6th Control System Cyber-Security Workshop (CS)2/HEP

EUROPEAN SPALLATION SOURCE

Security Measures for ESS PSS Software Development

Denis Paulic
Deputy Group Leader, Protection and Safety Systems

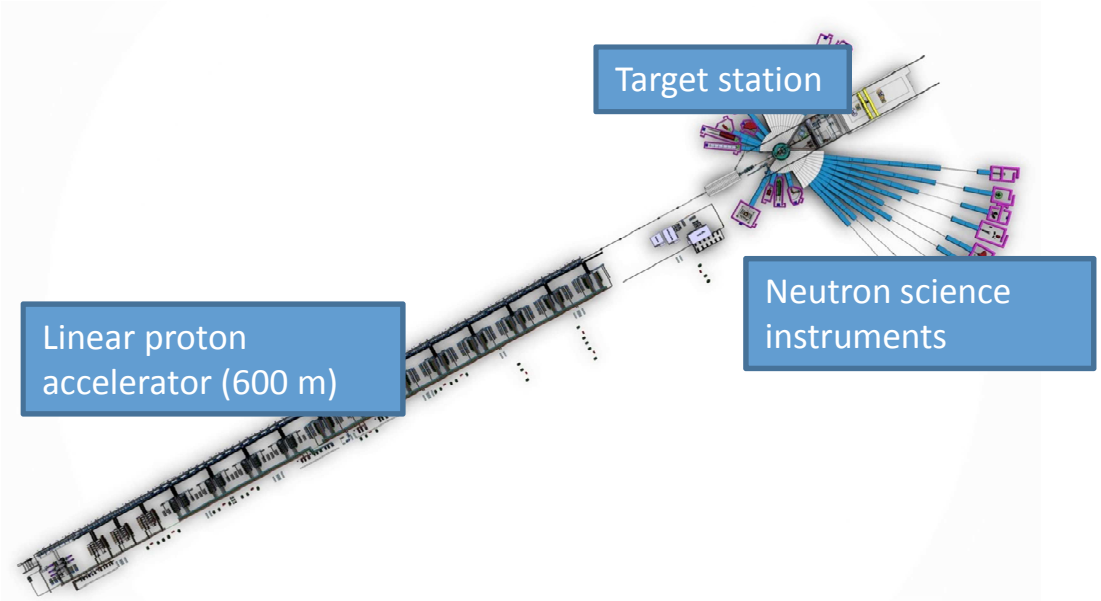
ESS/ICS/PS
Date: 2017-10-08

Contents

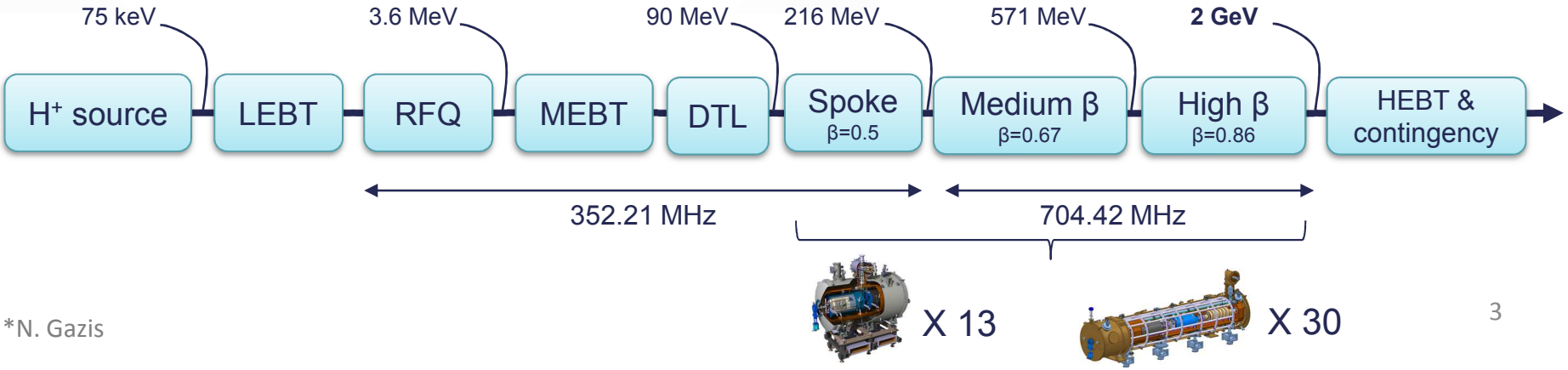
- ESS Overview
- Personnel Safety Systems
- Governance
- PSS Software Decisions
- System Integrity Measures for PSS

ESS Linac Overview

- The European Spallation Source (ESS) will house the most powerful proton LINAC ever built.



