Løsninger

- Historikk
- Applikasjoner
- Løsninger
  - Arbeidsmetoder
  - Kontroller / Basis System
  - Inngangs og utgangs moduler
  - Human - Machine Interface
  - Programvare /programmering
  - Communications
The prevention of accidents should not be considered a question of legislation, but instead our responsibility to fellow beings and economic sense

(Werner von Siemens in 1880)
Siemens Safety Systems.

- First project 1985, Oseberg Feltsenter
- To day nearly 30% of installed safety systems in Norwegian part of the North Sea.
- First solutions, Simatic PLC's with additional hardware, 2 PLC's running independently.
- Late in the eighties the first TÜV approved F systems.
- To-day a full range of S7 F, TÜV verified systems,
- Work procedures according to IEC61508, SINTEF verified
Siemens Safety Systems applications are based on long experience

- Stena Don 2000
- Statfjord A 2000
- Snorre B 2000
- Huldra 2000
- Oseberg South 2000
- Embla 2000
- Oseberg Gas 1999
- Troll C 1999
- Statfjord B 1998
- Visund 1998
- Eldfisk WIP 1999
- Oseberg East 1997

- Petrojarl Foinhaven 1996
- Njord A & B 1995
- Statfjord C 1995
- Vigdis 1995
- Ekofisk 1995
- Eldfisk alpha 1993
- Brage 1992
- Embla 1991
- Snorre TLP 1990
- Oseberg A 1988
- Oseberg B 1987
Siemens Safety Systems.

S7 400F(H) References (running or under construction)

- HULDRA (Norway) 2000
- MAERSK XL1 (worlds largest jack up, built in Korea) 2002
- EKOFISK 2/7A (installation partly on hold) 2002
- HALFDAN HBA (built in Holland) 2002
- MAERSK XL2 (built in Korea) 2002
- Halfdan 5 platforms (Denmark/built in Singapore and Holland) 2003-2006
- Al Shaheen (11 platforms in Qatar) 2003
- White Rose FPSO (Canada/built in Canada/Korea/Abu Dhabi/USA) 2005
- P50, Albacore Leste FPSO (Brazil) 2005
- PRA1 (Brazil) 2005
- Santa Fe (USA, 2 drilling Rigs) 2004
- Oseberg Field-centre (Norway) (113 off S7 400/400FH, 35000 I/O) 2005-2007
- Statfjord A/B/C ESD and F&G 2004-2006
- SSP300-1/2/3 (China/Brazil/UK/Norway) 2005-2007
- Blackford Dolphin 2006
- Snorre TLP 2006
Hva er et sikkerhetssystem (SIS)?

Disaster protection
Collection basin
Overpressure valve, rupture disc
Safety system (automatic)
Plant personnel intervenes
Basic automation

Disaster protection
Passive protection
Active protection

Safety shutdown
Safety Instrumented System (SIS)
Process alarm
Process control system
Normal activity
Process value
Hva er et sikkerhetssystem?

Low level

I / P

Reactor  PT 1A  PT 1B

PT

FT

Basic Process Control System (BPCS)

Inputs  Outputs

Safety Instrumented System (SIS)

Inputs  Outputs

Computer

Detectors

Logic solver

Actuating items
Og hva med “Equipment Under Control”, EUC?
Safety Systems Applications

Purpose

Risk reduction by safety systems, SIS

Residual Risk
Tolerable Risk
EUC risk

From IEC 61508:

Necessary Risk Reduction
Actual Risk Reduction
Increasing Risk

Risk reduction achieved by all safety-systems
Safety Systems Applications

What is Risk?
Who decides what is acceptable risk?

Examples of fatality risk figures

- Road accident 100cpm 1.0x10^-4/yr 1 av 100 (levetid 100 år)
- Car accident 150cpm 1.5x10^-4/yr 1,5 av 100
- Accident at work 10cpm 1.0x10^-5/yr 1 av 1000
- Falling Aircraft 0.02 cpm 2.0x10^-8/yr 2 av 1000 000
- Lightning strike 0.1cpm 1.0x10^-7/yr 1 av 100 000
- Insect/Snake bite 0.1cpm 1.0x10^-7/yr 1 av 100 000
- Smoking 20 per day 5000 cpm 5.0x10^-3/yr 1 av 2

cpm = chances per million of the population
Risk reduction by safety systems, SIS

- Containment Dike
- Control System
- Operator Intervention
- SIL1
- SIL2
- SIL3
- Safety Instrumented Function

Hazard #1

Likelihood vs. Consequence graph with Tolerable Risk Region and Unacceptable Risk Region.
Safe state?

