**Profibus-DP/PA**

**ProfiSafe, Profile for Failsafe Technology, V1.0**

Document No. 740257

**Members of the working group:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eric Dönges</td>
<td>TU München</td>
<td>089-289-23590</td>
</tr>
<tr>
<td>Uwe Grüff</td>
<td>Festo AG</td>
<td>0711-347-4184</td>
</tr>
<tr>
<td>Heinz-Theo Hannen</td>
<td>Hima GmbH &amp; Co. KG</td>
<td>06202-709-286</td>
</tr>
<tr>
<td>Torsten Kühn</td>
<td>Klöckner Moeller GmbH</td>
<td>0228-602-1811</td>
</tr>
<tr>
<td>Gerd Lausberg</td>
<td>Schmersal GmbH &amp; Co.</td>
<td>0202-6474-250</td>
</tr>
<tr>
<td>Dr. Thomas Laux</td>
<td>Wago Kontakttechnik GmbH</td>
<td>0571-887-464/345</td>
</tr>
<tr>
<td>Dr. Wolfgang Stripf</td>
<td>Siemens AG</td>
<td>0721-595-3046</td>
</tr>
</tbody>
</table>

**Working group chairman:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Herbert Barthel</td>
<td>Siemens AG</td>
<td>0911-895-3677</td>
</tr>
</tbody>
</table>
Contents

1 MOTIVATION ........................................................................................................................................ 5
  1.1 TERMINOLOGY .................................................................................................................................. 5

2 INTRODUCTION ..................................................................................................................................... 8
  2.1 POSSIBLE APPLICATION AREAS OF THE SAFETY PROFILE .......................................................... 8
  2.2 REQUIREMENTS PLACED UPON THE SAFETY PROFILE ................................................................. 8
  2.3 PRINCIPLE OF SAFE COMMUNICATIONS (GRAY CHANNEL) ............................................................ 8
  2.4 THE SAFETY PROFILE ....................................................................................................................... 9
  2.5 APPLICATION .................................................................................................................................... 10

3 BASICS OF THE SAFETY PROFILE ...................................................................................................... 11
  3.1 SYSTEM CHARACTERISTICS ............................................................................................................ 11
  3.2 MASTER-SLAVE OPERATION IN PROFIBUS-DP ................................................................................. 11
  3.3 BUS STRUCTURES ............................................................................................................................... 11
  3.4 DELIMITATION OF THE BUS COMPONENTS ..................................................................................... 12
  3.5 DELIMITATION OF THE COMMUNICATION FUNCTIONS .................................................................... 13
  3.6 RISK CONSIDERATION ....................................................................................................................... 13
  3.7 RELEVANT STANDARDS AND DIRECTIVES ...................................................................................... 14
  3.8 ERROR CASES THAT SHALL BE MASTERCED .................................................................................... 15

4 FUNCTIONAL PRINCIPLE OF SAFE COMMUNICATION ........................................................................ 16
  4.1 F MESSAGE STRUCTURE .................................................................................................................. 16
    4.1.1 F Process Data ............................................................................................................................ 17
    4.1.2 Status/Control Byte .................................................................................................................... 18
    4.1.3 Consecutive Number ................................................................................................................... 19
    4.1.4 CRC Signature ............................................................................................................................ 20
    4.1.5 Appended Standard User Data .................................................................................................. 20
  4.2 REGULAR F COMMUNICATION .......................................................................................................... 21
    4.2.1 Operational Behavior of F Host and F Slave ............................................................................... 21
    4.2.2 State Diagrams ............................................................................................................................ 24
  4.3 REACTION IN THE EVENT OF A MALFUNCTION ................................................................................ 30
    4.3.1 Repetition ................................................................................................................................... 30
    4.3.2 Loss .......................................................................................................................................... 30
    4.3.3 Insertion ..................................................................................................................................... 30
    4.3.4 Incorrect Sequence ..................................................................................................................... 30
    4.3.5 Corrupton of F Message Data .................................................................................................... 30
    4.3.6 Delay ....................................................................................................................................... 30
    4.3.7 Interconnecting Safety-Relevant and Standard Messages (Masquerade) .................................. 31
  4.4 F PARAMETER STRUCTURE .............................................................................................................. 31
    4.4.1 F_Device (ProfiSafe Participant) .................................................................................................. 32
    4.4.2 F_Source/Destination_Address (Codename, Password) ............................................................. 32
    4.4.3 F_WD_Time (F Watchdog Time) ................................................................................................ 32
    4.4.4 F_Prm_Flag (Parameters for the Profile Management) .................................................................. 32
    4.4.5 F_Check_SeqNr (Consecutive Number in the CRC2) ................................................................. 32
    4.4.6 F_Check_iPar (CRC1 including i-Parameters) .......................................................................... 32
    4.4.7 F_SIL (SIL Stage) ....................................................................................................................... 33
    4.4.8 F_CRC_Length (Length of the CRC2 Key) .................................................................................. 33
    4.4.9 F_Par_CRC (CRC1 across F-Parameters) .................................................................................. 33
    4.4.10 Structure of the F Parameter Block (Pnm telegram) ................................................................. 34
    4.4.11 F Data Fraction .......................................................................................................................... 34
    4.4.12 i-Parameter (individual F-Device Parameters) ......................................................................... 34
  4.5 F-PARAMETRIZATION ....................................................................................................................... 35
    4.5.1 F-Parametrization Tools ............................................................................................................. 35
    4.5.2 GSD Structure ............................................................................................................................. 36
    4.5.3 F-Parameter Assignment Paths ................................................................................................... 37
4.6 F-STARTUP COORDINATION ................................................................. 38
4.6.1 Standard Startup (F Slave State Machine) ................................................................. 39
4.6.2 Parameter Assignment Deblocking ........................................................................ 39
4.6.3 Interaction Diagrams for Parameter Assignments ............................................. 40
4.7 SAFE ALARM GENERATION ........................................................................ 41
4.8 DIAGNOSIS ............................................................................................... 42
4.9 F MODULE COMMISSIONING / REPAIR BEHAVIOR ................................ 42
4.10 REACTION TIMES .................................................................................. 42
4.11 PROBABILISTIC CONSIDERATIONS ...................................................... 43
4.11.1 Calculations ............................................................................................ 43
4.11.2 Operational Reliability of the Standard Profibus Components .................. 47
4.11.3 Practical Bit Error Rates of the Profibus .................................................... 47

5 USING THE PROFIBUS STANDARD ..................................................................... 48
5.1 PROFIBUS LAYERS 1 AND 2 ................................................................. 48
5.2 PROFIBUS DP .......................................................................................... 48
5.3 DEFINITION OF THE "GRAY" CHANNEL ................................................ 48
5.4 STANDARD EMC REQUIREMENTS OF THE PROFIBUS ................................. 48
5.4.1 CE Mark .................................................................................................. 48
5.4.2 Noise Emission ....................................................................................... 48
5.4.3 Noise Immunity ...................................................................................... 48
5.4.4 On Long Signal Cables >10m ..................................................................... 48
5.4.5 Static Discharge ....................................................................................... 49
5.4.6 High-Frequency Irradiation ....................................................................... 49
5.4.7 HF-Induced Current on Cables and Cable Shields ..................................... 49
5.4.8 Power Supply .......................................................................................... 49
5.4.9 Voltage Dips ........................................................................................... 49
5.4.10 Voltage Interruption ................................................................................ 49
5.4.11 Definition of the Malfunction ................................................................... 49
5.5 STANDARD INSTALLATION GUIDELINES FOR PROFIBUS ...................... 49

6 APPENDIX ...................................................................................................... 50
6.1 MEASURES AGAINST FAILURES BEFORE CRC2 CALCULATIONS ............... 50
6.2 CRC CALCULATION .................................................................................. 51
6.3 SAMPLE GSD FILE FOR A MODULAR F SLAVE .......................................... 53
6.4 APPLICABLE DOCUMENTS ........................................................................ 56
6.5 ABBREVIATIONS ....................................................................................... 56

Figure 2-1 F layer architecture ........................................................................... 9
Figure 2-2 Message model for safety-relevant data ............................................... 9
Figure 3-1 Typical system configuration ............................................................... 11
Figure 3-2 Bus structure ..................................................................................... 12
Figure 3-3 Entire safety function ........................................................................ 12
Figure 3-4 Risk consideration according IEC 61508 ........................................ 13
Figure 3-5 Profibus-DP, proportional risk ............................................................ 13
Figure 4-1 Error mastering measures ................................................................. 16
Figure 4-2 DP frame structure (Process Data) .................................................... 16
Figure 4-3 Complete F message structure ......................................................... 17
Figure 4-4 Modular slave with two F modules .................................................. 18
Figure 4-5 Embedding the F I/O data of compact and modular slaves .......... 18
Figure 4-6 Status byte ....................................................................................... 18
Figure 4-7 Control byte ..................................................................................... 19
Figure 4-8 Consecutive number function .......................................................... 19
Figure 4-9 CRC generation .............................................................................. 20
Figure 4-10  F communication structure .............................................................................................................. 21
Figure 4-11  F User Interfaces of F driver instances ........................................................................................................ 21
Figure 4-12  Monitoring the message transit time  F-CPU ↔ F output ................................................................. 22
Figure 4-13  Monitoring the message transit time  F input ↔ F-CPU ................................................................. 22
Figure 4-14  Interaction F host / F slave during start-up ...................................................................................... 24
Figure 4-15  Interaction F host / F slave during Host Power Off → On .............................................................. 25
Figure 4-16  Interaction F host / F slave with delayed Power On ........................................................................ 25
Figure 4-17  Interaction F host / F slave during Slave Power Off → On ............................................................ 26
Figure 4-18  F host states during interactions with the F slave ............................................................................ 27
Figure 4-19  F output (input) slave states ............................................................................................................. 28
Figure 4-20  Interaction F host / F slave while host recognizes CRC failure ....................................................... 29
Figure 4-21  Interaction F host / F slave while slave recognizes CRC failure .................................................... 29
Figure 4-22  F parameter data and CRC ............................................................................................................. 30
Figure 4-23  F_Prm telegram ............................................................................................................................... 34
Figure 4-24  Safety of individual device parameters ............................................................................................ 35
Figure 4-25  Dynamic i-parameter sets ............................................................................................................... 35
Figure 4-26  Standard device parameter in Profibus ............................................................................................ 36
Figure 4-27  F-parameter assignment for simple F slaves .................................................................................. 37
Figure 4-28  F-parameter assignment for complex F slaves .............................................................................. 38
Figure 4-29  Startup coordination with F parameters ........................................................................................... 39
Figure 4-30  Parameter assignment de-blocking by the F host .......................................................................... 39
Figure 4-31  Assigning "static" i-parameter from F host ....................................................................................... 40
Figure 4-32  Assigning "dynamic" i-parameter from operator level ........................................................................ 41
Figure 4-33  Reaction times ................................................................................................................................. 42
Figure 4-34  Residual error rates .......................................................................................................................... 43
Figure 4-35  Monitoring of corrupted messages ................................................................................................. 47
Figure 6-1  Typical procedure of a cyclic redundancy check .................................................................................. 51
Figure 6-2  Using a CRC table for generating the signature .................................................................................. 51
1 Motivation

The PROFIBUS, EN 50170, [8], field bus standard, which is the successor of the national DIN 19245, [1] through [3], standard, covers a wide range of communications applications in the automation hierarchy:

From I&C via control down to field level.

By simplifications and restriction to the two lowest layers of the ISO/OSI model, the specific requirements of industrial communications (such as short messages, deterministic, and high performance) were taken into account. The Profibus version for distributed I/O has gained particular importance in this context. Using a hybrid access procedure of master/slave and/or token principles, the base Profibus functions are employed here for the cyclic data exchange between peripherals and processing units.

