation and Objectives for PROFI BUS and PROFI NET

- The necessary means for safety applications on PROFI BUS DP & PROFI NET IO are to provide a similar flexibility and availability also for powerful functional safety devices like remote I/O, laser scanners, light curtains, level switches, shutdown valves, drives, robots, and alike.

- The requirement was that neither cables, and layer stack software nor other communication devices such as repeaters, links, and couplers should be changed.

- PROFI BUS DP and PROFI NET IO fall in the category of the so-called defined transmission systems, with configured and well-known participants and transmission properties, the preconditions of functionally safe communication.
Motivation and Objectives for PROFI BUS and PROFI NET (Contd.)

The PROFIsafe vision
Motivation and Objectives for PROFI BUS and PROFI NET (Contd.)

- Safe communication could be achieved by using redundant transmission lines and cross-checking as a basis for safety functions. However, the working group opted for a single-channel solution. The redundancy can still be added to the system as an option to provide additional higher availability/reliability for the operational functions.

<table>
<thead>
<tr>
<th>Application</th>
<th>PROFIBUS DP PROFINET IO</th>
<th>PROFI safe</th>
<th>Redundancy</th>
<th>PROFI safe and Redundancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>High availability</td>
<td>Suitable for all kinds of distributed automation</td>
<td>Factory and process automation: presses, robots, level switches, shutdown valves, burner control, cable cars, etc.</td>
<td>Process automation: chemical or pharmaceutical productions, refineries, offshore, etc.</td>
<td>Process automation: chemical or pharmaceutical productions, refineries, offshore, etc.</td>
</tr>
<tr>
<td>Functional safety</td>
<td>—</td>
<td>Prevent hazards through safety functions (required by laws or insurances)</td>
<td>Redundancy by itself does not provide functional safety</td>
<td>Prevent hazards through safety functions (required by laws or insurances)</td>
</tr>
</tbody>
</table>

Safety and Redundancy Options
Outline

- What is PROFI safe
- Why Do We Need Functional Safety in Automation?
- Dichotomy of Standard and Functional Safety Automation
- Motivation and Objectives for PROFI BUS and PROFI NET
- **PROFI safe, the Solution**
- Beyond Functional Safety Communication
PROFI safe, the Solution

Concept

- PROFIBUS DP and PROFINET IO, like most of the fieldbus systems, employ only the layers 1, 2, and 7 of the ISO/OSI model, only for real-time applications. In order to avoid any changes to any of these layers, the safety measures were added as a safety layer on top of layer 7, thus increasing the size of the OSI application layer by some kilobytes.

- Since the safety layer is only responsible for the transport of safety-related user, or process data, it takes the remaining parts of the (safety and) application layer to acquire and process these data.

- The safety-augmented process data are called a PROFI safe PDU. Ideally, a PROFI safe PDU shall be passed as a whole, and completely unmodified, from a (safety) sender to a (safety) receiver no matter what kind of transmission system both are using.
**PROFI safe, the Solution (Contd.)**

- **Black Channel**
  - A transmission system from one safety node to another is called a black channel.
  - The chosen communication technology does not matter except for a few basic constraints to be discussed later on in this chapter. Another implication is that none of the error detection mechanisms of the chosen communication technology is employed to guarantee the integrity of the transferred process data.
  - PROFI safe also employs the black channel principle for complex PROFIBUS DP and PROFINET IO structures.
PROFI safe, the Solution (Contd.)

- Black Channel (Contd.)

Complete communication paths for PROFI safe PDUs.
Possible Transmission Errors and Their Remedies

- Various errors may occur when messages are transferred in network topologies of the described complexity, be it due to hardware failures, extraordinary electromagnetic interference (EMI), or other influences.

- Message of a logical connection between two PROFIsafe safety nodes can be lost, occur repeatedly, or mirrored (loopback), be inserted from somewhere else, appear delayed, in an incorrect sequence, out-of-sequence due to storage elements in the network and/or show corrupted data.
PROFI safe, the Solution (Contd.)

