Automation Decision

Henry Robertson

12GeV PSS Final Design Review

September 16/17, 2009

Performance Characteristics of the Siemens S7F Distributed Safety

- TUV Certification - PLC components and Network protocol
- Integration in S7F-300; the automation task determines the system design
- Execution of standard control and protective functions on the same system (standard system with fail-safe capability - eliminates the need for dedicated fail-safe solutions)
- Connection of distributed I/O via PROFINET with PROFIsafe
- Use of standard Industrial Ethernet components (i.e. switches, CAT5 and fiber-optic cable)
- Creation of safety program using standard IEC programming languages
- Flexible adaptation to the task requirements by providing a wide range of fail-safe I/O

Safety in F-Systems

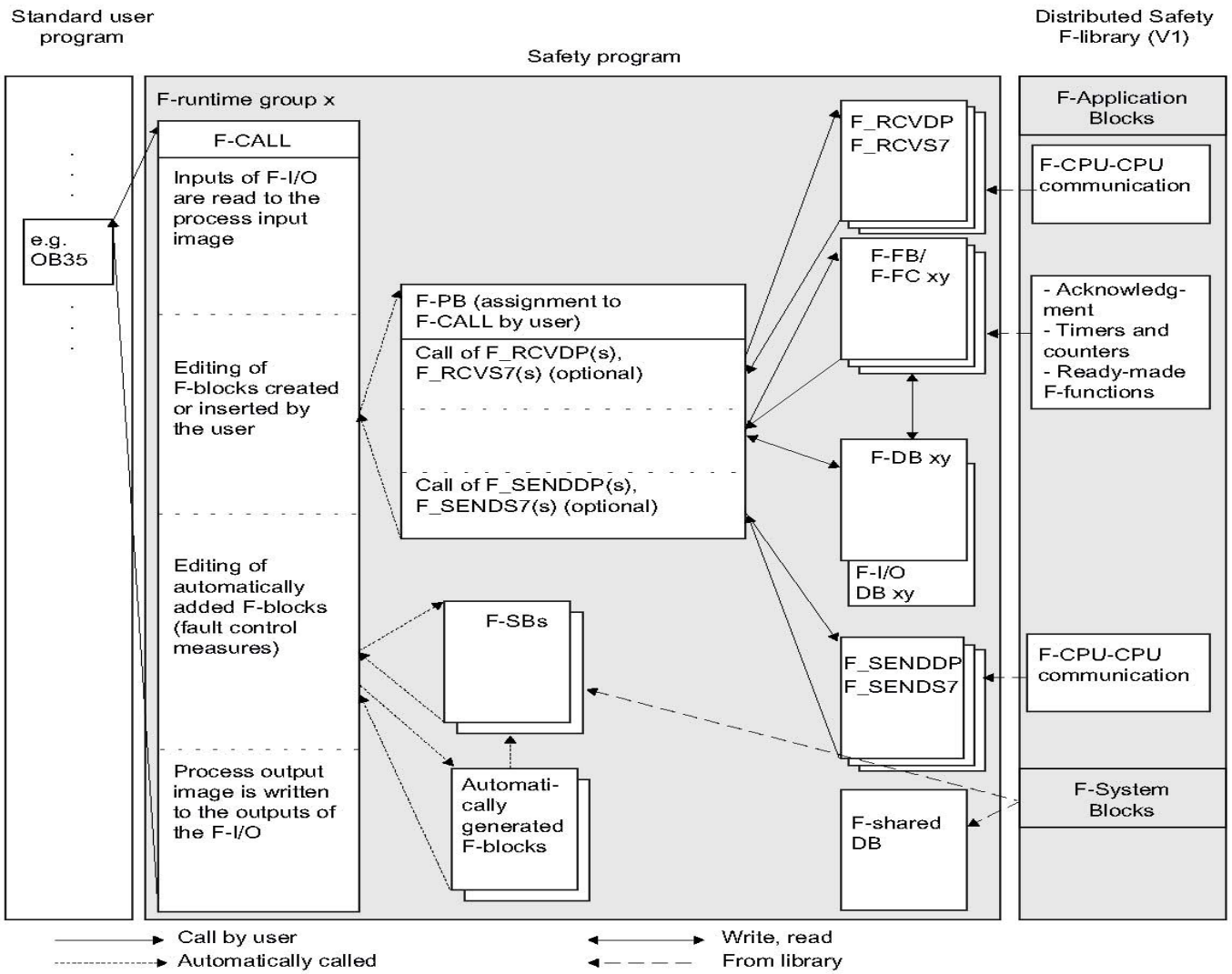
- Interaction of Components - To configure a fail-safe system, software and hardware components have to be combined a specified manner
- Wiring Fail-safe I/O - The user wires the F-I/O to the sensors and actuators so as to be able to achieve the required safety class
- Configuring Hardware - The user configures the F-Capable CPU and the F-I/O in STEP 7
- HW Config. This configuration must match the hardware configuration
- Creating safety programs - User creates fail-safe blocks in F-FBD or F-LAD. The associated F-block library provides fail-safe blocks that the user can use in his safety program