Can the Safety System bring the area or equipment to a safe state?

How?

What is required?
Applications Covered

- ESD, Emergency Shutdown
- F&G, Fire & Gas Detection, Fire-fighting
- Process Shutdown
- Fire-pump Logic
- Ballast Control
- Blow-down
- Riser release / Anchor Release
- Fire Dampers, Active Smoke Control
- HIPPS, High Integrity Pressure Protection System
Siemens Safety Systems,
Topology for total platform control system including safety

Solutions for Oil & Gas

A.O.Sveen, NTNU 2007
Fire & Gas Topology (sample)

Software is implemented according to procedure, SIL 3
Hardware design according to procedure, SIL 3

Remote "fail safe" input/output modules
F-SM's, SIL 2/3

Remote Input / Output modules, S1 or ET200M SIL0/1

Detectors (Sil2)  Fire Panel (Sil2)  PROFIBUS/Profisafe (Sil3)

S7-400FH (Sil3, and redundant)  Controller Cabinet

S7-400FH (Sil3)  S7-400F (Sil3)

F&G ESD Wide Screen Overview

Ethernet 100 Mbit

Communication to other nodes SIL 3

SIL 0/2/3

Operator Stations

Industrial Ethernet 100 Mbit

REDUNDANT SAFETY SERVERS

Built-in redundancy and self-diagnosis

Ethernet 100 Mbit
F&G System Topology (the different modules)

- **F&G Matrix**
- **Redundant Fail Safe Communications – SIL3 (Profisafe)**
- **Addressable Fire Detection Systems**
- **Redundant Communications Interface**
- **Fail Safe I/O Modules**
- **High Available & Fail Safe CPU’s**
- **Redundant Safety Servers**
- **Redundant Integrated Safety & Process Network**

**Note:** Separate bus systems are used for interface to matrixes to avoid common mode failures with field I/O.
ESD Topology (sample)

Controller Cabinet

- S7-400F(SIL3)
- PROFIBUS/ProfiSafe (SIL3)
- S7-400FH (SIL3, and redundant)
- Software is implemented according to procedure, SIL 3
- Hardware design according to procedure, SIL 3

Operator Stations

- Engineering Station
- Redundant Safety Servers (built-in redundancy and auto-repair)
- Communications to other nodes SIL3
- Ethernet 100 Mbit
- Communication to F&G ESD Wide Screen Overview

Field Termination Cabinet

- Remote Input/Output modules, F-SM SIL2/3 or ET200M SIL0/1
- F&G ESD Wide Screen Overview
- Remote Input/Output modules, IS1 or ET200M SIL0/1

Remote "fail safe" Input/output modules F-SM’s, SIL 2/3

Commands from OS to SIL3

- PROFIBUS/ProfiSafe (SIL3)
- Remote Input/Output modules, F-SM SIL2/3 or ET200M SIL0/1

A.O.Sveen, NTNU 2007
PSD Topology (sample)

Operator Stations

Engineering Station

Controller Cabinet

Remote ET200iS or "fail safe" Input/output modules F-SM's, SIL 2/3

Field Termination Cabinet or Junction Box

Remote Input/Output modules, IS1 or ET200M SIL0/1

Software is implemented according to procedure, SIL 3

Hardware design according to procedure, SIL 3

Commands from OS to SIL 3

Ethernet 100 Mbit

Redundant Servers

Industrial Ethernet 100 Mbit

Communication to other nodes SIL 3

PROFIBUS/Profisafe (SIL3)
Marine Control System (SIL 3)

Controller Cabinet A
- S7-400F(SIL3)
- A CPU
- Remote "fail safe" Input/output modules F-SM's, SIL 2/3
- PROFIBUS/ProfiSafe (SIL3)

Controller Cabinet B
- S7-400F(SIL3)
- B CPU

Remote Input / Output modules, IS1 or ET200M SIL0/1

Field Termination Cabinet or Junction Box

S7-400FH (SIL3, and redundant)