While automation solutions with distributed I/O gained widely acceptance through Profibus DP, failsafe applications were still relying on a second layer of conventional electrical techniques or special busses thus limiting the seamless engineering and interoperability. Additionally modern failsafe devices could not be fueled up as needed due to missing system support. It is the purpose of these Profibus directives to provide the corresponding enabling technologies.

The specific utilization of the communication functions by specific groups of participants is called a profile. A profile is a set of rules and definitions that are valid within a user or a field device group. The DP Safety Profile, in short ProfiSafe, describes the communications between failsafe peripherals and failsafe controllers. It is based on the requirements of the standards for safety-oriented applications and the experience of the PLC users and PLC manufacturers community. The DP Safety Profile be certified by TÜV and BIA (Institute for labor safety of the mutual indemnity association). Since the PA variation of the Profibus DP merely defines a different transmission technique, while the higher protocol layers are identical, the DP Safety Profile also applies to the Profibus PA.

The working group for producing this DP Safety Profile was founded by the PNO advisory board (PNO = PROFIBUS user organization e.V.). The DP Safety Profile is published as a suggestion of a PNO Directive. It is restricted exclusively to the description of the mechanisms that are required for safe communication, and their parameter assignments. The additional measures that are required in the terminal equipment (host/PLC or field device) to make it safe are not described here because they are irrelevant to "open" safe communications.

Albeit the measures for a safe connection of the AS-I bus are discussed in the working group, they will not be described in this profile.

In the following text, the terms "safety-oriented", "safety-relevant" and "failsafe" will be used equally, and be abbreviated by the letter "F".

Chapters 1 through 3 give a general introduction into the requirements and basics of safe communications that are relevant to this profile. Chapter 4 discusses the solution principles in detail. Chapter 5 describes the valid Profibus boundary conditions. The calculations and sources used for deriving the profile are specified in Chapter 6.

1.1 Terminology

- **Bit information**: Encoded binary information without a technical unit.
- **Codename for sender and recipient**: This code is usually within the address space of a F communication device an unambiguous source-destination parameter that is used as a "password" between the F communication partners.
- **Configuration**: Defining the standard communication between the units and defining the specific device parameters.
- **Configuration (FailSafe)**: Defining the F-communication between the F-units and defining the specific F-device parameters.
- **Consecutive number**: Consecutive count that is transferred from the sender to the recipient that is monitored there with respect to the sequence (increment 1) and the interval to the next value. Also known as heartbeat.
- **Control bits**: Bits that are used for triggering control functions. In contrast to bits that
represent a data item (such as a numeric value).

**Cycle**
Interval at which a list of instruction is repetitively and continuously executed.

**Driver**
Software module used for abstracting the hardware with respect to the remaining software.

**EMC**
Electro-magnetic compatibility: electro-magnetic "Worst Case"-boundary conditions for the normal utilization of the ProfiSafe profile. See Profibus standards.

**Encapsulated (closed) system**
Conducted electrical or optical message transfer, radio, infrared, but without public data transmission and with the following characteristics:
- authorized access only
- known maximum number of communicating partners ("F" and standard)
- transmission media is known and well defined

**Error**
Errors are static conditions that exist throughout the product lifecycle, and are inherent characteristics of the system.

**Failsafe (F-...)**
Ability of a system that by adequate technical or organizational measures prevents from hazards either deterministically or by reducing the risk to a tolerable measure.

**Failsafe values**
If the system is triggered to a failsafe state it uses failsafe values instead of process data.

**F-Driver**
Software that administers safe messages within F-Hosts and F-Slaves according to the ProfiSafe directives.

**Failure (states)**
The nonperformance of a system to achieve its intended function within its performance constraints. Failures are events that occur and some point in time, leading to a failed condition (state).

**Fault**
A fault is an unsatisfactory system condition. Thus, failure states and errors are different kinds of faults.

**Fault reaction**
Fault reaction basically means indicating a communication malfunction by setting the fault bits in the status byte and
- within F-Output: Shutting down the outputs, and/or automatic safe reaction of the actuator unit.
- within F-CPU: Corresponding user program reaction possible; F-I/O-Data be set to default values.
- within F-Input: Sets only fault bits in the F status byte; F-I/O-Data be set to default values.

**Frame (Telegram)**
Data unit that is transported on layer 2 of the ISO/OSI model [9].

**Function block**
Self-contained program part that possesses a specific functionality.

**"gray channel"**
Single-channel standard Profibus communication facility that is used by the ProfiSafe failsafe profile (F-Driver).

**Hazard**
A state or set of conditions of a system that, together with other conditions in the environment of the system will inevitably lead to an accident.

**Host**
Information processing unit that is able to perform the F profile mechanisms, and services the "gray" channel. This is usually a PLC or an IPC with an adequate operating system.

**i-parameter**
Individual F device parameters, e.g. detection zone coordinates of a laser scanner.

**I/O module**
Addressable sub I/O unit in a DP slave.
**Master**

Active communication partner that triggers the slave for information exchange.

**Message (packet or TPDU)**

Due to the missing higher layers ( >2 ) of the ISO/OSI model in Profinbus, the process data including safety and control information within a frame corresponds to the transported message [9].

**PES**

Programmable electronic safety-related system

**Process data**

Here: The data in a message that is required for process control.

**Profile**

Specific utilization of the communication functions by specific user groups.

**Reaction time**

The time between the "electrical" recognition of an emergency request and the "electrical" initiation of a safety reaction. The response time consists of several time segments, including the bus transfer time.

**Reliability**

Reliability can be specified as the mean number of failures in a given time (failure rate $\lambda$), or as the mean time between failures (MTBF) for items which are repairable or as mean time to failure (MTTF) for items which are not repairable. For repairable items, it is often assumed that failures occur at a constant rate, in which case the failure rate $\lambda = 1/MTBF$. The reliability of components usually is measured in FIT (= one failure in $10^9$ device-hours) during its operating stage after the infant mortality stage and before the wear-out stage ("bathtub" curve).

**Risk**

A combination of the likelihood of an accident and the severity of the potential consequences

**Scan rate**

Time between any two read processes on input signals.

**Shared I/O**

Several Hosts/PLCs access the same inputs and outputs. Common utilization of inputs is less problematic than sharing outputs.

**Slave**

Passive communication partner that is usually triggered by the master for exchanging information.
2 Introduction

2.1 Possible Application Areas of the Safety Profile
- Manufacturing industry
  - rapid protection of personnel and machines, such as
  - emergency stop functions
  - light gates
  - guard doors
  - scanners
  - drives with integrated safety
- Process industry
- Fuel engineering
- Public transport, such as cable railways

2.2 Requirements Placed Upon the Safety Profile
- Independence between safety-relevant communication and standard communication
  Using standard devices and "safe devices" at the same DP system shall be possible!
- Suitable for safety level SIL3 (IEC61508), AK6 (DIN V 19250); control category 4 (EN 954-1)
- Satisfying the safety requirements in a single-channel communication system → redundancy only for increased reliability
- Any DP master or "links" can be used
- DP masters, ASICs, links, couplers, ... shall remain unmodified (gray channel) → security functions above OSI layer 7 (i.e. profile, no DP protocol changes or enhancements).
- Environmental conditions according to Profibus requirements.
- The implementation of the safe transmission function shall be restricted to the communication end device (CPU / host – slave and/or I/O module).
- The security profile shall not reduce the permitted number of devices (restrictions may occur during mapping in case of PA).
- There is always a 1:1 communication relationship between the F devices.
- The transmission duration times be monitored

2.3 Principle of Safe Communications (Gray Channel)
ProfiSafe’s way of safe communication is based on the experience made in the railway signaling technique as it has been laid down in the European Standard prEN 50159-1 "Railway Applications: Requirements for Safety-Related Communication in Closed Transmission Systems" [5].
On this basis, safe communication is performed by
- a standard transmission system (here: Profibus-DP)
- and additional safety transmission functions as a profile on this standard transmission system.
The standard transmission system includes the entire hardware of the transmission system and the related protocol functions (i.e. OSI layers 1, 2 and 7 according to figure 2-1).
Safety applications and standard applications are sharing the same standard Profibus DP communication systems at the same time.
The safe transmission function comprises all measures to deterministically discover all possible faults / hazards that could be infiltrated by the standard transmission system or to keep the residual error (fault) probability under a certain limit. This includes
- random malfunctions, e.g. due to EMI impact on the transmission channel
- failures / faults of the standard hardware
- systematic malfunctions of components within the standard hardware and software
This principle delimits the certification effort to the "safe transmission functions". The "standard transmission system" does not need any additional certification.

Transmission is performed via electrical or optical conductors. Permissible topologies and transmission features of the standard transmission system, and the components of the "gray" channel are described in Chapter 5.3.

2.4 The Safety Profile

Figure 2-2 shows the model of the complete message structure on the transmission medium [5]. The F profile is "embedded" in the DP transmission protocol (layer 7) and in the transmission code (layer 2), and defines the layers "safety procedures" and "safety code".

![Diagram of F layer architecture](image-url)
2.5 Application

**Host – field device**

The F profile describes the F communication between safety-oriented units via the PROFIBUS-DP/PA. The method described in this profile permits a "safe" field device to cyclically exchange safety-relevant data with a "safe" CPU (host).

**Host - Host**

Not included in the first version of this profile description.

**Field device – field device (cross communication)**

The ProfiSafe principle will cover this operational mode also. There will be little extensions like e.g. additional process data within an acknowledgment message. The details will not be included in the first version of this profile description.

**Failsafe shared inputs**

Multi-master operation of safe CPUs/Hosts with safe I/O is permitted, "Failsafe Shared Inputs" is not (not included in the first version of this profile).

**Dynamic configuration**

In particular in the field of robots, there may be two or more automation subunits that will only be activated when they are "docked". This is also possible in the safety field.

**Other safe busses**

Exchanging safe information with other "safe" bus systems is possible if a corresponding F gateway behaves like a safe Profibus slave.

**EMC field**

Same as standard Profibus
3 Basics of the Safety Profile

3.1 System Characteristics

![Diagram of Typical System Configuration]

The system configuration shown in the figure above characterizes a typical structure of interconnected hosts/PCs, safety-oriented hosts/PLCs, distributed I/O's, field devices, safety-oriented field devices and monitoring units on the Profibus-DP/PA. In this structure (blue dotted line in figure 3-1), a safety-oriented host/PLC controls, via the Profibus-DP master, several subordinate safety-oriented and non-safety-oriented Profibus-DP slave units/modules. The encapsulated (closed) transmission system may extend across several segments that are interconnected via repeaters.

The connection to other safe bus systems via F gateways is not discussed in this Profibus profile description.

3.2 Master-Slave Operation in PROFIBUS-DP

The PLC/IPC is the host in a PROFIBUS-DP system. The related DP master is in a stand-alone module or it is a subunit of the host. The I/O stations are slaves. The master (PLC) addresses each slave (I/O module) once in a DP cycle. In this process, a fixed number of output bytes is sent to the slave or the slave reads a fixed number of input bytes respectively.

3.3 Bus Structures

In contrast to the typical system configuration, Figure 3-2 shows the possible bus structure (i.e. how far the F profile extents into the individual units). A standard DP slave, for example, can accommodate a safe F module for the connection of an emergency stop pushbutton. Multi-master operation of safe hosts is permitted, "Failsafe Shared Inputs" (not included in the first version of this profile) are not. A mix of F host and standard host is possible.
It is within the user’s responsibility to employ adequate organizational and/or technical measures (e.g. call-back, firewall, etc.) to ensure that unauthorized access from the connected programming and/or engineering stations cannot jeopardize safe operation. These devices are not usually participants in a safe operation.