Safety in F-Systems

- Safety checks are performed and additional F-blocks for fault detection are incorporated automatically when the executable safety program is compiled. This ensures that failures and errors are detected and appropriate reactions are triggered to maintain the F-system in the safe state or bring it to a safe state.

- In addition to the safety program, a standard user program can be run on the F-CPU. A standard program can coexist with a safety program in an F-CPU because the safety-related data of the safety program are protected from being affected unintentionally by data of the standard user program. Data are exchanged between the safety program and the standard user program in the FCPU by means of bit memory or by accessing the process input and output images (PII, PIO).

Safety in F-Systems



Overview of Access Protection

- Access to the S7 Distributed Safety F-system is protected by two password prompts: one for the F-CPU and another for the safety program.

- For the password for the safety program, a distinction is made between an offline password and an online password for the safety program:

  – The offline password is part of the safety program in the offline project on the programming device. The password for the safety program prevents unauthorized users from making changes to the safety program. In S7 Distributed Safety it also prevents any unauthorized changes to the configuration and parameterization of the F-CPU and F-I/O.

  – The online password is part of the safety program in the F-CPU. The password for the F-CPU protects the F-Systems from unauthorized downloads to the CPU from the engineering system (ES) or programming device (PG).

SIMATIC Safety Integrated - Processor

- For SIMATIC Safety Integrated systems, the processing unit consists of fail-safe single-channel controllers and fail-safe dual-channel I/O modules. Fail-safe communication takes place via the safety-oriented PROFIsafe profile. SIMATIC Safety Integrated is certified and suitable for use in accordance with:

- IEC 61508: 2000 SIL 1 - 3
- EN 594-1: 1997 Cat. 2 - 4
- IEC 61511: 2003
- EN 60204-1: 1997
- EN 62061: 2005
- NFPA 79-2002, NFPA 85
- EN ISO 13849-1: 2006 PL a - e

SIMATIC Safety Integrated - F-I/O

- Safety Class, Category, Performance in accordance with IEC 61508, EN 954-1, EN ISO 13849-1: 2006:
- SIL2 Category 3 PLd 1oo1 evaluation In the F-I/O
- SIL3 Category 4 PLe 1oo2 evaluation In the F-I/O; or in safety program with Fblock
- SIL3 Category 4 PLe 2oo3 evaluation In safety program with F-block