Communication to other nodes SIL3

Commands from OS to SIL3

Redundant Servers

Industrial Ethernet 100 Mbit

Siemens

Software is implemented according to procedure, SIL 3
Hardware design according to procedure, SIL 3

Manual Ballast Functions

Synchronization link

Remote "fail safe" Input/output modules F-SM's, SIL 2/3
Subsea PSD solution and HIPPS, both SIL3
- The safety level is applicable for:
  - The total solution
  - All the projects lifecycles

- The system solution covers EUC, including HMI
  - HW engineering, construction and testing
    - By use of standard hardware set-up
    - With special modules approved by TÜV

- Software
  - Function blocks (basic blocks approved by TÜV)
  - Protocols and drivers approved by TÜV
  - Application program (according to procedure)

- Maintenance procedures
- Operation and Modification Procedures
IEC 61508, Quality Assurance and some direct requirements

Software safety lifecycle

9.1 Software safety requirements specification
9.1.1 Safety functions requirements specification
9.1.2 Safety integrity requirements specification

9.2 Software safety validation planning

9.3 Software design and development

9.4 PE integration (hardware/software)

9.5 Software operation and modification procedures

9.6 Software validation

To box 12 in figure 2 of part 1

To box 14 in figure 2 of part 1

NOTE 1 Activities relating to verification, management of functional safety and functional safety assessment are not shown for reasons of clarity but are relevant to all overall, E/E/PES and software safety lifecycle phases.

NOTE 2 The phases represented by boxes 10 and 11 are outside the scope of this standard.

NOTE 3 Parts 2 and 3 deal with box 9 (realisation) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.
Safety requirements shall be specified, and the requirements shall be traceable through all engineering phases.

◆ Internal procedures for development of software according to IEC61508
  ● Procedures developed in co-operation with SINTEF Tele and Data.
    – specification
    – planning
    – implementation
    – verification
    – validation
    – modifications.

◆ Internal procedures for hardware design and production according to IEC61508
  ● Made on the same structure as the SINTEF verified SW procedure.
Risk Determination (one of several methods)

Risk Graph

S: Severity of injury/damage
1: small injury, minor environmental damage
2: serious irreversible injury of many people involved or a death temporary serious environmental damage
3: death of many people long-term serious environmental damage
4: catastrophic results, many deaths

F: Frequency and/or exposure time to hazard
1: seldom - quite often
2: frequent - continuous

A: Avoiding hazard
1: possible
2: not possible

P: Probability of Occurrence
1: very low
2: low
3: relatively high

_required Safety Integrated Level (SIL) of the Safety System_
## Safety Integrity Levels, direct requirement IEC61508

<table>
<thead>
<tr>
<th>Requirement Class (AK) DIN V 19250</th>
<th>Safety Integrity Level (SIL) IEC 61508</th>
<th>Probability of failure on demand per h (constant operation) (IEC 61508)</th>
<th>Probability of failure on demand (on demand operation) (IEC 61508)</th>
<th>Control Category EN 954-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>AK 1</td>
<td>---</td>
<td>--</td>
<td>--</td>
<td>B</td>
</tr>
<tr>
<td>AK 2 and 3</td>
<td>SIL 1</td>
<td>10⁻⁵ to 10⁻⁶</td>
<td>10⁻¹ to 10⁻²</td>
<td>1 and 2</td>
</tr>
<tr>
<td>AK 4</td>
<td>SIL 2</td>
<td>10⁻⁶ to 10⁻⁵</td>
<td>10⁻² to 10⁻³</td>
<td>3</td>
</tr>
<tr>
<td>AK 5 and 6</td>
<td>SIL 3</td>
<td>10⁻⁷ to 10⁻⁸</td>
<td>10⁻³ to 10⁻⁴</td>
<td>4</td>
</tr>
<tr>
<td>AK 7 and 8</td>
<td>SIL 4</td>
<td>10⁻⁸ to 10⁻⁹</td>
<td>10⁻⁴ to 10⁻x</td>
<td>---</td>
</tr>
</tbody>
</table>

- Independent Authority (*e.g. TÜV*) classifies control systems according to their safety measures
Safety Integrity Levels, direct requirement IEC61508
IEC61508 requires higher fail safe fraction from “intelligent” components