Parameter	Value	Units
Max energy	2	*GeV*
Peak current	62.5	*mA*
Repetition rate	14	*Hz*
Pulse length	2.86	*ms*
Average power	5	*MW*
RF frequency	352/704	*MHz*
Maximum losses	1	*W/m*



*N. Gazis

Personnel Safety Systems

- **Safety interlock system**
  - If the Beam is ON → No Access
  - If Access is allowed → No Beam permit
  - If Emergency → Hard switch-off all hazardous equipment

- **Access control system**
  - Authorisation and authentication
  - Entry stations
  - Access point sub-systems

- **ODH detection system**
  - If oxygen level is below treshold → No Access, activate lights and sounders

ODH = Oxygen Deficiency Hazard

Governance

- **IEC 61508 : 2010**
  - Functional safety of electrical/electronic/programmable electronic safety-related systems
- **IEC 61511 : 2016**
  - Functional safety - Safety instrumented systems for the process industry sector
  - PSS application program
- **The Swedish Radiation Safety Authority (SSM)**
  - Radiation risk analysis will be carried out before the facility is taken into operation.
  - A formalised search of each PSS controlled area will be carried out before the facility is operated.
  - Two independent technical design solutions will be used in each system.
  - External events
  - Single failure
  - Common cause failure
  - Redundancy
  - Diversity
  - Separation

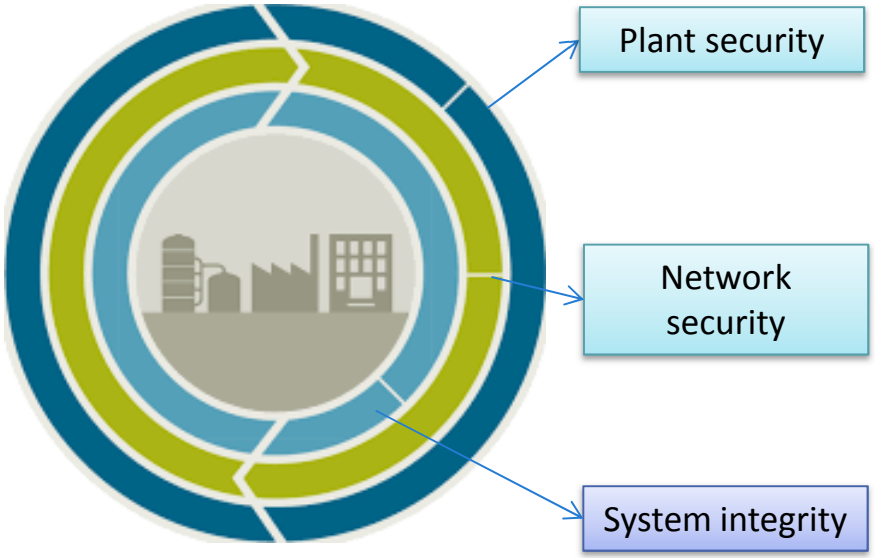
Governance for Software Security

- **IEC 61511 : 2016**
  - **Part 1, Clause 8.2.4.**
    - A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in:
      - A description of devices covered by this assessment (SIS, BPCS, any device connected to SIS)
      - A description of identified threats that could exploit vulnerabilities and result in security events
      - A description of potential consequences resulting from security events and likelihood of these events occurring.
      - Consideration of various phases, such as design, implementation, commissioning, operation, and maintenance
      - The determination of requirements for additional risk reduction
      - A description of, or references to information on, the measures taken to reduce the… threats.
- **IEC 61508 : 2010**
  - **Part 1, Clause 7.4.2.3**
    - If the hazard analysis identifies the malevolent or unauthorised action, constituting a security threat,…, then a security threats analysis should be carried out
- **IEC 62443 - Security for Industrial Automation and Control Systems**
- **NIST Special publication 800-82: Guide to Industrial Control Systems (ICS) Security**

NIST = National Institute of Standards and Technology
SIS = Safety Instrumented System