Integrated Diagnostics

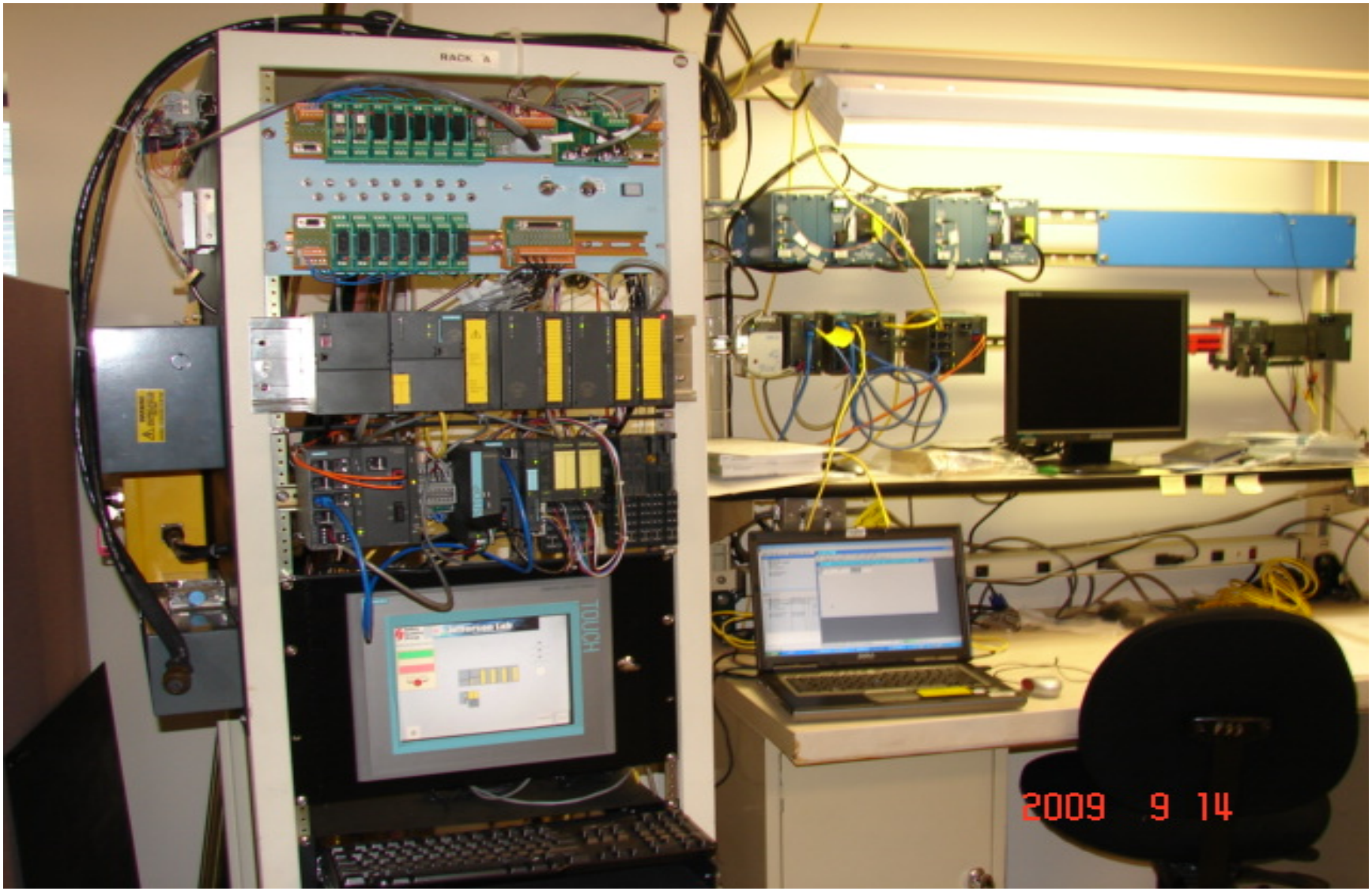
- Products and modules with integrated diagnostics function

- Plant-wide system diagnostics for detection and automatic signaling of faults:
  - Diagnostics with display of relevant information
  - Fault text information
  - Unambiguous module identification (number)
  - Address/slot information
  - Chronological time stamp
  - Predefined message windows/views for visualization on the HMI device