Hardware safety integrity: architectural constraints on type A safety-related subsystems

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>&lt; 60 %</td>
<td>SIL1</td>
</tr>
<tr>
<td>60 % - 90 %</td>
<td>SIL2</td>
</tr>
<tr>
<td>90 % - 99 %</td>
<td>SIL3</td>
</tr>
<tr>
<td>&gt; 99 %</td>
<td>SIL4</td>
</tr>
</tbody>
</table>

Hardware safety integrity: architectural constraints on type B safety-related subsystems

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>&lt; 60 %</td>
<td>not allowed</td>
</tr>
<tr>
<td>60 % - 90 %</td>
<td>SIL1</td>
</tr>
<tr>
<td>90 % - 99 %</td>
<td>SIL2</td>
</tr>
<tr>
<td>&gt; 99 %</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

A.O.Sveen, NTNU 2007
Safety Integrity Levels, PFD calculation

F&G loop with Gas detector and control valve.

Safety reliability Block diagram:
Components S7-400F/FH

- High available System S7-417FH as a basis
  - CPU 417-4H
  - TÜV certified failsafe function blocks

- Engineering /Hardware Configuration/Programming
  - Configuration of the S7-400F-Hardware with Standard HW-Config.
  - Graphical Engineering (programming) with Standard CFC (Continuous Function Chart)
  - TÜV certified failsafe function blocks in a separate library (failsafe function blocks to be used in the fail safe part)
  - Coexistence of Standard- and F-Applications in one CPU

- Connection to the Process
  - Failsafe I/O modules
  - Special Profil PROFIsafe to ensure failsafe communication via Standard-Profibus-DP
Basic principle “Protected F-Islands”

- CPU hardware
- Standard user programs
- Any faults in other modules, environmental factors
- Safety-related user program
- Failsafe I/O modules
- Safety-related frame
S7 400F F/H system - modularity,

- Standard Engineering Software
- Standard-CPU 417-4H
- Standard I/O’s (ET200M)
- Standard-ProfibusDP
- ProfiSafe Protocol
- F-Programming Tool
- F-Application Program
- F-I/O’s (ET200M)
S7-400H
Redundancy Principle

PROCESS

Synchronization, information and status exchange
I/O Configuration
Switching of master by use of redundant Profibus

Target:
Reduce common mode faults for the switch-over to a minimum

Achieved by:
Very simple component does the switchover

Redundant IM 153-2
IO with active backplane bus performing the switchover

Profibus-DP

L+
L+

Active backplane bus

Bus module

IM

IM
Redundant S7-400H
A Synchronization Procedure is required

Synchronization of all commands whose execution would trigger different states in both partial PLCs
Flexible Set-up’s
Together, the listed principles result in a flexible set-up

Fail Safe
- AS 414 F
- AS 417 F
- ET 200M
- F-I/O Modules
- IM 153
- Safety Module
- Standard I/O Modules
- S7-400F
- PROFIBUS-DP
- F-E/A Moduls
- SIL 3, AK6

Fail Safe and High Availability
- redundant S7-400FH
- redundant PROFIBUS-DP
- redundant F-E/A Moduls
- SIL 3, AK6
- AS 414 F
- AS 417 F
- ET 200M
- F-I/O Modules
- IM 153-2
- Safety Module
- Standard I/O Modules
Flexible Set-up’s

- Mix to meet the goals of the application
- Field Device redundancy can be designed to achieve safety and availability goals
- CPU/IO safety is not dependant on redundancy
  - All components are SIL3-capable
  - Redundancy only for availability
Flexible Set-up’s

- IO and Field Device redundancy can be matched to:
  - Minimize cost
  - Maximize availability
Flexible Set-up's

- Multiple Fault Tolerant
  - Fieldbus architecture allows system to tolerate multiple faults without interruption
  - I/O redundancy independent of CPU redundancy
- All components rated for SIL3
  - No degraded mode
  - Safety not dependent on redundancy
Alternative setup by others

Fail Safe and High Availability (sample from Triconex) due to 2003 HW voting
Input and output modules to SIL 3, 2 and 1

- **F-SM, Fail Safe Modules**
  - SIL3, 2 or 1 dependant on configuration (TÜV)
    - SIL 3 also in single configuration for most modules
    - SIL 3 with single or redundant bus connection
  - Allows standard modules on same bus