Cyber Security Study

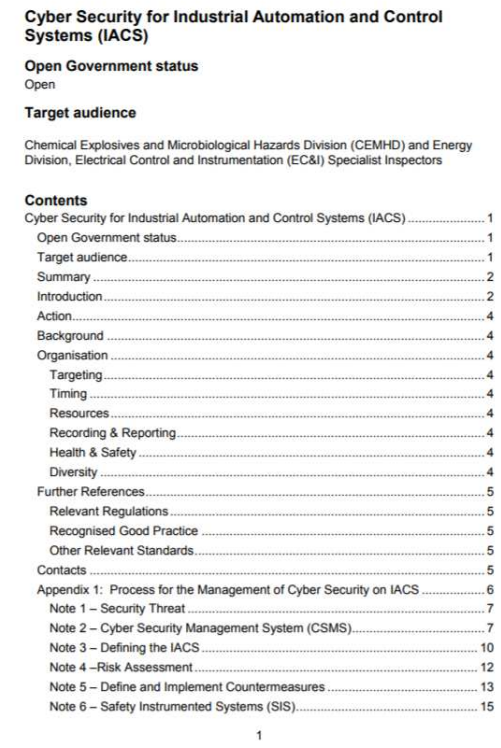
- Defence-in-Depth – applying multiple countermeasures in a layered manner.



- Network security layer: In-kind partner from Estonia: *Cyber security risk assessment and mitigation plan for the ICS*, based on IEC 62443.
  - Initial meeting: 2016-10-17
- PSS planned actions:
  - IEC 61511:2016
  - **HSE operational guidance** (based on IEC 62443)
  - NIST framework (NIST SP 800-82)

HSE = Health and Safety Executive
NIST = National Institute of Standards and Technology
SP = Special Publication

HSE Guidance



Cyber Security for Industrial Automation and Control Systems (IACS)

Open Government status
Open

Target audience

Chemical Explosives and Microbiological Hazards Division (CEMHD) and Energy Division, Electrical Control and Instrumentation (EC&I) Specialist Inspectors

Contents

1

HSE Operational Guidance

- Appendix 1 – Process for the management of cybersecurity on IACS
- Appendix 2 – Example of simple network drawings
- Appendix 3 – Risk Assessment (based on IEC 62443 high level one)
- Appendix 4 – Security Contermeasures
- Appendix 5 – Additional SIS Considerations

HSE Guidance - Example

Example of proposed risk assessment scheme from HSE:

Consequence Category	Major Accident
A (High)	Failure of or unauthorised access to a high integrity layer of protection (PFD < 0.1), including systems that are capable of manipulating this LOP
B (Medium)	Failure of or unauthorised access to a lowi ntegrity layer of protection (PFD ≥ 0.1), including systems that are capable of manipulating this LOP
C (Low)	Failure of or unauthorised access to a system that doesn't have a safety function.

Security risk = Likelihhod * Consequence category

LOP = Layer of Protection

PSS Software Decisions

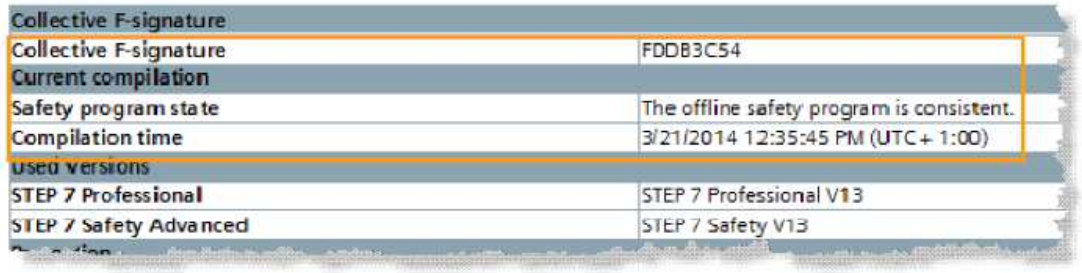
- Latest version of Siemens SIMATIC STEP 7
  - V13 SP1 → V14 SP1,
  - TIA Portal including:
    - Safety Advanced:
      - Safety checks are automatically performed in the software;
      - Fail-safe blocks for error detection and error reaction are inserted automatically when the safety program is compiled;
    - WinCC Comfort for HMI programming.
- 2-train fail-safe PLC system
  - Siemens fail-safe CPUs allow the processing of standard and safety programs on a single CPU.
    - Certified to satisfy the Safety Integrity Level SIL3 in accordance with IEC 61508:2010.
    - **Integrated system diagnostics;**
    - **4-level security concept.**