### 3.4 Delimitation of the Bus Components

The entire safety function shall be considered for the acceptance of the system.

**Inspection of the complete safety function of control loops** according to IEC 61508:

![Diagram of control loops]

The whole path is safety relevant:

- **Scan safe Information**
- **Process safe information**
- **Initiate safe reaction**

The units "safety-oriented input", "safety-oriented logic processing", and "safety-oriented output" are not included in the discussion of the F profile.
We only define the measures that implement the F communication in the individual communication end points. The F profile ensures the protection of the data between the peripheral F modules and/or safe directly connected sensors/actuators/F-PA units and the F-CPU. There are no additional requirements placed upon the components DP master, DP slave, PA master, DP/PA link. They belong to the "gray channel".

This means:

a) **not** safety-relevant are: ASICs, bus drivers, lines, repeaters, links, and the slave interface of modular slaves (see definition "gray channel").

b) **safety-relevant** are: Safety profile, F watchdog functions, F addressing, F parameters, peripheral F modules, and/or safe field devices.

### 3.5 Delimitation of the Communication Functions

The F profile only supports the cyclic service (DP).

Acyclic services are used for communicating non-safety-relevant data.

Parts of the slave parametrization are safety-relevant, and are protected via the cyclic service.

### 3.6 Risk Consideration

Figure 3-4  Risk consideration according IEC 61508

Figure 3-5  Profibus-DP, proportional risk
The risk reduction of a facility is achieved via a safety function provided by a safety-oriented electrical/electronic/programmable electronic system (E/E/PES) with a certain residual error probability (Safety Integrity). The contribution of the Profibus-DP to this residual error probability may be 1%. This means that the residual error probability of the DP bus, in conjunction with the ProfiSafe profile, shall be 100 times "better" than it is required in SIL3, for example.

Thus, the residual error probability of the other components involved in the safety control loop results as 99/100 of the value that is required in SIL. This assessment deals with balancing the individual implementation efforts.

According to [6], the following bit error probability values are valid for transmission systems including bus drivers (this chart originates from Dieter Conrad’s book, “Datenkommunikation”, 3rd edition).

<table>
<thead>
<tr>
<th>Bit error probability p</th>
<th>Transmission system</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;10^{-3}</td>
<td>Radio link</td>
</tr>
<tr>
<td>10^{-4}</td>
<td>Unshielded telephone cable</td>
</tr>
<tr>
<td>10^{-5}</td>
<td>shielded, &quot;twisted-pair&quot; telephone cable</td>
</tr>
<tr>
<td>10^{-6} - 10^{-7}</td>
<td>Digital telephone cable of Deutsche Telekom (ISDN)</td>
</tr>
<tr>
<td>10^{-9}</td>
<td>Coaxial cable in locally delimited applications</td>
</tr>
<tr>
<td>10^{-12}</td>
<td>Fiber optics cable transmission</td>
</tr>
</tbody>
</table>

Thus, the typical error frequency (bit error probability) on the shielded DP cable is less than or equal to 10^{-5}. The calculation of the profile, however, is based on the bit error rate of the "gray channel". The Hamming distance of the standard Profibus protocol is 4; this does not influence safe communication, however.

According to IEC 61508 [5], the following residual error rate values are permitted in the individual SIL stages:

<table>
<thead>
<tr>
<th>SIL</th>
<th>Probability of a hazardous error per hour in uninterrupted operation mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>&gt;10^{-9} ......&lt;10^{-7}</td>
</tr>
<tr>
<td>2</td>
<td>≥10^{-7} ......&lt;10^{-6}</td>
</tr>
<tr>
<td>1</td>
<td>≥10^{-6} ......&lt;10^{-5}</td>
</tr>
</tbody>
</table>

Thus, the required residual error rate of <10^{-9}/h results for the entire equipment within the range of the ProfiSafe profile for SIL3.

### 3.7 Relevant Standards and Directives

- **General standards for systems with safety responsibility**
  - IEC 61508 Base standard for safety-relevant electronic/programmable electronic systems
  - DIN V VDE 801 A1

- **Principle of safe communication**
  - prEN 50159-1/2 "Railway applications: Requirements for Safety-Related Communication in Closed/Open Transmission Systems"

- **Process engineering (chemistry, petrol)**
  - IEC 61511 "... Safety instrumented Systems for the Process Industry”
  - VDI/VDE 2180 "Protection of process-engineering plants using process control means).
  - DIN V 19251 Instrumentation and control – MSR protective equipment, requirements and measures related to the safe function

- **Fuel systems**
  - prEN50156 "Electrical equipment of fuel systems ..." (burner control)

- **Machine safety**
  - EN / IEC 60204-1"Electrical equipment of industrial machines "

© Copyright PNO 1999 – All Rights Reserved
3.8 Error Cases That Shall Be Mastered

According to [4], the following transmission errors exist:

- Repetition
- Loss
- Insertion
- Incorrect sequence
- Corrupted process data
- Delay
- Interconnecting safety-relevant and standard messages (masquerade)
- Erroneous addressing (double-, wrong-)

It is within the responsibility of the profile that is described here, to provide additional safety measures over and above the means that already exist in Profibus that permit the necessary residual error rate to be reached.
4 Functional Principle of Safe Communication

The above-mentioned measures for mastering failures that shall be taken are a significant component of the F profile. Due to the existing protective functions of the standard Profibus, only a selection of the measures listed in the position document DKE-AK 226.03, [4] is required. The measures shall be taken and monitored within one FailSafe unit.

<table>
<thead>
<tr>
<th>Failure:</th>
<th>Measure:</th>
<th>Consecutive Number</th>
<th>Time expectation with acknowledge</th>
<th>Codename for sender and recipient</th>
<th>Data Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repetition</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Insertion</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Incorrect Sequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Corrupted Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delay</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interconnecting of F- and Standard Messages (Masquerade), incl. wrong- und double addressing</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Excerpt from table of the position paper DKE-AK 226.03

Figure 4-1 Error mastering measures

4.1 F Message Structure

![Figure 4-2 DP frame structure (Process Data)](image-url)

SB ZB 0 1 2 3 4 5 6 7 PB EB

Sync time SD LE LER SD DA SA FC

33 TBit 68H ... ... 68H ... ... ...

Data Unit = Standard or Failsafe-Process Data

FCS 1...244 Bytes ED 16H

1 Cell = 11 Bit

TBit = Clock-Bit = 1 / Baudrate
SD = Start Delimiter (here SD2, var. data length)
LE = Length of Process Data
LER = Repetition of Length; no check in FCS
DA = Destination Address
SA = Source Address
FC = Function Code (Message type)

Data Unit = Process Data, for Failsafe Process Data also, max. 244 Bytes (across data within LE)

FCS = Frame Checking Sequence
ED = End Delimiter
SB = Start-Bit
ZB0...7 = Character-Bit
PB = (even) Parity Bit
EB = Stop-Bit
Figure 4-2 shows the frame structure of the single-channel PROFIBUS-DP communication that contains the F process data within its data unit as well as the basic Profibus safety measures via Parity and Frame Checking Sequence.

![Frame Structure Diagram]

Figure 4-3 Complete F message structure

A maximum of 128 bytes out of the maximum possible 244 bytes can be used for F process data. This is due to the limitation of the data consistency to a maximum of 64 words in the case of Profibus-DP (a maximum of 64 words can consistently be exchanged at any one time between the host and the bus master). CRC generation, however, requires a contiguous data area.

Two operational modes can be chosen by parametrization: few F process data up to 12 Bytes together with 16 Bit CRC2 (2 Bytes) and F process data up to 122 Bytes together with 32 Bit CRC2 (4 Bytes).

In addition, 4 bytes in total are required for the status/control byte, 1 byte for the consecutive number, and 2 to 4 bytes for the CRC2 code.

The F profile permits standard process data to be appended to the F message segment (F slaves only). In this case, the F slave needs one codename (F source-destination relationship) for the F process data area and another one for the standard process data area.

The following sections give a detailed description of the components of the F data structure.

4.1.1 F Process Data

The data of the safe I/O peripherals is accommodated in this frame section. The code corresponds to the one of the standard Profibus. In the case of only a few F process data up to 12 Bytes one should for performance reasons choose 16 Bit CRC by parametrization.

The appended standard process data is used, for example, in gateways to other safe field buses in order to be able to include standard I/O data in the transport via a single slave address.

Besides the compact slaves, there are modular slaves with F and standard I/O units and subaddresses. Their Profibus head-end station, that is considered as a part of the "gray channel", is used for agreeing the structure of a "modular" message frame via the parametrization. In this case, F module process data may also be a part of the frame. The amount of data corresponds to the net amount of data in Profibus DP minus 4 or 6 Bytes respectively. That means for a head-end station with m F modules a reduction of m times 4 or 6 Bytes respectively.
Process Data
Modular Slave

<table>
<thead>
<tr>
<th>Slot</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cfg-ID</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Module</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

$\Sigma = 244$ Bytes

Figure 4-4  Modular slave with two F modules

Configuration supposes Slot = Cfg-ID = Module.

Figure 4-5  Embedding the F I/O data of **compact** and **modular** slaves

4.1.2 Status/Control Byte

<table>
<thead>
<tr>
<th>Bit7</th>
<th>Bit6</th>
<th>Bit5</th>
<th>Bit4</th>
<th>Bit3</th>
<th>Bit2</th>
<th>Bit1</th>
<th>Bit0</th>
</tr>
</thead>
<tbody>
<tr>
<td>tbd</td>
<td>res</td>
<td>res</td>
<td>Failsafe values (FV) activated</td>
<td>Communication failure: WD-timeout</td>
<td>Communication failure: CRC or consecutive number</td>
<td>Failure exists in F slave or F module</td>
<td>F slave has new i-parameter values assigned</td>
</tr>
</tbody>
</table>

The status byte is contained in each slave frame.

Bit 0 is set when the F slave has new parameter values assigned.

Bit 1 is set for at least two (2) message cycles, if there is a malfunction in the F slave itself.

Bit 2 is set if the F slave is recognizing a F communication failure, i.e. if the consecutive number is wrong or the data integrity is violated (CRC). This bit information enables the F host to count all erroneous messages within a defined time period T and to trigger a configured safe state of the system if the number exceeds a certain limit (maximum residual failure rate). See also chap. 4.11.1.
Bit 3 is set if the F slave is recognizing a F communication failure, i.e. if the watch dog time in the F slave is exceeded.

Bit 4 is set if the F input slave is sending failsafe values (FV) or the F output slave set FVs respectively.

Bit 5,6 are reserved (res).

Bit 7 can be defined according to the manufacturer requirements (tbd).

<table>
<thead>
<tr>
<th>Bit7</th>
<th>Bit6</th>
<th>Bit5</th>
<th>Bit4</th>
<th>Bit3</th>
<th>Bit2</th>
<th>Bit1</th>
<th>Bit0</th>
</tr>
</thead>
<tbody>
<tr>
<td>tbd</td>
<td>tbd</td>
<td>res</td>
<td>res</td>
<td>res</td>
<td>res</td>
<td>res</td>
<td>i-parameter assignment de-blocked</td>
</tr>
</tbody>
</table>

Figure 4-7  Control byte

The control byte is sent with each DP master message frame.

Bit 0 is set if a parametrization request is detected or a F slave needs new i-parameters. In this case the system uses the failsafe values (FV).

Bits 1 to 5 are reserved (res).

Bits 6,7 can be defined according to the manufacturer requirements (tbd).