Possible Transmission Errors and Their Remedies (Contd.)

Out of the numerous remedies known from literature, PROFI safe focuses on those presented in the matrix shown in the table.

These include the following:

1. The numbering of the PROFI safe PDUs (sign-of-life)
2. A time expectation with acknowledgment (watchdog)
3. A Codename between sender and receiver for each direction (password)
4. Data integrity checks (cyclic redundancy check [CRC])
PROFIsafe, the Solution (Contd.)

- Possible Transmission Errors and Their Remedies (Contd.)

Black channel and PROFIsafe properties of logical connections.

Black Channel Error Types and Safety Measures of PROFIsafe

<table>
<thead>
<tr>
<th>Communication Errors</th>
<th>Monitoring Number (Virtual)</th>
<th>Timeout with Receipt</th>
<th>Codename for Sender and Receiver</th>
<th>Data Integrity Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corruption</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Unintended repetition</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incorrect sequence</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unacceptable delay</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insertion</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Masquerade</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Addressing</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Out-of-sequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loopback of messages</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PROFI safe, the Solution (Contd.)

Possible Transmission Errors and Their Remedies (Contd.)

The following so-called *proper* polynomials are chosen for the usage with PROFI safe \((r = \text{length of the CRC signature})\):

- \(r = 16\) Bit: \(0x4EAB\)
- \(r = 24\) Bit: \(0x5D6DCB\)
- \(r = 32\) Bit: \(0xF4ACFB13\)
SIL

- Safety integrity level (SIL) is defined as a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a safety instrumented function (SIF).

- Assignment of SIL is an exercise in risk analysis

- There are several methods used to assign a SIL. These are normally used in combination, and may include:
  - Risk matrices
  - Risk graphs
  - Layers of protection analysis (LOPA)
PROFI safe, the Solution (Contd.)

SIL (contd.)

- There are several problems inherent in the use of safety integrity levels. These can be summarized as follows:
  - Poor harmonization of definition across the different standards bodies which utilize SIL
  - Process-oriented metrics for derivation of SIL
  - Estimation of SIL based on reliability estimates
  - System complexity, particularly in software systems, making SIL estimation difficult to impossible

- The following standards use SIL as a measure of reliability and/or risk reduction.
  1. ANSI/ISA S84 (Functional safety of safety instrumented systems for the process industry sector)
  2. IEC EN 61508 (Functional safety of electrical/electronic/programmable electronic safety related systems)
  3. IEC 61511 (Safety instrumented systems for the process industry sector)
  4. EN 50128 (railway applications – software for railway control and protection)
  5. EN 50129 (railway applications – safety related electronic systems for signalling)
  6. EN 50402 (fixed gas-detection systems)
  7. ISO 26262 (automotive industry)
PROFIsafe, the Solution (Contd.)

- SIL Monitor

  PROFIsafe is not relying on the basic data integrity checks of PROFIBUS DP, or PROFINET IO, or other transmission mechanisms.

  The entire error detection necessary to attain the required SIL (in factory automation usually SIL3 as the maximum --- 7 9s) is advantageously only implemented in the superimposed PROFIsafe protocol.

Examples of proper and improper generator polynomials
PROFI safe, the Solution (Contd.)

- SIL Monitor (Contd.)

  A Mechanism was created that guarantees the compliance with SIL levels over the service life of a distributed safety-related automation solution, irrespective of the employed components and the configuration.
PROFI safe Parameters

- The configuration part of an engineering tool uses the electronic General Station Description (GSD) of particular F-Device-Slave to arrange for the format of the standard process data to be transferred within the PDU of a message between a PROFINET IO controller–PROFIBUS DP master and its PROFINET IO device–PROFIBUS DP slave. The same happens in case of PROFI safe PDUs.