Integrated Access Protection Measures

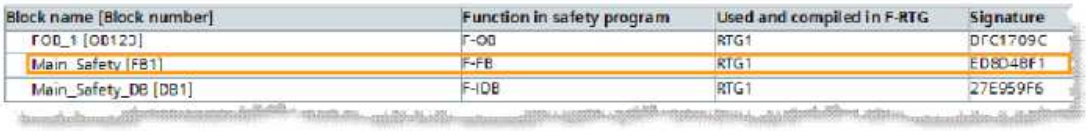
- Components with integrated security features
  - S7-1500 controller with activated ”Protection level”
    - The access to PSS safety software will be protected by two password prompts: one for the safety program and another for the safety CPU!
    - Checking the collective signature of the safety program (Checksum test):
      - In case of the software misuse, the system goes to Alarm mode;
      - PSS system administrator shall be informed immediately;
      - Checksum will change after any error-free safety software re-generation.
- HMI panels in ”Secure mode”
- Managed network switches (password protected)
- Firewalls
  - passwords/certificates
- Central user administration
  - user accounts and policies
- Enforcing of security guidelines
  - password validity, incorrect logging on monitoring, etc.

Checksum Test - F-runtime Group Information DB

Symbolic name	Data type	For processing in the safety program	For processing in	Description
MODE	BOOL	x		
F_SYSINFO				
MODE	BOOL	—		
TCYC_CURR	DINT	—		
TCYC_LONG	DINT	—		
TRTG_CURR	DINT	—		
TRTG_LONG	DINT	—		
T1RTG_CURR	DINT	—	x	Not supported by *STEP 7 Safety V13 SP1.*
T1RTG_LONG	DINT	—	x	Not supported by *STEP 7 Safety V13 SP1.*
F_PROG_SIG	DWORD	—	x	Collective F-signature of the safety program
F_PROG_DAT	DTL	—	x	Compilation date of the safety program
F_RTG_SIG	DWORD	—	x	Collective F-signature of the F-runtime group
F_RTG_DAT	DTL	—	x	Compilation date of the F-runtime group
VERS_S7SAF	DWORD	—	x	Version identifier for *STEP 7 Safety*