4.1.3 Consecutive Number

The consecutive number is used for monitoring the "life" of the sender and the communication link by the recipient. It is used in an acknowledgment mechanism for monitoring the propagation times between sender and recipient.

The value "0" is reserved for the first run. Thus, the consecutive number counts in cyclic mode from 1... 255, wrapping over back to 1 at the end.

*) in mixed I/O slaves the acknowledge may contain F process data also

Figure 4-8  Consecutive number function
4.1.4 CRC Signature

Once the F parameters (source-destination relationship or codename, SIL, watch dog times, etc.) have been loaded, these identical parameters are employed in an identical procedure in the source and in the target for producing CRC1 keys (CRC1). The CRC1 key, the failsafe process data, and the status or control byte are used for producing another 2-byte / 4-byte CRC2 key (CRC2) in the source. The CRC1 key provides the initial value for the calculation of CRC2 that is transferred cyclically. In the target, the identical CRC key is generated and the keys are compared. The subsequent cyclic transfer only requires one CRC2 key comparison (that can be done very rapidly).

![Figure 4-9 CRC generation](image)

The CRC1 recalculations shall be executed once a day, i.e. within 24 h (maximum cycle time of self testing).

4.1.5 Appended Standard User Data

With F slaves, the F profile permits standard user data to be appended to the F message part until the maximum frame length is reached. In this case, the F slave requires one codename (F source-destination relationship) for the F process data area and one for the standard process data area.

The appended standard process data is used, for example, in F gateways to other safe field buses in order to be able to include standard I/O data in the transport via a single slave address.

F modules in modular slaves only know F process data.
4.2 Regular F Communication

The following chapters are dealing with the "dynamics" of the ProfiSafe profile. First of all the start-up and cyclic behavior, later on the failure reactions.

4.2.1 Operational Behavior of F Host and F Slave

Figure 4-10 shows that each F input and each F output requires a F message frame management (F driver) in order to handle the ProfiSafe profile. The corresponding F host (F CPU) operates with an instance of a F message management (F driver) for each F input or F output respectively. The whole standard Profibus communication equipment between F drivers belongs to the "gray channel". The arrows are indicating the cyclic data transport between the F drivers: the safety addenda (consecutive number, CRC, status/control byte) are transferred in addition to the F process data from the F input to the F CPU. As an acknowledgment, the F input merely receives the safety addenda (safety code).

![F communication structure](image)

**Figure 4-10** F communication structure

Accordingly, the F output receives the safety addenda in addition to the F process data, and uses it for acknowledgment.

![F User Interfaces of F driver instances](image)

**Figure 4-11** F User Interfaces of F driver instances
Message frame management and F parametrization of F host and F peripherals are tasks of the F drivers within the F CPU and the F slaves. Figure 4-11 shows the user interface at the failsafe control program level. There are several signals available to the programmer to manipulate failsafe processes according to the standards.

- **Codename**: The F host – slave 1:1 relationship parameter (4 Bytes) initiates an instance incl. CRC1

- **Operator Acknowledgment OA**: In changing this signal from 0 to 1 the user is able to release a safety function after a fault reaction (failsafe control loop specific) via a F control program (type: boolean).

- **FV activated**: This signal is available to F control programs and indicates that the outputs are set to failsafe values and the inputs are sending failsafe values due to a fault recognized by F host or F slave (type: boolean).

- **Fault**: This signal is available to F control programs and indicates that the F host or F slave recognized any of these failures: timeout, CRC, consecutive Nr., slave malfunction (type: boolean). In any of these cases outputs are set to failsafe values and inputs are sending failsafe values as long as faults are recognized until the OA signal will release the safety function.

- **General release**: This signal is available to F control programs (type: boolean). Usage of any process values instead of failsafe values only is possible if this signal turns from 0 to 1. Can be used for a general release of the safety system after startup.

- **Output and input values**: During normal operation these are user defined process values.

The following figure 4-11 demonstrates how the F driver is using the underlying PROFIBUS-DP communications and some timing definitions. Meaning of the short arrows: in Profibus-DP, the DP master sends the frame more frequently to the slave than it receives it from the host (F-CPU).

![Figure 4-12 Monitoring the message transit time F-CPU ↔ F output](image)

The main features of the operational behavior are listed below:

- **Startup (synchronization)**: To synchronize after a cold restart, new parametrization, or timeout of F input/F output, the F driver starts with the consecutive number “0”. Next, the F-CPU increments the consecutive number in each call modulo 256, skipping the value 0. At the latest before the monitoring time is about to expire, F input/F output expects a message with a consecutive number that is incremented by 1. A F output does not supply any process value after it has received a consecutive number of 0.

- **F protocol cycle**: F input/F output sends a F message frame with the same consecutive number (F protocol cycle).
col cycle) to acknowledge the reception of a F message from the F-CPU.

The F-CPU cycle shall not exceed the F protocol cycle (it may be shorter).

**Time monitor (watch dog)**

Arrival of a new correct message frame at the F device within the watchdog time is monitored. This verification can be performed as often as necessary, but at least once at the end of the monitoring time interval. It is permitted and tolerated that one incorrect message frame (with faulty CRC code or where the consecutive number has been incremented by more than 1) arrives before a new correct frame is received. This means that this does not lead to a safe state error reaction. When the watchdog time expires, the related recipient switches over to a safe state.

The slowest Profinet DP cycle time may not be longer than half the monitoring time. The F-CPU cycle may be shorter than the monitoring time.

**Monitoring the consecutive number**

A new correct message frame is characterized by the fact that at least the consecutive number has been incremented by 1 and that either the entire rest of the F frame part is unchanged or has been changed faultlessly. This means that an incorrect change of the consecutive number by +1 is not recognized at once, but only after another DP cycle or F protocol cycle. This will then lead to a fault reaction.

Assuming two simultaneous faults, i.e. "failure of the F-CPU" and "incorrect incrementing" of the consecutive number is not realistic. Neither is the case of simultaneous failures where a smart device in the gray channel continuously increments the consecutive number by +1 while the F-CPU has failed.

The simultaneous case "safety-oriented request" and "incorrect incrementing" of the consecutive number by +1 is discovered immediately with the request message and leads to the described fault reactions.

**Frame repetition**

A complete message frame repetition in the event that a new correct message frame has not been received inside the watchdog time interval is not supported.

**SIL monitor**

Every corrupted message (CRC and consecutive Nr. failure) will be counted during a configurable **monitor time period**. The failsafe values are set whenever more than one such failure occurred. The cases, where CRC=0 and the consecutive Nr.=0, shall not be counted, they cause the setting of the failsafe values instead.

**Monitor time period (T)**

The monitor time period T is a constant value with the dimension hour (h), that results from the requested SIL and the configured CRC length (see chap. 4.11.1):

<table>
<thead>
<tr>
<th>SIL</th>
<th>CRC</th>
<th>Length of process data</th>
<th>Time period (h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>16 Bit</td>
<td>&lt; 16 Bytes</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>16 Bit</td>
<td>&lt; 16 Bytes</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>32 Bit</td>
<td>&lt; 128 Bytes</td>
<td>0.1</td>
</tr>
<tr>
<td>2</td>
<td>32 Bit</td>
<td>&lt; 128 Bytes</td>
<td>0.01</td>
</tr>
</tbody>
</table>
4.2.2 State Diagrams

The following chapter demonstrates the operational behavior of F host and F slave by means of interaction and state diagrams.

The figures show the interaction messages of F host and F slave during start-up phase. Three phases are covered: both partners during start-up, host temporarily switches power off or slave temporarily switches power off while its partner is still operating. The following figures are informing about the states and the corresponding transitions. The states the respective F system is passing through are represented by numbers within circles.

![State Diagrams](image-url)

Figure 4-14 Interaction F host / F slave during start-up
Figure 4-15 Interaction F host / F slave during Host Power Off → On

Figure 4-16 Interaction F host / F slave with delayed Power On
Figure 4-17 Interaction F host / F slave during Slave Power Off → On
Figure 4-18  F host states during interactions with the F slave
After Power On the output slave is setting "0". Immediately after F parametrization it is setting failsafe values.

After Power On the input slave is sending "0". Immediately after F parametrization it is sending process values.
Figure 4-20 Interaction F host / F slave while host recognizes CRC failure

Figure 4-21 Interaction F host / F slave while slave recognizes CRC failure
4.3 Reaction in the Event of a Malfunction

4.3.1 Repetition

Quote: "The malfunction of a bus device causes old and obsolete messages to be repeated at the wrong time so that a recipient would dangerously be disturbed (e.g. guard door is reported closed albeit it has already been opened)."

Remedial action: The data in DP mode is transferred cyclically. Thus, an incorrect message that is inserted once will immediately be overwritten by a correct message. The thereby possible delay of an emergency request can be one watch dog time.

4.3.2 Loss

Quote: "The malfunction of a bus device deletes a message (e.g. request for "safe operational stop")."

Remedial action: Lost information will be discovered by the stringently incrementation and surveillance of the consecutive number.

4.3.3 Insertion

Quote: "The malfunction of a bus device inserts a message (e.g. deselection of the "safe operational stop")."

Remedial action: Due to the stringently sequential expectation of the consecutive number, the recipient will discover an inserted message.

4.3.4 Incorrect Sequence

Quote: "The malfunction of a bus device modifies the message sequence. Example: Prior to initiating the safe operational stop you want to select the safely reduced velocity. The machine will be running instead of being stopped when these messages are confused."

Remedial action: Due to the stringently sequential expectation of the consecutive number, the recipient will discover any incorrect sequence.

4.3.5 Corruption of F Message Data

Quote: "The malfunction of a bus device or the transmission link corrupts messages."

Remedial action: The CRC2 code discovers a corruption of the data between sender and recipient.

<table>
<thead>
<tr>
<th>F parameter data</th>
<th>DP net data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>F user data</td>
</tr>
<tr>
<td></td>
<td>status/</td>
</tr>
<tr>
<td></td>
<td>control byte</td>
</tr>
<tr>
<td></td>
<td>across</td>
</tr>
<tr>
<td></td>
<td>F process data</td>
</tr>
<tr>
<td></td>
<td>and</td>
</tr>
<tr>
<td></td>
<td>F parameters</td>
</tr>
<tr>
<td></td>
<td>m bytes</td>
</tr>
<tr>
<td></td>
<td>1 byte</td>
</tr>
<tr>
<td></td>
<td>2 / 4 bytes</td>
</tr>
</tbody>
</table>

Figure 4-22  F parameter data and CRC

The CRC2 code is generated across the F parameters (including F source-destination relationship) and across the F process data and the control/status byte. The source-destination relationship of F-CPU and F slave is defined in the configuration, and retentively stored.

After a repair, the F address of a F device be restored / adjusted before F operation is resumed.

4.3.6 Delay

Quote: "1. The operational data exchange exceeds the capacity of the communication link. 2. A bus device causes an overload situation by simulating incorrect messages so that a service that belongs to the message is delayed or prevented."
Remedial action:

- Consecutive number in the sender data and in the acknowledgment data.
- Watchdog time in the respective recipient (watchdog time for F communication).

The watchdog time is a part of the whole safety time of the safety control loop. The total time guaranteed by the PES is the sum of the following time segments:

+ input delay of the F input slave (operation time)
+ watchdog time "F communication": F input ↔ F-CPU
+ Scan rate or execution time in the F-CPU
+ watchdog time "F communication": F-CPU ↔ F input
+ output delay of the F output slave (operation time)

The ProfiSafe DP profile defines the meaning of the "F communication" watchdog time.

### 4.3.7 Interconnecting Safety-Relevant and Standard Messages (Masquerade)

Quote: "The malfunction of a bus device causes safety-relevant messages and non-safety-relevant messages to be mixed".