- **ET 200 M**
  - Can also cover SIL1 and SIL2 solutions

- **ET200 iSP**
  - Small granularity modules for Zone 1, can also cover SIL1 applications
F-Digital Output, with built in redundancy, self verification and degrading

If "Output driver" fails to bring output to safe state, "0", the microcontroller does, based on the read back, order the "Second disconnection facility" to shut the card down.
S7-300 Fail Safe Modules

- **Redundant microcontroller in each IO module**
- **Safety Integrated Level**
  - 1oo1 evaluation, SIL 2, AK 4
  - 1oo2 evaluation, SIL 3, AK 6
- **Diagnose of internal and external errors**
  - mutual function checking of the microcontrollers
  - input or output test
  - branching of the input signals to both microcontrollers
  - discrepancy analysis of the redundant input signals
  - readback of the output signals and discrepancy analysis
- **Second disconnection facility in the case of outputs**
- **Communication with CPU via Profisafe**
A large number of modules are available

- **SM326F, DI  DC24V**
  24 x SIL2, 12 x SIL3, with diagnostics interrupt

- **SM326F, DI  NAMUR [EEEx ib]**
  8 x SIL2, 4 x SIL3 with diagnostics interrupt

- **SM326F, DO  DC24V/2A**
  10 x SIL3, current source, diagnostics interrupt

- **SM336F, AI  4-20mA**
  6 x SIL2 or 3, with diagnostics interrupt

- and more
Fail Safe I/O Modules
Library for interfaces to field devices

Library with standard, pre-verified instrument interfaces
(made in Norway)

**SAFETY INPUTS AND OUTPUTS, S7 400F WITH SAFETY I/O MODULES, F-SM’S**

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI-41F</td>
<td>Safe analogue input, 4-20 mA, 2 Wire, SIL 2.</td>
</tr>
<tr>
<td>AI-43F</td>
<td>Safe analogue input, 4-20 mA, 3 Wire, SIL 2, current source</td>
</tr>
<tr>
<td>AI-44F</td>
<td>Safe analogue input, 4-20 mA, 3 Wire, SIL 2, high power consumpt.</td>
</tr>
<tr>
<td>AI-50F</td>
<td>Safe high available analogue input, 4-20 mA, 2 Wire, 2 coil 3.</td>
</tr>
<tr>
<td>AI-51F</td>
<td>Safe analogue input, 4-20 mA, 2 wire, to digital, SIL 2</td>
</tr>
<tr>
<td>AI-IS-41F</td>
<td>Safe analogue input, 4-20 mA, EEx (i)(a), 2 Wire, SIL 2.</td>
</tr>
<tr>
<td>AI-IS-51F</td>
<td>Safe analogue input, EEx ib IIC, 4-20 mA, to digital, SIL 2</td>
</tr>
<tr>
<td>DI-41F</td>
<td>Safe digital input, SIL 2</td>
</tr>
<tr>
<td>DI-42F</td>
<td>Safe high available, digital input, SIL 2</td>
</tr>
<tr>
<td>DI-44F</td>
<td>Safe digital input from clean contact / NAMUR, SIL2</td>
</tr>
<tr>
<td>DI-IS-41F</td>
<td>Safe, EEx ib IIC, digital input from clean contact / NAMUR, SIL2</td>
</tr>
<tr>
<td>DI-IS-46F</td>
<td>Safe, high available, EEx ib IIC, double clean contact /NAMUR, SIL2 /</td>
</tr>
<tr>
<td>DI-IS-46F</td>
<td>Safe, EEx ib IIC, double clean contact /NAMUR, SIL3.</td>
</tr>
<tr>
<td>DO-41F</td>
<td>Safe, digital output, 24 V DC, 2A, SIL2 / 3</td>
</tr>
<tr>
<td>DO-41FR</td>
<td>Safe digital output, SIL 2 with relay, SIL2</td>
</tr>
<tr>
<td>DO-RE-45F</td>
<td>Safe, high available, digital output, 24 V DC, 2A, SIL2 / 3</td>
</tr>
<tr>
<td>DO-46F</td>
<td>Safe, digital output with manual release, 24 V DC, 2A, SIL2 / 3</td>
</tr>
<tr>
<td>DI-MA-41F</td>
<td>Safe, high available digital input from pushbutton, SIL 3</td>
</tr>
<tr>
<td>DI-MA-42F</td>
<td>Safe, high available digital input from pushbutton, SIL 2</td>
</tr>
<tr>
<td>DI-MA-44F</td>
<td>Safe, digital input from pushbutton, SIL 3</td>
</tr>
<tr>
<td>DI-MA-45F</td>
<td>Safe, high available digital input from pushbutton, SIL 3</td>
</tr>
<tr>
<td>DI-MA-46F</td>
<td>Safe, high available digital input from pushbutton, SIL 2</td>
</tr>
<tr>
<td>DI-MA-47F</td>
<td>Safe digital input from pushbutton (with LED), open contact, SIL 2</td>
</tr>
<tr>
<td>DI-MA-48F</td>
<td>Safe digital input from pushbutton (without LED), open contact, SIL 2</td>
</tr>
<tr>
<td>DO-MA-41F</td>
<td>Safe digital output to LED / LAMP, SIL2 / 3</td>
</tr>
<tr>
<td>DO-MA-42F</td>
<td>Safe digital output to two LED / LAMP, SIL 2 / 3</td>
</tr>
<tr>
<td>DO-MA-43F</td>
<td>Safe digital output to LED in fire fighting release pushbutton, SIL 2</td>
</tr>
</tbody>
</table>