- There are two groups of safety-related parameters. The F parameters (F-Parameter) are associated with the PROFI safe protocol layer and the i (= individual) parameters (iParameter) with the individual safety related technology firmware of a safety device.
PROFI safe, the Solution (Contd.)

PROFI safe Parameters (Contd.)

PROFIBUS DP message structure.

PROFINET IO message structure.
PROFI safe, the Solution (Contd.)

- **Structure of PROFI safe PDUs**
  
  - The PROFI safe protocol is located on top of the fieldbus application layer and realized in the form of state machines on the sender (F-Host*) as well as on the receiver side (F-Device) to cover start-up, regular, and error behavior.

  - The structures of the PROFI safe PDUs from F-Host and F-Device are symmetrical. The F-Host sends F-Output data (in case of actuators) and the F-Device returns F-Input data (in case of sensors). The maximum length in both cases is 13 bytes.

  - As mentioned already, PROFI safe uses numbering of PROFI safe PDUs together with a watchdog timer to check Timeliness and Codenames to check Authenticity of the transmitted safety process data. Researches have shown that both numbering and Codename require each 32 bits.
PROFI safe, the Solution (Contd.)

- Structure of PROFI safe PDUs (Contd.)

Implicit method of PROFI safe via Monitoring Number (F-Device).
Structure of PROFI safe PDUs (Contd.)

A special procedure, called MNR-Generator, creates 64-bit-long elements of an exclusive number sequence based on the individual Codename of the particular F-Device and a pseudo random number generator. The initial elements of the sequence are built as follows:

- CNNR_64[1] = f (constant, Codename)
- CNNR_64[2] = CNNR_64[1] \times constant

The cyclically used elements are built as follows (similar to a Fibonacci sequence):

- CNNR_64[0] = CNNR_64[1] + CNNR_64[2]
- CNNR_64[2] = CNNR_64[1]
- CNNR_64[1] = CNNR_64[0]
PROFI safe, the Solution (Contd.)

- Structure of PROFI safe PDUs (Contd.)

  Principle of the disjoint and random Monitoring Numbers

Mastering propagation times.
Outline

- What is PROFI safe
- Why Do We Need Functional Safety in Automation?
- Dichotomy of Standard and Functional Safety Automation
- Motivation and Objectives for PROFI BUS and PROFI NET
- PROFI safe, the Solution
- Beyond Functional Safety Communication
Beyond Functional Safety Communication

- **Safety-Related Programmable Control Logic**
  
  - PROFI safe specifies how to connect any type of F-Host to PROFI safe communications. But it does not dictate how safety-related signals and process values are to be processed within an F-Host.
  
  - The representation in the Continuous Function Chart is well accepted. Approved relay-based safety circuits now can be offered as a standard certified software library.
  
  - The functional safety application software has a time diversity structure; it executes in protected areas where it cannot be influenced by the standard application program.
Commissioning and Repair

- In order to be able to address the individual signals and/or process values during programming, the fieldbus must be configured using an engineering tool.

- In case of F-Devices, additional steps are required supplying the F-Parameters to the PROFI safe layer: Codename, watchdog time, etc.

- During start-up of the fieldbus network, the F-Host with its associated PROFINET IO controller or PROFIBUS DP master sequentially provides all devices with the necessary parameters including F-Parameters before it starts cyclic operation.
Commissioning and Repair (Contd.)

Possible retrofit options with PROFI safe
Beyond Functional Safety Communication (Contd.)

- **Commissioning and Repair (Contd.)**

  - PROFIsafe has shown ways for mastering these tasks—the so-called three-component model that separates the responsibilities of device manufacturers and system manufacturers by using suitable interfaces.

  - In order to perform diagnostics, it uses a proprietary parameterization and diagnostics program. The program could also be routed to the F-Device using acyclic services of PROFIBUS DP or PROFINET IO that are accessible via the Tool Calling Interface or FDT/DTM interface technology.

  - Together with the network configuration and F-Parameterization of an F-Slave/F-Device with the help of the engineering tool, an associated iPar-Server function is instantiated.
Beyond Functional Safety Communication (Contd.)