Remedial action: The data comes from the correct sender or go to the correct recipient [authenticity]. This is guaranteed by the CRC2 signature across the F parameters (which includes the F source-destination relationship).

Principle of safe addressing:

a) Detecting the interconnection of safety-relevant and non-safety-relevant messages is guaranteed by the fact that a standard device is not capable of creating a F message frame with the correct CRC2 and the correct consecutive number.

b) Detecting data from a different sender or for a different recipient is guaranteed by the fact that the F sender that belongs to the F source-destination relationship (codename) is the only one that generates exactly the matching CRC key that is expected by the F receiver. At the same time, the recipient employs this CRC key for implicitly checking the authenticity of the F sender address (since it was included in the CRC).

c) A retentive selection of the F address in the individual devices can be achieved through one of the following methods:
   - Coding switch in the unit (the F slave address of compact slaves, for example)
   - A one-time device parametrization by software that requires to be checked whether the correct device has been addressed. This shall be repeated when a unit is replaced.
   - By address mechanisms that are independent of Profinet-DP addressing.

Sabotage is not assumed.

### 4.4 F Parameter Structure

The parameter values of the Profinet devices on the "gray channel" are assigned according to the Profinet standard description, i.e. via GSD files from the Class 1 Profinet master (cyclic) or, with Profinet-PA, via DDL and class 2 master (acyclic). The F parameters that are additionally required for the F profile can be loaded via several alternative parametrization ways.

Here is an overview:

- F_Device Identification telling that the unit supports ProfiSafe (corresponds to command byte)
- F_S/D_Address "Code word" between sender and recipient
- F_WD_Time Watchdog time in the F unit (default in GSD: operation time of a F slave)
- F_Prm_Flag Parameter word containing several parameters for the profile management
- F_Check_SeqNr Including the consecutive number into the CRC2
- F_Check_iPar Including individual F device parameter into the CRC1
- F_SIL Check: configured = employed F device ?
- F_CRC_Length CRC2 length
- F_Par_CRC CRC1 across the F parameters
4.4.1 **F_Device (ProfiSafe Participant)**

This parameter marks a unit as a F device that supports the ProfiSafe profile. It can also be used for distinguishing between safety-oriented and non-safety-oriented units. This parameter has to be distributed to the F component during startup. It corresponds to the command byte in the Prm-message.

4.4.2 **F_Source/Destination_Address (Codename, Password)**

The addresses of the F components of a safety control loop F input, F-CPU and F output shall be unambiguous. Locally, each F device has the configured source-destination relationship of the safe communication link with its partner. It is retentively stored in the F devices, a part of the F parameter set, and, consequently, is cyclically checked by the F profile. The F_S/D_Address parameters are logic address designations that can freely but unambiguously be assigned and are allocated to the Profibus addresses during the configuration (see chap. 4.3.7).

The addresses 0 and 0xFFFFh be excluded.

The parameter consists of two parts: F module/slave and F host: each Unsigned 16.

4.4.3 **F_WD_Time (F Watchdog Time)**

Locally, each F device maintains a configured F watchdog time for each source-destination relationship. The device starts this timer whenever it sends a safe message frame.

The F watchdog time consists of at least four times the slowest DP cycle time (that results from the worst-case calculations of the entire configuration) plus two times the slower scan rate of the combination of the related sender and recipient. The configured value overwrites the default value within the GSD.

It is encoded as follows: Unsigned 16; time base 1ms.

Remark: a manufacturer of a F device assigns the device operation time (scan rate) to the default value of the parameter F_WD_Time. An engineering tool will then be able to propose the necessary F watchdog times and to calculate the overall reaction times.

4.4.4 **F_Prm_Flag (Parameters for the Profile Management)**

The chapters 4.4.5 up to 4.4.8 are describing the details of the F_Prm_Flag parameter word. It has the following structure:

```
 15 14 13... 6 5 4 3 2 1 0
  ↑___ ↑___ ↑___ ↑___ ↑___ ↑___ ↑___ ↑___  F_Check_SeqNr
  ↑___ ↑___ ↑___ ↑___ ↑___ ↑___ ↑___ ↑___  F_Check_iPar
  ↑___ ↑___ ↑___ ↑___ ↑___ ↑___ ↑___ ↑___  F_SIL
  ↑___ ↑___ ↑___ ↑___ ↑___ ↑___ ↑___ ↑___  F_CRC_Length
  ↑___ ↑___ ↑___ ↑___ ↑___ ↑___ ↑___ ↑___  reserved
  ↑___ ↑___ ↑___ ↑___ ↑___ ↑___ ↑___ ↑___  Version No. of F parameter set
```

4.4.5 **F_Check_SeqNr (Consecutive Number in the CRC2)**

This parameter defines whether or not the consecutive number shall be included in the CRC2 key. The parameter is distributed to the F component during startup.

It is encoded as follows: bit 0 of the parameter word "F_Prm_Flag"

```
 15... 6 5 4 3 2 1 0
 0 = No check
 1 = check
```

4.4.6 **F_Check_iPar (CRC1 including i-Parameters)**

This parameter defines whether or not the CRC3 of individual device parameters shall be included in the cyclic CRC2 key (see chap. 4.4.9). If "check" is selected, CRC1 is generated across the F-parameters first and then across the i-parameters including its CRC3. The parameter is distributed to the F component during startup.
It is encoded as follows: bit 1 of the parameter word "F_Prm_Flag".

<table>
<thead>
<tr>
<th>15..6 5 4 3 2 1 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = No check</td>
</tr>
<tr>
<td>1 = check</td>
</tr>
</tbody>
</table>

### 4.4.7 F_SIL (SIL Stage)

The F profile permits parallel operation of standard communication and safety-relevant communication. In the safety-relevant case, risk-related safety circuits with different SIL (Safety-Integrity-Level) stages are distinguished. The F devices are able to use this locally available information for checking the agreement between the SIL stage and the partner. If the configured SIL stage is higher than the one in the connected F unit, the "device failure" status bit is set and a safe state reaction is triggered. There are four different stages: 1, 2, 3, 4.

It is encoded as follows: Bits 2 and 3 of the parameter word "F_Prm_Flag".

<table>
<thead>
<tr>
<th>15..6 5 4 3 2 1 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 = SIL1</td>
</tr>
<tr>
<td>0 1 = SIL2</td>
</tr>
<tr>
<td>1 0 = SIL3</td>
</tr>
<tr>
<td>1 1 = SIL4</td>
</tr>
</tbody>
</table>

### 4.4.8 F_CRC_Length (Length of the CRC2 Key)

Depending on the length of the F process data (12 or 122 bytes) and the SIL stage, a CRC of 2, or 4 bytes is required. This parameter transfers the expected length of the CRC2 key in the F message frame to the F component. The parameter depends on the slave/module and is distributed to the F components during startup.

It is encoded as follows: Bits 4 and 5 of the parameter word "F_Prm_Flag".

<table>
<thead>
<tr>
<th>15..6 5 4 3 2 1 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 = reserved</td>
</tr>
<tr>
<td>0 1 = 2 Byte CRC</td>
</tr>
<tr>
<td>1 0 = 4 Byte CRC</td>
</tr>
<tr>
<td>1 1 = reserved</td>
</tr>
</tbody>
</table>

### 4.4.9 F_Par_CRC (CRC1 across F-Parameters)

This CRC1 key is generated by the engineering tool across the F-parameters. The initial value for CRC1 is 0. The same 16 Bit CRC polynomial is used (14EABh). CRC1 is the initial value for cyclic CRC2 computation.

In case of 32 Bit CRC polynomial (1F4ACFB13h) the initial value for CRC2 calculations is "0000xxxx", where xxxx=CRC1.

It is encoded as: Unsigned 16.
4.4.10 Structure of the F Parameter Block (Pmr telegram)

![Diagram of F parameter block](image)

The figure shows the structure of the F parameter block within a standard Profibus Prm-Telegram. The byte ordering is according to standard Profibus. The following applies to modular slaves: For each F module, a F_Prm_Block is inserted in the Prm-Telegram. The allocation to the module can be established on the basis of the slot number.

4.4.11 F Data Fraction

Standard process data can be appended to a F message frame. For compact F slaves, this is achieved by allocating a separate module identification. F modules in modular slaves are not able to support this mechanism.

4.4.12 i-Parameter (individual F-Device Parameters)

F peripherals are increasingly provided with smart functions that require extensive parameter values to be assigned. In particular in the event of a device replacement it is expedient to load these parameters directly via the bus on the standard path. These parameter records usually exceed the range of the GSD data (a laser scanner with approximately 1 kB per protection zone leads to an overall quantity of up to 90kB) and so the ProfiSafe directives provide additional mechanisms.

The following figure shows a proposal for the protection of large amounts of individual F device parameters. The F source/destination relationship (codename) allows checking of delivery to the configured recipient and the CRC keys allow checking of the i-parameter integrity using the same CRC polynomial like with the F-parameters (14EABh). A special procedure shall be used for ensuring the data integrity between the i-parameters within the destination and within the source. See section "CRC Signature".

The requirements for more flexibility in today's manufacturing areas can be solved by recipe programs via program controlled dynamic i-parameter assignments. Thus several different sets of e.g. coordinates for detection zones of laser scanners ("blanking") can be assigned one after the other (Fig. 4-25). The identification number of the actual i-parameter set shall be communicated cyclically within the F process data.

The F host system should provide mechanisms ("read data set") to acquire e.g. detection zone coordinates via teach-in into the F host itself or into an engineering tool.
### F-Parametrization

ProfiSafe provides scaled methods for i-parameter supply of F devices because of the different handlings of field devices within the manufacturing and the process industries.

#### 4.5.1 F-Parametrization Tools

The discussion of use cases yielded the following F system requirements and resulting subsets for integrated respectively separate F parameter assignment tools:
1. Swift unit replacement and automatic reparametrization are mandatory in manufacturing industries. Not all customers will accept memory cards that contain the parameters. They request adequate programming facilities at the parametrization tool, or the customer shall put the equipment on the desk for parameter value assignment.

2. Individual parametrization software for each manufacturer or unit cannot be accepted. Parameter value profiles and/or templates shall be defined for each device class, and be certified by the PNO. For more complex and special parameters, the general-purpose parametrization tool shall provide a "plug-in" interface for the device manufacturers that permits the specific (e.g. graphical) acquisition of the device parameters. However, these parameters shall be supplied to the general-purpose parametrization tool in a standardized form (GSD, DDL, XML?). See Figure 4-26.

3. A F parametrization tool shall be able to calculate worst case reaction times of safety control loops.

4. A general-purpose parametrization tool on the Profibus shall be able to load parameters across network hierarchies into a host (manufacturing industries) and/or into field devices (process industries). This requires a separate user interface to exist. A "service interface" shall be provided for tooling machine or plant manufacturers for their own visualization software invoking basic Profibus/ProfiSafe service functions.

5. All parameters shall be available from a common archive. It shall be possible to lock accidental incorrect loading of parameters by service personnel.

6. Four different roles can be seen and the corresponding access locking (e.g. by passwords) is required:
   – Operator
   – Service (unit replacement)
   – Authorized customer (program modifications)
   – Device manufacturer (device data that is only accessible to the manufacturer provide information about unauthorized utilization and unjustified claims of recourse)

7. A change log shall record each and every change in program and parameter value assignment.

Remark: It is mandatory to take the appropriate measures against all kinds of faults during acquisition, manipulation and transport of the F- and i-parameters. It is not the task of the ProfiSafe directives to provide a complete list of measures and their assessment. Please see the appendix 6.1 for further hints.