**Hardware Types**
circuit code DO-RE-45F
Fail Safe I/O Modules
Development of interfaces to field devices

Man må ofte ting i sammenheng før en oppdager at det kan være spesielle feilsituasjoner
Fail Safe I/O Modules
Development of interfaces to field devices

Det er utrolig hvor lite komplisert det skal være før noe kan gå galt
PROFIBUS PA Fieldbus solution to SIL1 / 2.

- SINTEF Study "Evaluation of PROFIBUS PA against SIL1 / 2 requirements.

- Conclusion, SIL 1, provided set-up with extensive diagnosis is selected.
  - Fail to operate figures are nearly satisfying SIL2 requirements

- ProfiSafe PA, TÜV certified SIL 2, is scheduled.
Operator interface to SIL3

- Man - Machine interface for daily use are the Operator Stations (but Bill Gates deliver no SIL3 solutions)

- Matrix solutions ensures SIL3 in all situations

- Operator Stations with commands to SIL3
  - High end servers and operator stations, with redundancy and extensive diagnosis
  - Special TÜV approved procedure for safe commands from operator stations to F-area (safe island)

- Matrix solutions to SIL3
  - LED elements connected to SIL3 remote I/O
  - Necessary information for an emergency situation
  - Necessary input element to put the process to safe state

- Matrix solutions ensures SIL3 in all situations
Simple solutions
Pushbuttons lamps and switches are lifting and maintaining the SIL for the total HMI.
CPU-Software Architecture

- **Standard-User Program**
- **F-User Program**
  - **F-User Blocks**
    - F-Standard-blocks
    - F-System-blocks
      - Program execution
      - Communications
  - **F-Control Blocks**
    - Program execution
    - Self tests
- **Standard-Operating System**
  - **Safety-relevant sections of the operating system**
    - F-Access protection
    - Safety-relevant System Func. Calls
    - Safety-relevant Self tests
S7-F Concept, Double processing in diverse environments

Instead of redundancy of HW, Siemens Safety System runs redundant SW on same HW.

- Multi-channel storage of safety-critical data in instance DBs in the CPU, e.g. as word-oriented complement COMP
- Multi-channel processing of the safety function in F-FBs by SP7-ASIC of the CPU
  - Standard operation on DATA
  - Multi-channel operation on COMP
- CPU-internal comparison in the output driver to improve error locating
  Error handling: disable outputs and stop CPU
- CPU-external comparison in receiver (F-output modules and processing F-CPUs)
  Error handling: safe substitute values and error message
Time redundancy and Diversity instead of hardware redundancy

- Time redundancy and instruction diverse processing
- Logical program execution and data flow monitoring
- Bool and Word Operations processed in different parts of the CPU
- 2 independent hardware timer
Programming
Graphical programming CFC acc. to IEC 1131

F-Library
Certified (TÜV) function blocks
Links are structs
Simplified ESD Program Overview (sample)
Engineering tool
Program Protection

Read/Write protection with password
Enabling of the Failsafe function of the CPU 417-4H or 414-4H
Program protection
Program Signature

Signature of F-Program for TÜV Certification. Program taken out of CPU cannot be downloaded unless carrying the correct signature.