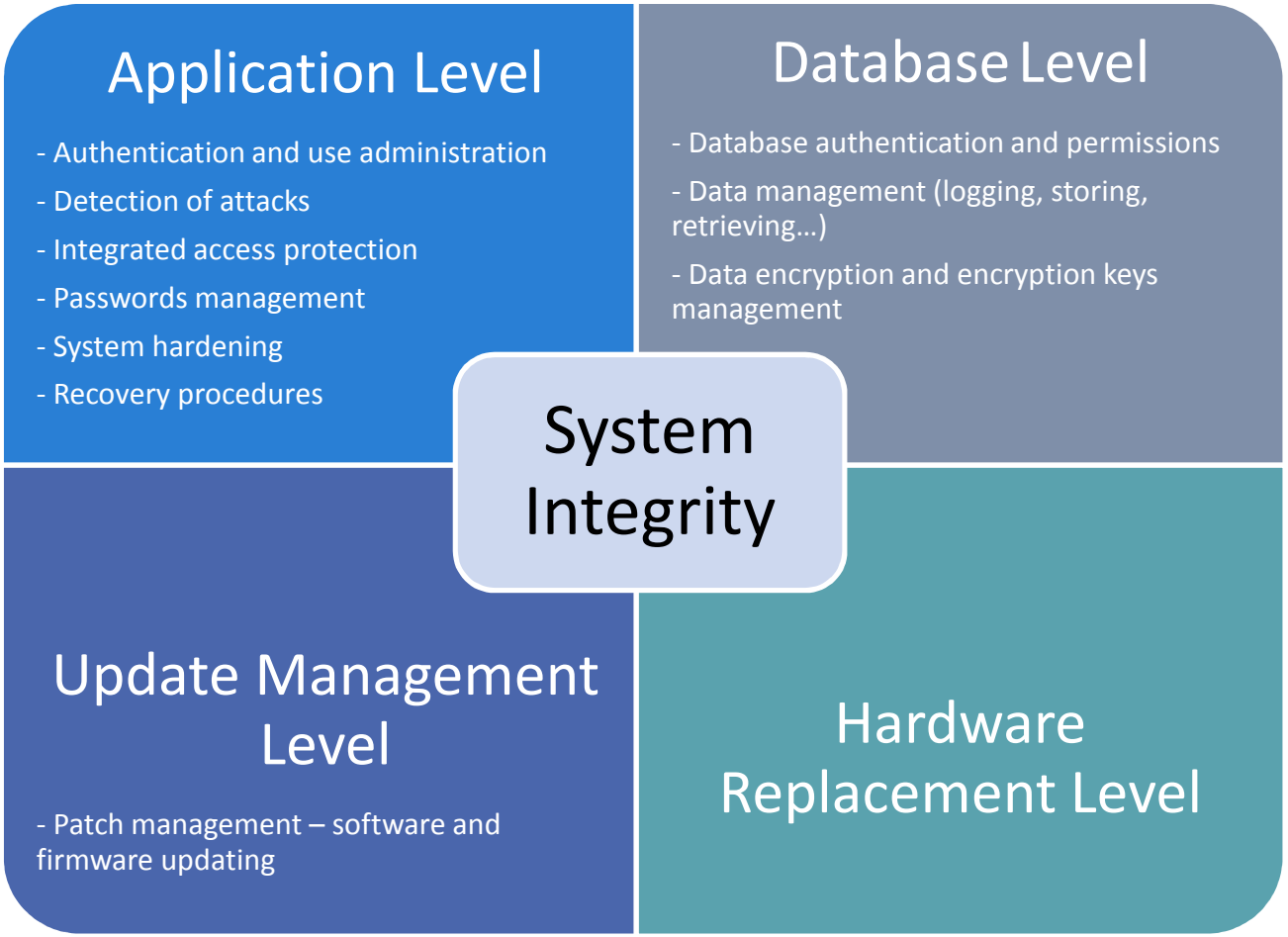


Collective F-signature	
Collective F-signature	FDDB3C54
Current compilation	
Safety program state	The offline safety program is consistent.
Compilation time	3/21/2014 12:35:45 PM (UTC+1:00)
Used versions	
STEP 7 Professional	STEP 7 Professional V13
STEP 7 Safety Advanced	STEP 7 Safety V13



Block name [Block number]	Function in safety program	Used and compiled in F-RTG	Signature
FOD_1 [OB123]	F-OB	RTG1	DFC1709C
Main_Safety [FB1]	F-FB	RTG1	ED8D48F1
Main_Safety_DB [DB1]	F-DB	RTG1	27E959F6

PSS Software - System Integrity Layer



System Hardening and Antivirus Software Measures

Engineering workstation requirements:

- No Internet/Intranet connection, disabled WLAN and Bluetooth.
- Most of the activated services disabled:
  - Booting and auto-start mechanisms, Flash, Java, Webserver, FTP, Remote Desktop, Adobe, Internet Explorer…
- Unused interfaces will be deactivated or mechanically blocked:
  - Ethernet/Profinet ports; USB, Firewire, etc.;
- Configured / activated user accounts will be reduced to the necessary minimum.
- Regular checks, particularly of locally configured user accounts are planned.
- Siemens supports compatibility tests with:
  - Trend Micro Office Scan,
  - Symantec Endpoint Protection,
  - McAfee VirusScan Enterprise (+ McAfee Application Control as a whitelisting mechanism).
- Safety and availability must generally be assured even in the case of infection with malware. This means that the virus scanner must under no circumstances execute the following actions without permission:
  - Remove files or block access thereto;
  - Place files in quarantine;
  - Block communication;
  - Shut systems down.

Patch Management and Firmware Updates Measures / Options

- Siemens supports with compatibility tests of Microsoft security patches.
- Recommendation from Siemens:
  - Patch distribution via central patch server in DMZ and Windows Server Update Services (WSUS).
    - Set up the update groups and processes for online updates to simplify patch distribution.
- Firmware updates might be needed to fix security related vulnerabilities
  - Modifications included in Configuration management
- As soon as information on a vulnerability becomes available, the weak point will be evaluated for relevance to the application concerned.

Requirements For Operator Interface

- SIS status information critical to maintaining the SIL shall be available as part of the operator interface:
  - where the process is in its sequence
  - indication that SIS protective action has occurred
  - indication that a protective function is bypassed
  - information about automatic actions from PSS system
  - status of sensors and final elements
  - the loss of energy where that energy loss impacts safety
  - the results of diagnostics
- SIS operator interface shall prevent changes to SIS application software.
- Any writing from standard to safety part of the SW shall be documented and tested to make sure it cannot lead the system to an unsafe state.

SIS = Safety Instrumented System

PSS Configuration Management

Objective:

- To describe the generic configuration management process during the development of Personnel Safety Systems;
- To ensure procedures to be used for uniquely identifying all constituent parts of hardware and software items.
- To specify procedures for preventing unauthorized items from entering the process.

- In addition to IEC 61508:
  - ISO 9001 Quality management systems – Requirements
  - ISO 10007:2004 Quality managements systems – Guidelines for configuration management

Questions?

EUROPEAN SPALLATION SOURCE

Thank you for your attention!