4.5.2 GSD Structure

Essentially there is only one additional keyword "F_Device_Supp" necessary within a GSD structure. This keyword needs to be inserted twice in the GSD file of a compact or modular F slave:
   - first as a general keyword to distinguish a safety related slave from a standard slave.
   - additionally in each F modul.
With the help of this keyword a special F configuration module (F control) inside the engineering tool may be launched.

Profisafe recommends the usage of the keyword "Prm_Structure_Supp" in order to indicate that the F slave is expecting a block structure within a F-Prm-Telegram (details to be published by other working groups). The structure of a typical GSD file for a F device can be seen in appendix 6.3. There is a special agreement for the F parameter "F_WD_Time". Since this parameter is contained in the Prm-block of a F module and is described by a default value and a range, this default value is defined as the \textit{operation time} of the F slave. The F configuration tool can use the value as the basis for the calculation of the F watch dog time and over all reaction time. The manufacturer of a F device is usually the provider of the default value via the corresponding GSD file.

Excerpt from the GSD file of a F device:

```
; User_Prm_Data-Definition 8
ExtUserPrmData=8 "F_WD_Time" ; reference number 8
Unsigned16 3 0-65535 ; time base=1ms; default (operation time)=3ms; max=65.5s
EndExtUserPrmData
End of excerpt from GSD file...
```

### 4.5.3 F-Parameter Assignment Paths

![Diagram of F-parameter assignment for simple F slaves](image)

**Figure 4-27** F-parameter assignment for simple F slaves

Simple slaves can be supplied via the standard Prm-Telegram path described in the following chapters. The total amount of F parameters hereby can not exceed the upper limit of 234 bytes.
For complex devices a decision shall be made whether an automatic startup assignment is requested or a separate assignment from a parametrization tool. In each case the F host shall deblock the assignment (see chap. 4.5.4), that is only permitted, if there is no hazardous process state.

Basically, two ways are possible:

- Startup parameter value assignment from a class 1 (cyclic or acyclic) Profibus master
- Startup parameter value assignment by a class 2 master (acyclic through, e.g. PG/ES or PC)

### 4.6 F-Startup Coordination

The F-startup that is embedded into the Profibus standard startup is described here.
4.6.1 Standard Startup (F Slave State Machine)

After Power-On a F slave switches into the state "Wait_Prm" where it is possible to assign an address by software. The transition into the state "Wait_Cfg" is initiated by a Prm-Telegram "Set Parameter" that in our case contains the F parameter also. By means of a "Chk_Cfg" telegram the F DP slave receives the information how to configure the Inputs and Outputs and with successful assignment it transits to state "Data_Exch" and waits for cyclic data exchange with its DP master. Within each of the states status requests are permitted at any time ("on Telegram" = per telegram request "Slave_Diag") [10].

4.6.2 Parameter Assignment Debloking

Due to a diagnosis message of the F slave that needs additional i-parameters or per external request the F host sets bit 0 ("parameter assignment deblocked") within the control byte of its next message. The F slave receives then via Write-Data-commands data set by data set the i-parameters and acknowledges at the end by setting bit 0 ("F slave has new i-parameter values assigned") within the status byte of its next message.

Remark: Debloking is only permitted, if there is no hazardous process state.
4.6.3 Interaction Diagrams for Parameter Assignments

Figure 4-31 Assigning "static" i-parameter from F host
4.7 Safe Alarm Generation

Due to swift polling in the user program, the speed of determining modifications of the F process data and the CRC is satisfactory.

There is no safety-related utilization of the alarm of the Profibus protocol.
4.8 Diagnosis

The safe diagnosis of F slave and communication failures is possible via the status byte. The F host provides means to count the number of reported erroneous communication messages during configurable time periods. If configurable upper limits are exceeded the safe control loop switches to a safe state. The F host supports monitoring of the number of reported erroneous communication messages.

Every standard diagnostic option of standard Profibus is possible.

4.9 F Module Commissioning / Repair Behavior

F modules can be replaced while the system is running. Restart of the corresponding safety control loop is only permitted, if there is no hazardous process state.

4.10 Reaction Times

The time between the "electrical" recognition of an emergency request and the "electrical" initiation of the safety reaction is relevant in safety technique. This response time consists of several individual time values including the bus transfer times.

![Diagram of reaction times]

Figure 4-33 Reaction times

+ input delay of the F input slave (operation time)
+ watchdog time "F communication": F input ↔ F-CPU
+ Scan rate or execution time in the F-CPU
+ watchdog time "F communication": F-CPU ↔ F input
+ output delay of the F output slave (operation time)

Compared with the standard, the safety profile requires additional execution time (F driver). The fact that a standard slave can extend the DP cycle time in the event of a failure shall also be taken into account.

DESINA requirement: 5 ms "single" bus transfer time is achieved.
4.11 Probabilistic Considerations

4.11.1 Calculations

To EN50159-1 and IEC61508, the following applies to SIL3:

\[ R_{DP} = R_{HW} + R_{EMI} + R_{IC} < 10^{-9} / h \]

The three terms are calculated as follows:

\[ R_{HW} (Hardware - failure) = (x1 \cdot \lambda_{HWF} + x2 \cdot \lambda_{HWS}) \cdot P_{US} \]

\[ \lambda_{HWF} = \text{failure probability of the HW of the 2 currently communicating F devices} \]
\[ \lambda_{HWS} = \text{failure probability of the HW of the max. 120 currently not communicating devices} \]
\[ x1 = \text{fraction (0...1) of the hazardous faults in the involved components} \]
\[ x2 = \text{fraction (0...1) of the hazardous faults by the components that are not involved} \]
\[ P_{US} = \text{max. residual error probability for 16/32-bit CRC, at a bit error rate of 0 ...0,5} \]

See chapter 4.11.2 “Operational Reliability of the Standard Profibus Components”.

\[ R_{EMI} (EMI - impact) = f_w \cdot P_{UB} \cdot P_{US} \]

\[ f_w = \text{Frequency of corrupted messages on the transmission system} \]
\[ P_{UB} = \text{Residual error probability for Profibus-DP at a bit error rate of } 10^{-4} (\text{EN60870-5-1}) \]
\[ P_{US} = \text{max. residual error probability for 16/32-bit CRC, at a bit error rate of 0 ...0,5} \]
To EN50159-1 this term is valid, if safety code (ProfiSafeCode) and transmission code (BusCode) are independent. The probabilities of both data integrity check mechanisms, parity and frame checking sequence from standard Profibus (HD=4) and CRC from ProfiSafe can be treated as independent since computer simulations did not show any significant "filter gaps".

Furthermore according to EN50159-1 the "properness" of the used CRC polynomials has to be proven. This requires calculation of the residual error rate (Pue) as a function of the bit error rate (epsilon) for a given polynomial, here for the 16 bit version (14EABh), as well as for the 32 bit version (1F4ACFB13h).

A polynomial will be assessed "proper" if there is no significant "humpback" curve with increasing bit error rate, i.e. if it rises monotonously.

The following figures are showing the diagrams for the 16 Bit polynomial:

Properness for **4 Bytes** of data:

![Diagram 16 Bit Polynomial 4 Bytes]

Properness for **8 Bytes** of data:

![Diagram 16 Bit Polynomial 8 Bytes]

© Copyright PNO 1999 – All Rights Reserved
Properness for **12 Bytes** of data:

![Graph for 12 Bytes](image)

Properness for **16 Bytes** of data:

![Graph for 16 Bytes](image)

In contrast a polynomial (199999331h) with worse Properness:

![Graph for Polynomial](image)
The following figures are showing the diagrams for the 32 Bit polynomial:

Properness for **52 Bytes** of data:

![Diagram showing properness for 52 Bytes]

Properness for **132 Bytes** of data:

![Diagram showing properness for 132 Bytes]

The third term covers the possible failures of the safety mechanisms (parity and frame checking sequence) within the Profibus-ASIC.

\[
R_{TC} \quad (Transmission\text{code}f\text{ailure}) = P_{\epsilon S} (typ) \cdot k_2 \cdot 1/T
\]

\[k_2 : \text{only one out of 10,000 HW failures creates a fault of the Profibus safety mechanisms (parity and frame checking sequence) on the ASIC that passes unrecognized, i.e. } k_2 = 1 \cdot 10^{-4} \text{ will be used for the estimates.}\]
The monitored time period wherein a well-defined maximum number of corrupted messages on the transmission system shall not exceed without the system switching into a safe state.

The reflections about $T$ lead directly to Fig. 4-32. The combination of the bus failure causes provides a (fictive) frequency of corrupted messages on the Profibus transmission system. The standard safety mechanisms of the Profibus (1. Filter) are recognizing every failure up to $HD=4$, thus only special bit patterns $HD>4$ are reaching the ProfiSafe safety mechanisms. For the number of unrecognized corrupted messages the worst case value of $2^{-n}$ shall not be taken ($n=16, \text{bzw } 32$), since the overall frequency of corrupted messages on the bus is continuously monitored.

![Diagram](image_url)

Figure 4-35  Monitoring of corrupted messages

If the safety mechanisms within the standard Profibus ASIC are failing (very little probability), then corrupted messages with statistical bit patterns are reaching the ProfiSafe safety mechanisms. In this case the more favourable value $P_{US}(typ)$ can be used for the estimate:

$$f_w \cdot \left\{ P_{UB}(typ) \cdot P_{US} + P_{US}(typ) \right\} = \frac{1}{T} \left( P_{UB}(typ) \cdot P_{US} + P_{US}(typ) \right) \leq R_{EMI}$$

The ProfiSafe profile allows simple monitoring of every corrupted message within the F host via the status byte within the acknowledgment of a F slave.

4.11.2 Operational Reliability of the Standard Profibus Components

In thousands of field applications, the Profibus has proven its reliability. Thus, it is obvious to determine practical base security of the Profibus to keep the effort required for the additional security layer as small as possible. Currently, this data is provided by return goods statistics that go down to component level. Components that are integrated into a "gray" channel are included (i.e. from the host down to the safety equipment in the slave). Information about the operational reliability can be found in Chapter 502.2 of DIN V VDE 0801 A1.

4.11.3 Practical Bit Error Rates of the Profibus

In order to support the stochastic considerations, the bit error rates of the Profibus as they are quoted in the literature shall be measured in practical examples. Besides cables and driver blocks, the data transmission procedure also plays a role. With Profibus-DP, this is RS485 and NRZ encoding; with Profibus-PA it is IEC1158-2 and Manchester-II encoding.
5 Using the PROFIBUS STANDARD

5.1 PROFIBUS Layers 1 and 2
The F profile is based on the Profibus services and specifications to EN 50170 Volume 2, that are required for Profibus-DP applications. The F profile does not require any additional layer 2 services.

5.2 PROFIBUS DP
PROFIBUS-DP to EN 50170 Volume 2 requires the base range (startup, cyclic transfer, and watchdog). Consistent transfer with a minimum of one F message frame byte shall be possible.

5.3 Definition of the "Gray" Channel
Here, the maximum topological structures as they are defined in the standard are used as the basis. For example, a maximum of three repeaters is currently permitted. Increasing this limit may be possible if more favorable failure rates of the F overall system will result in the course of the profile definition.

Any baud rate is permitted.

5.4 Standard EMC Requirements of the Profibus

5.4.1 CE Mark
All electrical devices that are put on the market and can generally be purchased shall carry the CE mark. A prerequisite of the CE mark is the conformity with the ENs that shall be declared by the company who launches the electrical device. An additional prerequisite is the conformity with the corresponding product standards during the development phase.

The EMC Directive affects all units, systems and plants that contain electrical or electronic components.