The signature is generated by the programming tool, and is changed after every change of the program.
Programming
Comparison of existing and changed program

Comparison of different F-program versions
Deviations shall be checked before download of change
Engineering
Failsafe I/O Modules, diagnostics is set due to SIL

Enabling of the failsafe function
Signal evaluation:
1001 (SIL 2) 1002 (SIL 3)
Communication concepts to SIL3 /2/1

- PROFIBUS DP / ProfiSafe for communication to approved ProfiSafe equipment, SIL3 / 2.
  - F-SM remote I/O modules
  - Autrosafe fire panel
  - Other S7 400F or S7 300F nodes

- Drivers for Ethernet communication to S7 F nodes, SIL3.
  - Drivers for communication on Ethernet between safety programs in S7 nodes.

- Communication from OS to safety program to SIL3
  - Special routine and function blocks for verified command from OS to F-area (safe island).

- Combination of PROFIBUS DP /PROFIBUS PA to SIL 1
High Available Communication (not required to achieve SIL)

Configuration with Optical Ringbus

Redundant optical ringbus

S7-400H

Redundancy replacement diagram:

PS  CPU  CP  Bus  CP  CPU  PS
PS  CPU  CP  Bus  CP  CPU  PS
Basic concepts for communication to SIL3 and SIL2

enabling failsafe fieldbus applications ....
Basic concepts for communication to SIL3 and SIL2
Add required safety layer to a standard protocol

„Black/Gray Channel“: ASICs, Links, Cables, etc. are not safety relevant

Non safety critical functions, like e.g. diagnosis

"ProfiSafe": Parts of the safety critical communications systems: Adressing, Watch Dog Timers, Sequenzing, Signatur, etc.

Safety relevant, but not part of the ProfiSafe-Proifs: Safety I/O and the Safety Control Systems
Basic concepts for communication to SIL3 and SIL2
Content of required safety layer must cover possible failures

### Failure Types and remedial Measures ...

<table>
<thead>
<tr>
<th>Failure type:</th>
<th>Remedy:</th>
<th>Sequence Number</th>
<th>Time Out with Receipt</th>
<th>Codename for Sender and Receiver</th>
<th>Data Consistency Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repetition</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deletion</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insertion</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Resequencing</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Corruption</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Delay</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Masquerade (standard message mimics failsafe)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>FIFO failure within Router</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The measures must be executed and monitored inside one failsafe unit
Standard Profibus DP Message...

Data Unit = Standard- or Failsafe-Data
1... 244 Bytes

FCS = Frame Checking Sequence (across data within LE)
ED = End Delimiter
SB = Start-Bit
ZB0...7 = Character-Bit
PB = (even) Parity Bit
EB = Stop-Bit

TBit = Clock-Bit = 1 / Baudrate
SD = Start Delimiter (here SD2, var. Data Length)
LE = Length of Data
LER = Repeated LoD, not in FCS
DA = Destination Address
SA = Source Address
FC = Function Code (Type of Message)
... and a ProfiSafe Message ...
(the extra layer included in the user telegram)

---

<table>
<thead>
<tr>
<th>F-I/O-Data</th>
<th>Status / Controlbyte</th>
<th>Sequence Number</th>
<th>CRC</th>
<th>Standard-I/O-Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. 12 / 122 Bytes</td>
<td>1 Byte</td>
<td>1 Byte</td>
<td>2/4 Bytes *)</td>
<td>(240/238 - F-Data)</td>
</tr>
</tbody>
</table>

*) 2 Byte for a max. of 12 Byte F I/O data
4 Byte for a max. of 122 Byte F I/O data

Max. 244 Bytes DP-Data
Safety Control Loops and Residual Error (PFD) Probability....

100 %, total figure for allowed PFD (Probability of Failure on Demand)

1 % (Profisafe share of total for SIL3)

e.g. Safety Integrity Level (SIL) 3 : 10^{-7} / h
(Share of ProfiSafe: 1% = 10^{-9} / h)
Safety communication possibilities integrated (principles of ProfiSafe used)