- Commissioning and Repair (Contd.)

The iPar-Server for fast device replacement.
Beyond Functional Safety Communication (Contd.)

- **Availability**

  - The availability plays a significant role in safety technology. It is a precondition. There is too much of a risk that a frequent—and apparently groundless—trip of the safety devices causes the system to shutdown (Bhopal effect). There are mainly five areas that influence the availability of a system:

    1. Design—assembly of the devices
    2. Facility layout and installation
    3. Operating conditions
    4. Reliability of the components (bathtub curve)
    5. Requirements for operator actions

  - The operating conditions of a system have a strong influence on the reliability—availability. As we all know, a temperature rise of 10 K reduces the service life of an electronic device by 50%.
Beyond Functional Safety Communication (Contd.)

- **Status of PROFI safe-Related Specifications and Guidelines**
  
  - The PROFINET User Organization had published version 1.0 of the PROFI safe specification for PROFINET DP, followed by version 2.0 in September 2005 incorporating PROFINET IO.
  
  - Current version 2.6 covers research results on quantitative considerations for the properties of Timeliness, Authenticity, Data Integrity, and CRC behavior in case of the implicit transmission as described in this publication. (~2013)
  
  - All versions have been confirmed by positive reports from the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) and the worldwide operating Safety-Assessment Organization (TUV).
Beyond Functional Safety Communication (Contd.)

- **Standards Catching Up**
  - The development of PROFI safe is based on IEC 61508, which focuses on safety functions, on quantitative SILs as opposed to qualitative levels in previous safety standards, and on software development procedures and communication.
Peculiarities for Different Industries

- After 15 years and more, PROFI Safe is very well accepted within factory automation. The discussions about the need of using a separate safety bus in addition to the standard fieldbus for the implementation of distributed safety technology are gone in favor of a single cable solution.

- Safety applications in process engineering require a consideration that exceeds the functional safety.

- Communication faults, such as line interruptions or short circuit, were recognizable, the devices were proven-in-use, and safety monitoring was performed in the F-Host system by interpreting redundant signals and voters.
Beyond Functional Safety Communication (Contd.)

- **Peculiarities for Different Industries (Contd.)**

  - To take this into account, PROFI safe communication has been specified compatibly into the existing PA device model. The related specification especially deals with the following topics:
    1. Switching between standard and safety modes
    2. Preparation and commissioning phases
    3. New parameters in the Physical Block of the PA device model
    4. Safety-related data structures for the cyclic data exchange
    5. Configuration data

  - Due to the contingency that parameters have to be edited during operation, particular commission in phases have been designed that permit existing parameter assignment tools based on Electronic Device Descriptions to be used.
Beyond Functional Safety Communication (Contd.)

- Peculiarities for Different Industries (Contd.)

The same field device can be used either as a non-safety-related or as a safety-related field device.
Beyond Functional Safety Communication (Contd.)

- **Test and Certification**
  
  - The PROFI safe mechanisms are based on finite-state machines. Thus, it was possible via a validation tool for finite-state machines to mathematically prove that PROFI safe is working correctly even in cases where more than two independent errors or failures may occur.

The PROFI safe certification procedure.
Beyond Functional Safety Communication (Contd.)

Development Tools and Support

Using PROFIsafe in factory automation with short reaction times, and—on the other hand—in hazardous areas in PA with lowest power dissipation, places contradictory tasks. Since most modern devices use microprocessors, implementing the PROFIsafe procedure in software is an obvious solution.

Generic PROFI safe driver for F-Slaves and F-Devices
Beyond Functional Safety Communication (Contd.)

- **Prospects**
  - The sophisticated safety-related devices mentioned in this publication with its many possibilities to use iParameters to adapt to all kinds of safety applications in a flexible manner are causing the requirement for continuous automatic monitoring of security, safety, and data integrity.

Audit trailing for secured safety parameters.
Thank you!