Applications:

<table>
<thead>
<tr>
<th>Industry</th>
<th>Separation from the public low-voltage mains by separate transformer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residential areas, office, light industry</td>
<td>Electrical energy is taken from the public low-voltage mains</td>
</tr>
<tr>
<td>Requirements</td>
<td>Limitation of the noise radiation and definition of the noise immunity of conducted and irradiated interference</td>
</tr>
<tr>
<td>Responsible</td>
<td>Manufacturer, importer, distributor</td>
</tr>
<tr>
<td>Mark</td>
<td>CE</td>
</tr>
</tbody>
</table>

Standards:

<table>
<thead>
<tr>
<th>Industry</th>
<th>EN 50082-2 Basic specification noise immunity, March 1995</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wohnbereich</td>
<td>EN 50082-1 Basic specification noise immunity, August 1997</td>
</tr>
</tbody>
</table>

5.4.2 Noise Emission
Not relevant with ProfiSafe.

5.4.3 Noise Immunity
Below, only the noise immunity characteristics for industrial applications are shown because they represent the most severe requirements.

See Chapter 5.4.11 for a definition of the assessment criteria.

5.4.4 On Long Signal Cables >10m
Long bus cables. Also laid together with process cables.
Test according to IEC 61000-4-4, 1995 “Electrical fast transient/burst immunity test” (Burst)
Test according to **IEC 61000-4-5, 1995** “Surge immunity test”

### 5.4.5 Static Discharge

Test according to **IEC 61000-4-2, 1995** “Electrostatic discharge immunity test”

### 5.4.6 High-Frequency Irradiation

Test according to **EN 61000-4-3, 1996** "Radiated Electromagnetic Field Requirements"

Test according to **ENV 50204, 1995** "Radiated electromagnetic field from digital radio telephones Immunity test”

### 5.4.7 HF-Induced Current on Cables and Cable Shields

Test according to **ENV 50141, 1993** "Immunity to conducted disturbances induced by RF fields" (corresponds to IEC 61000-4-6) and to **NAMUR** draft May 1998

### 5.4.8 Power Supply

Test according to **EN 61000-4-11, 1994**

### 5.4.9 Voltage Dips

<table>
<thead>
<tr>
<th>Reduction by</th>
<th>Duration</th>
<th>Assessment criterion</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 %</td>
<td>10 ms</td>
<td>B</td>
</tr>
<tr>
<td>60 %</td>
<td>100 ms</td>
<td>C</td>
</tr>
</tbody>
</table>

Sudden voltage change at zero crossing

### 5.4.10 Voltage Interruption

<table>
<thead>
<tr>
<th>Reduction by</th>
<th>Duration</th>
<th>Assessment criterion</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; 95 %</td>
<td>5000 ms</td>
<td>C</td>
</tr>
</tbody>
</table>

Sudden voltage change at zero crossing

### 5.4.11 Definition of the Malfunction

Reaction of the test object in its performance characteristic (function): Interpretation of "B” in F areas: The specified reaction denotes a fault reaction to a safe state; the communication functions remain working correctly. Usually after manual deblocking and a safety delay time the system returns to normal operation. The latter also is possible automatically with special applications in process industries.

<table>
<thead>
<tr>
<th>Assessment criterion</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function unit</th>
<th>Continuous interference (HF irradiation, HF-induced current, magnetic field)</th>
<th>Transient interference (Burst, ESD) on the bus</th>
<th>Surge on power supply, not on the fieldbus</th>
<th>Voltage interruption inside the permissible duration</th>
<th>Voltage interruption outside the permissible duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety equipment with ProfiSafe</td>
<td>no impairment</td>
<td>Fault reaction to a configured safe state</td>
<td>Fault reaction to a configured safe state</td>
<td>Fault reaction to a configured safe state</td>
<td>Fault reaction to a configured safe state; complete restart</td>
</tr>
</tbody>
</table>

### 5.5 Standard Installation Guidelines for Profibus

Necessary prerequisite for ProfiSafe communications is the observance of the **Installation Guidelines for Profibus-DP/FMS, V1.0**

September 1998, Order Nr. 2.112

During design phase of a F slave the appropriate standards regarding excess voltage and electric shock protection shall be observed.
6 Appendix

6.1 Measures against Failures before CRC2 Calculations

Failures may occur during acquisition and processing of individual device parameters. These aspects are not within the scope of this profile description but the main failure root causes and the appropriate remedial measures are mentioned.

<table>
<thead>
<tr>
<th>Parameter integrity</th>
<th>Addressing failures</th>
<th>Parametrization at the wrong point in time</th>
<th>Wrong sequence of the i-parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized access to the F device (slave or host)</td>
<td>partially</td>
<td><strong>X</strong></td>
<td></td>
</tr>
<tr>
<td>Address switches in field devices; unambiguous addresses</td>
<td></td>
<td><strong>X</strong></td>
<td></td>
</tr>
<tr>
<td>Complete functional testing</td>
<td><strong>X</strong></td>
<td><strong>X</strong></td>
<td><strong>X</strong></td>
</tr>
<tr>
<td>Teach-In; Self-Learning</td>
<td><strong>X</strong></td>
<td><strong>X</strong></td>
<td><strong>X</strong></td>
</tr>
<tr>
<td>Read-Back of the i-parameters from the field device via diverse path</td>
<td><strong>X</strong></td>
<td>partially</td>
<td><strong>X</strong></td>
</tr>
<tr>
<td>Read-Back of the i-parameters via a diverse path from F-host, that generates CRC2 across i-parameters also</td>
<td><strong>X</strong></td>
<td>partially</td>
<td><strong>X</strong></td>
</tr>
<tr>
<td>Diverse processing of the i-parameters (Acquisition and Test)</td>
<td><strong>X</strong></td>
<td>partially</td>
<td><strong>X</strong></td>
</tr>
<tr>
<td>Failsafe configuration of the i-parameters or failsafe engineering tool</td>
<td><strong>X</strong></td>
<td>partially</td>
<td><strong>X</strong></td>
</tr>
<tr>
<td>Version management of GSD type file and F device</td>
<td><strong>X</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For end-users a similar catalogue of failure / remedial measures shall be generated and processed.
### 6.2 CRC Calculation

This procedure detects 99.9985% of all errors that result from data modifications. It also discovers sequential errors because the signature check takes the sequence of the words into account.

For the 16-bit CRC code, the value \(14EAB\)h is used as the generator polynomial. The number of data bits may be odd or even. The value that is generated after the last byte corresponds to the transferred CRC code.

```pascal
procedure crc16(x: Byte; var r: word);
{ CRC – Pascal, using division procedure
 with every procedure call one Byte x will be operated;
 CRC value: r contains the 16 Bit of the CRC;
 The CRC value r(x) = CRC value of the F-parameters
 be initialized before the first call of a CRC calculation;
 Generator polynomial = 4eab hex }
const
  g = $4eab;
var
  i: byte;
beginn := 1 to 8 do
  begin
    if ( r and $8000) = 0 then
      begin
        if (x and $80) = 0 then r := r shl 1
          else r:= (r shl 1) xor 1;
      end
    else
      begin
        if (x and $80) = 0 then r := (r shl 1) xor g
          else r:= (r shl 1) xor g xor 1;
      end;
x := x shl 1;
  end;
end;
```

Figure 6-1 Typical procedure of a cyclic redundancy check

#### Runtime-optimized variant

The runtime-optimized variant for the calculation of the CRC code requires slightly more memory space, and is described below.

The following figure shows the signature generation using a CRC table:

```
<table>
<thead>
<tr>
<th>CRC-Table (16Bit, 256 elements):</th>
</tr>
</thead>
<tbody>
<tr>
<td>16-Bit signature of 0 (= 0h)</td>
</tr>
<tr>
<td>16-Bit signature of 1 (= 04EAbh)</td>
</tr>
<tr>
<td>16-Bit signature of 2 (= 09D68h)</td>
</tr>
<tr>
<td>. . . . . . . . . .</td>
</tr>
<tr>
<td>16-Bit signature of 253</td>
</tr>
<tr>
<td>16-Bit signature of 254</td>
</tr>
<tr>
<td>16-Bit signature of 255 (= 0C4B3h)</td>
</tr>
</tbody>
</table>
```

**Explanation:**

- 1. \(n = \text{(old signature } H\text{) XOR (act. Byte)}\)
- 2. \(H \oplus L\)
- 3. \(\text{old signature } L, L\)
- 4. \(\text{new signature } H, H\)

Figure 6-2 Using a CRC table for generating the signature
The values 0-255 that are encoded using the generator polynomial (here: $14EABh$) are specified in the word-structured CRC table.

1. First, the current byte is EXORED with the high part of the signature register.
2. The result is used as an offset to the table. The signature is read from the table.
3. The high byte of the word from the table is EXORED with the low byte of the old signature. The result is the new byte of the signature.
4. The low byte of the word from the table is the new low byte of the signature.

These operations are only performed once for a byte.

The corresponding formula for the 16 Bit CRC calculations is: \[ r = \text{crctab16}[(r >> 8) ^ *q++] ^ (r << 8) \]
And its corresponding table:

<table>
<thead>
<tr>
<th>Hex</th>
<th>CRC16</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000</td>
<td>04EB</td>
</tr>
<tr>
<td>09EB7</td>
<td>D01C</td>
</tr>
<tr>
<td>0D3C5</td>
<td>0D3E</td>
</tr>
<tr>
<td>0DE7A</td>
<td>0E9D</td>
</tr>
<tr>
<td>0E78A</td>
<td>0E79</td>
</tr>
<tr>
<td>0F93D</td>
<td>0FBB</td>
</tr>
<tr>
<td>0F94F</td>
<td>0D4A</td>
</tr>
<tr>
<td>0AA45</td>
<td>0A55</td>
</tr>
<tr>
<td>0F01F</td>
<td>0FA5</td>
</tr>
<tr>
<td>0FA8B</td>
<td>0C5EC</td>
</tr>
<tr>
<td>0BBF8</td>
<td>0C5E</td>
</tr>
<tr>
<td>0BBF6</td>
<td>0C4B3</td>
</tr>
</tbody>
</table>

And its corresponding formula for the 16 Bit CRC calculations is: \[ r = \text{crctab16}[(r >> 8) ^ *q++] ^ (r << 8) \]
And its corresponding table:

<table>
<thead>
<tr>
<th>Hex</th>
<th>CRC32</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000</td>
<td>F44CB13</td>
</tr>
<tr>
<td>07DA54D0</td>
<td>853F67C</td>
</tr>
<tr>
<td>0EFA69A8</td>
<td>1B081F2</td>
</tr>
<tr>
<td>098C57D7</td>
<td>6DC0A66F</td>
</tr>
<tr>
<td>02B8C243</td>
<td>0DF50D50</td>
</tr>
<tr>
<td>05C81C97</td>
<td>A8847E74</td>
</tr>
<tr>
<td>0C4541EB</td>
<td>0FBBF9DF</td>
</tr>
<tr>
<td>0B38075F</td>
<td>472C8E2</td>
</tr>
<tr>
<td>075F80B6</td>
<td>0A54A9B5</td>
</tr>
<tr>
<td>02CCE652</td>
<td>D408F49</td>
</tr>
<tr>
<td>0B50392E</td>
<td>4CCFC23D</td>
</tr>
<tr>
<td>0C4840DF</td>
<td>3B2F6E9</td>
</tr>
<tr>
<td>07C047C5</td>
<td>8AB83D6</td>
</tr>
<tr>
<td>08D04C11</td>
<td>F7FCT02</td>
</tr>
<tr>
<td>095C11ED</td>
<td>6707EAC</td>
</tr>
<tr>
<td>0E7A95F9</td>
<td>5BB04A4</td>
</tr>
<tr>
<td>0AFFA10C</td>
<td>5B5C5A1F</td>
</tr>
<tr>
<td>0D8249D8</td>
<td>2C866ECB</td>
</tr>
<tr>
<td>054CA3C7</td>
<td>B3D4AD0</td>
</tr>
<tr>
<td>0684A0E7</td>
<td>9F081BF4</td>
</tr>
<tr>
<td>1C7D043</td>
<td>E8DCF24</td>
</tr>
<tr>
<td>0F88B18A</td>
<td>0CA4A99</td>
</tr>
<tr>
<td>08FDC55E</td>
<td>7B073E4D</td>
</tr>
<tr>
<td>17A0962</td>
<td>E30G635</td>
</tr>
<tr>
<td>0674ACF5</td>
<td>94D5B7ES</td>
</tr>
<tr>
<td>0D3F40ED</td>
<td>275822DD</td>
</tr>
<tr>
<td>0BBF88B5</td>
<td>B2F74FA6</td>
</tr>
<tr>
<td>0BBF88B5</td>
<td>B2F74FA6</td>
</tr>
</tbody>
</table>