Integrated Diagnostics

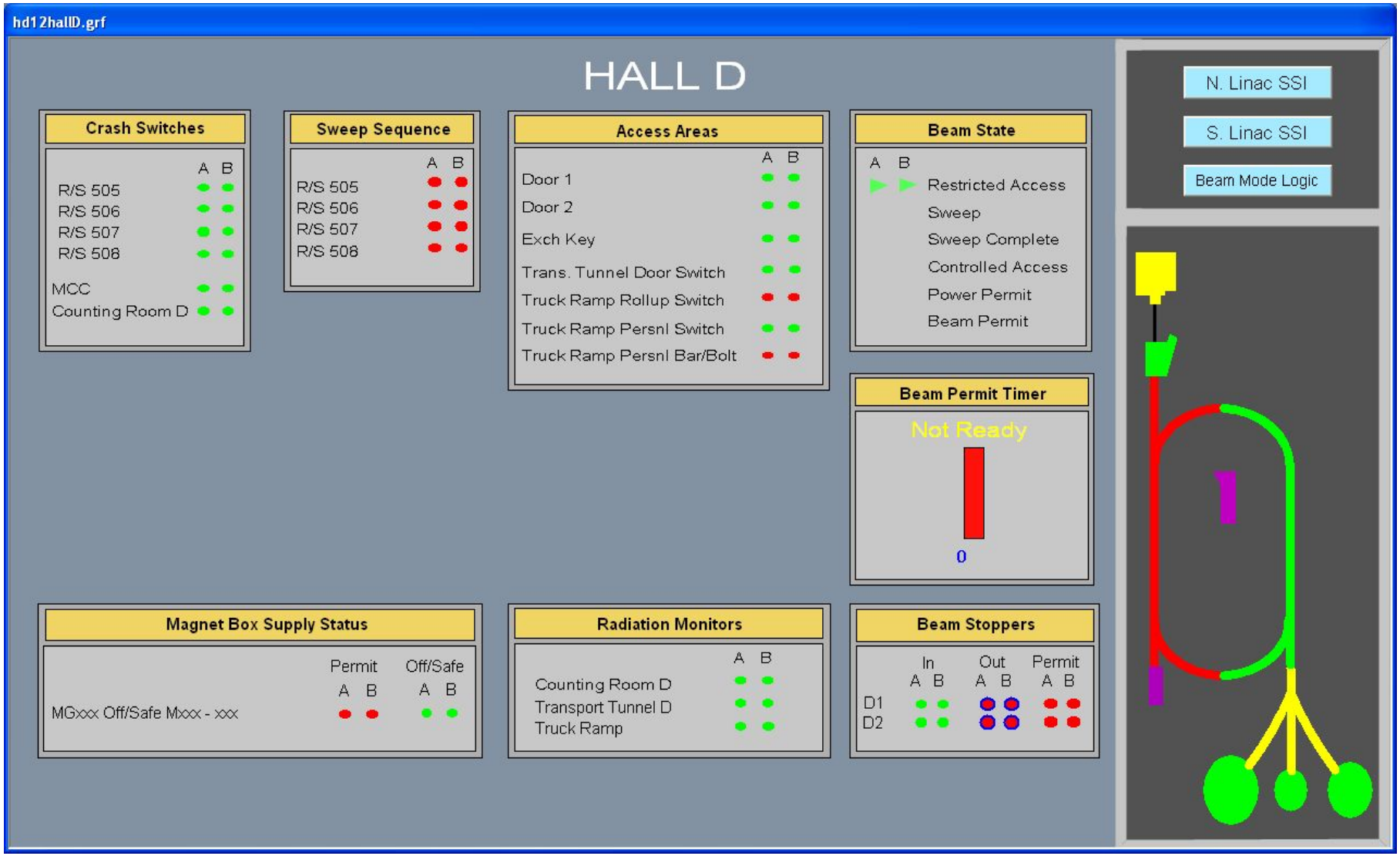
- Diagnostics displays with different degrees of detail (hierarchy) are generated automatically from configuration data:
  - Control level
  - Field level
  - Operations management level
  - Plant-wide diagnostics
  - Transfer of configuration from STEP 7
  - Diagnostics enabling Controller
  - Detection of fault
  - Line-width display of information
  - Distributed I/O

Test Stand / Mockup



Test Stand / Mockup

iFix HMI Display



Automation Decision

Questions?