And its corresponding formula for the 32 Bit CRC calculations is: \[ r = \text{crctab32}[(r >> 24) ^ *q++] & 0xff \]
6.3 Sample GSD File for a modular F Slave

; Sample GSD file for a slave with F-module parametrization
; demonstration only, no real product
; File name : SIEM2222.GSD
; Revision : 1.1 Bitmap SX
; Last changes : 17-Feb-1999

#Profibus_DP
Vendor_Name = "SIEMENS AG"
GSD_Revision = 2
Model_Name = "F-Device"
Revision = "1.0"
Ident_Number = 0x2222
Protocol_Ident = 0 ; 0 = PROFIBUS-DP
Slave_Family = 9 ; = Others
Prtm_Struct_supp = 1 ; 1 = block structure supported
Station_Type = 0 ; 0 = DP-Slave
FMS_supp = 0 ; no FMS/DP mixed device
F_Device_supp = 1 ; 1 = F-device (launches "F-Control" within parametrization tool)
Hardware_Release = "A1"
Software_Release = "V1.0"
9.6_supp = 1
19.2_supp = 1
93.75_supp = 1
187.5_supp = 1
500_supp = 1
1.5M_supp = 1 ; 9.6 up to 12,000 Kbaud supported
3M_supp = 1
6M_supp = 1
12M_supp = 1
MaxTsdrl_9.6 = 60
MaxTsdrl_19.2 = 60
MaxTsdrl_93.75 = 60
MaxTsdrl_187.5 = 60
MaxTsdrl_500 = 100
MaxTsdrl_1.5M = 150
MaxTsdrl_3M = 250
MaxTsdrl_6M = 450
MaxTsdrl_12M = 800
Redundancy = 0 ; redundancy not supported
Repeater_Ctrl_Sig = 2
24V_Pins = 0
Bitmap_Device = "UNIVSLVE"

;Slave specific data

;Text definition for User_Prm_Data
PrtmText = 1 ; Reference number 1
Text(0) = "SIL 1"
Text(1) = "SIL 2"
Text(2) = "SIL 3"
Text(3) = "SIL 4"
EndPrtmText

;Text definition for Check/no check
PrtmText = 2 ; Reference number 2
Text(0) = "No Check"
Text(1) = "Check"
EndPrmText
;
:Text definition for CRC-Length
:
PrmText = 3 ; Reference number 3
Text(0) = "2 Byte CRC"
Text(1) = "4 Byte CRC"
EndPrmText
;
: Ext-User-Prm-Data-Def-List:
:
:User_Prm_Data definition 1
ExtUserPrmData = 1 "Slot" ; Reference number 1
Unsigned8 1 1-254 ; Default = 1, Max = 254
EndExtUserPrmData
;
:User_Prm_Data definition 2
ExtUserPrmData = 2 "F_Prm_Flag" ; Reference number 2
Unsigned16 0 0-65535 ; Default = 0, Max = 65535
EndExtUserPrmData
;
:User_Prm_Data definition 3
ExtUserPrmData = 3 "F_Dest_Add" ; Reference number 3
Unsigned16 1 1-65534 ; Default = 1, Max = 65534
EndExtUserPrmData
;
:User_Prm_Data definition 4
ExtUserPrmData = 4 "F_Source-Add" ; Reference number 4
Unsigned16 1 1-65534 ; Default = 1, Max = 65534
EndExtUserPrmData
;
:User_Prm_Data definition 5
ExtUserPrmData = 5 "F_WD-Time" ; Reference number 5
Unsigned16 3 0-65535 ; Default = 3, Max = 65535, Manufacturer defines
EndExtUserPrmData ; maximum device operation time via default value
;
:User_Prm_Data definition 6
ExtUserPrmData = 6 "F_SIL " ; Reference number 6
BitArea(2-3) 1 0-3 ; Default = 1, Min = 0, Max = 3
Prm_Text_Ref = 1 ; Pointer to text definition 1
EndExtUserPrmData
;
:User_Prm_Data definition 7
ExtUserPrmData = 7 "F_Check_SeqNr" ; Reference number 7
Bit(0) 0 ; Default = 0,
Prm_Text_Ref = 2 ; Pointer to text definition 2
EndExtUserPrmData
;
:User_Prm_Data definition 8
ExtUserPrmData = 8 "F_Check_iPar" ; Reference number 8
Bit(1) 0 ; Default = 0,
Prm_Text_Ref = 2 ; Pointer to text definition 2
EndExtUserPrmData
;
:User_Prm_Data definition 9
ExtUserPrmData = 9 "F_CRC_Length" ; Reference number 9
BitArea(4-5) 2 0-3 ; Default = 2, Min = 0, Max = 3

© Copyright PNO 1999 – All Rights Reserved
Prm_Text_Ref = 3 ; Pointer to text definition 3
EndExtUserPrmData
;
;***************************
;***************************
;
Freeze_Mode_supp = 0 ; Freeze-Mode not supported
Sync_Mode_supp = 0 ; Sync.-Mode not supported
Auto_Baud_supp = 1 ; automatic Baudrate check
Max_Diag_Data_Len = 6
Set_Slave_Add_supp = 1
User_Prm_Data_Len = 100 ; Length of the total User-Prm-Data
Min_Slave_Intervall = 6 ; 0.6ms
Modular_Station = 1
Max_Module = 5 ; max. Nr. of modules to choose from
Max_Input_Len = 100
Max_Output_Len = 100
Max_Data_Len = 200
;
Module = "F-Module 16Byte-E 4Byte-A" 0xC0, 0x83, 0x8f
F_Device_supp = 1 ; F-Slave
Ext_Module_Prm_Data_Len = 12
Ext_User_Prm_Data_Const(0) = 12 ; predefined F_Prm-Block length
Ext_User_Prm_Data_Const(1) = 4 ; predefined F_Prm-Block identifier
Ext_User_Prm_Data_Const(2) = 0 ; predefined Slot number
Ext_User_Prm_Data_Const(3) = 0 ; predefined Specifier
Ext_User_Prm_Data_Const(4) = 0x00 ; predefined F_Prm-Flag high
Ext_User_Prm_Data_Const(5) = 0x00 ; predefined F_Prm-Flag low
Ext_User_Prm_Data_Ref(2) = 1
Ext_User_Prm_Data_Ref(4) = 7
Ext_User_Prm_Data_Ref(4) = 8
Ext_User_Prm_Data_Ref(4) = 6
Ext_User_Prm_Data_Ref(4) = 9
Ext_User_Prm_Data_Ref(6) = 3
Ext_User_Prm_Data_Ref(8) = 4
Ext_User_Prm_Data_Ref(10) = 5
EndModule
Module = "F-Modul 16Word-E 16Byte-A" 0xC0, 0x8f, 0x9f
F_Device_supp = 1 ; F-Slave
Ext_Module_Prm_Data_Len = 12
Ext_User_Prm_Data_Const(0) = 12 ; predefined F_Prm-Block length
Ext_User_Prm_Data_Const(1) = 4 ; predefined F_Prm-Block identifier
Ext_User_Prm_Data_Const(2) = 0 ; predefined Slot number
Ext_User_Prm_Data_Const(3) = 0 ; predefined Specifier
Ext_User_Prm_Data_Const(4) = 0x00 ; predefined F_Prm-Flag high
Ext_User_Prm_Data_Const(5) = 0x00 ; predefined F_Prm-Flag low
Ext_User_Prm_Data_Ref(2) = 1
Ext_User_Prm_Data_Ref(4) = 7
Ext_User_Prm_Data_Ref(4) = 8
Ext_User_Prm_Data_Ref(4) = 6
Ext_User_Prm_Data_Ref(4) = 9
Ext_User_Prm_Data_Ref(6) = 3
Ext_User_Prm_Data_Ref(8) = 4
Ext_User_Prm_Data_Ref(10) = 5
EndModule
;
Module = "E-/A-Modul" 0xF4 ; standard I/O module
; consistency, 5 Words Inputs and Outputs
EndModule
6.4 Applicable Documents

[7] prEN 50159-1: (Railway Applications) "Requirements for Safety-Related Communication in Closed Transmission Systems 

6.5 Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>American Standard Code for Information Interchange</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application Specific Integrated Circuit</td>
</tr>
<tr>
<td>C</td>
<td>Coverage</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check [9], [11]</td>
</tr>
<tr>
<td>DB</td>
<td>Data Block</td>
</tr>
<tr>
<td>DDL</td>
<td>Device Description Language</td>
</tr>
<tr>
<td>DIN</td>
<td>Deutsches Institut für Normung (German Institute for Standards)</td>
</tr>
<tr>
<td>DKE-AK</td>
<td>Working Group of the German Electrotechnical Commission within DIN and VDE</td>
</tr>
<tr>
<td>DP</td>
<td>Decentralized Peripherals</td>
</tr>
<tr>
<td>EMI</td>
<td>Electro Magnetic Interference</td>
</tr>
<tr>
<td>EN, prEN</td>
<td>European Norm, preliminary ...</td>
</tr>
<tr>
<td>ESD</td>
<td>ElectroStatic Discharge</td>
</tr>
<tr>
<td>F</td>
<td>Failsafe</td>
</tr>
<tr>
<td>FB</td>
<td>Function Block</td>
</tr>
<tr>
<td>GSD</td>
<td>Geräte-Stamm-Daten (Device Data Base)</td>
</tr>
<tr>
<td>HD</td>
<td>Hamming Distance</td>
</tr>
<tr>
<td>HW</td>
<td>Hardware</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>ISO/OSI</td>
<td>International Standards Organization / Open Systems Interconnection (Reference Model)</td>
</tr>
<tr>
<td>M</td>
<td>Module</td>
</tr>
<tr>
<td>PA</td>
<td>Process Automation</td>
</tr>
<tr>
<td>PES</td>
<td>Programmable Electronic (Safety-Related) System</td>
</tr>
<tr>
<td>PG/ES</td>
<td>Programmer/Engineering Station</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>S</td>
<td>Standard</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>SW</td>
<td>Software</td>
</tr>
<tr>
<td>TPDU</td>
<td>(Transport) Protocol Data Unit [9]</td>
</tr>
<tr>
<td>VDE</td>
<td>Association of German Electrical Engineers VDE</td>
</tr>
<tr>
<td>VDI</td>
<td>Association of Engineers VDI</td>
</tr>
<tr>
<td>XML</td>
<td>Extendable Markup Language (World Wide Web Consortium)</td>
</tr>
</tbody>
</table>