



Wir schaffen Wissen – heute für morgen

Controls Security at PSI

Current Status

R. Krempaska, A. Bertrand, C. Higgs, R. Kapeller, H.Lutz

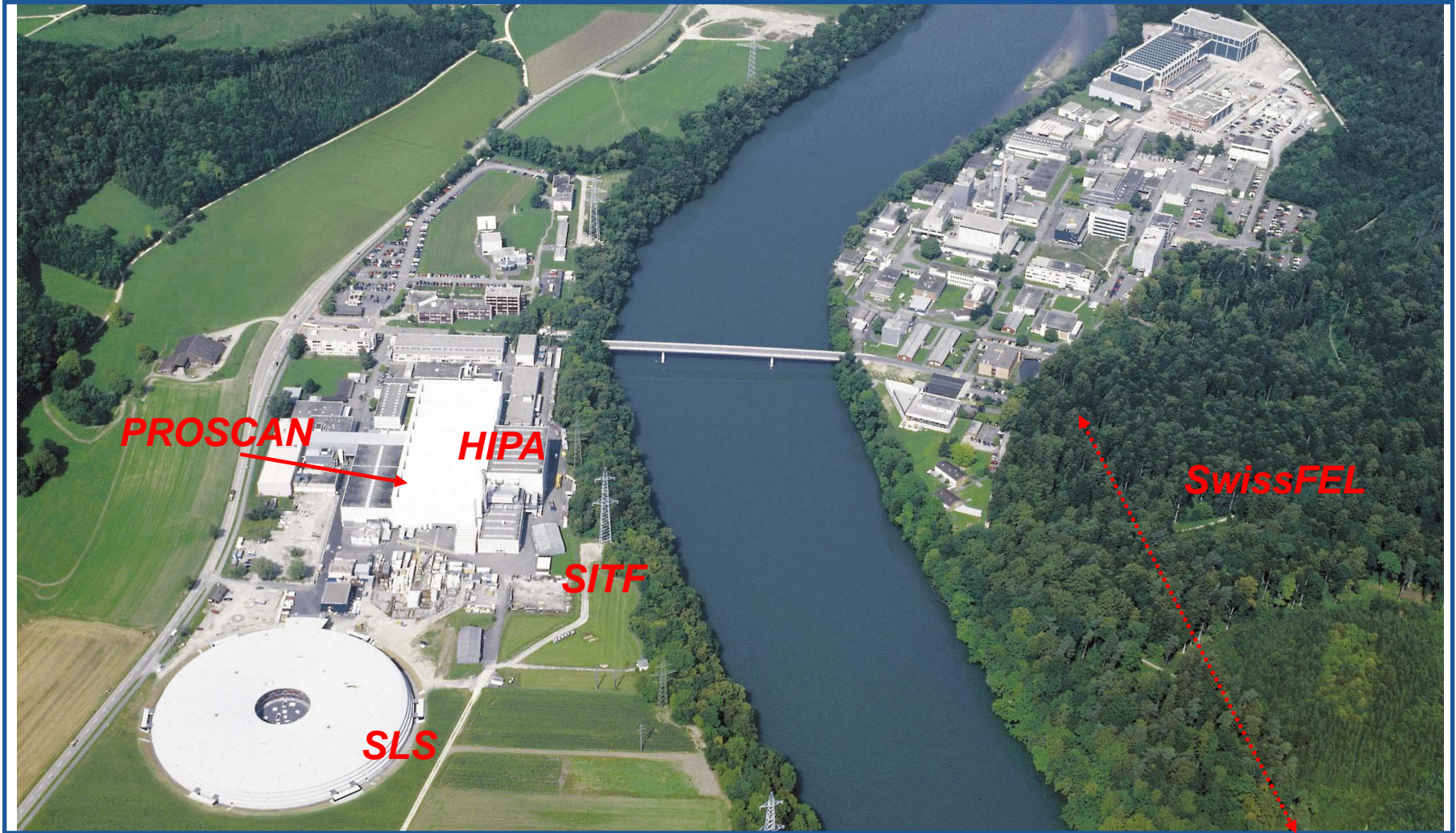
GFA Controls IT

October, 2013

Outline

- **Overview of PSI Large Research Facilities**
- **Control System Network Security**
 - Private Machine Networks
 - Network Architecture and Hardware
 - Local and Remote Access
- **Control System Infrastructure**
- **Challenges**

PSI and Large Research Facilities



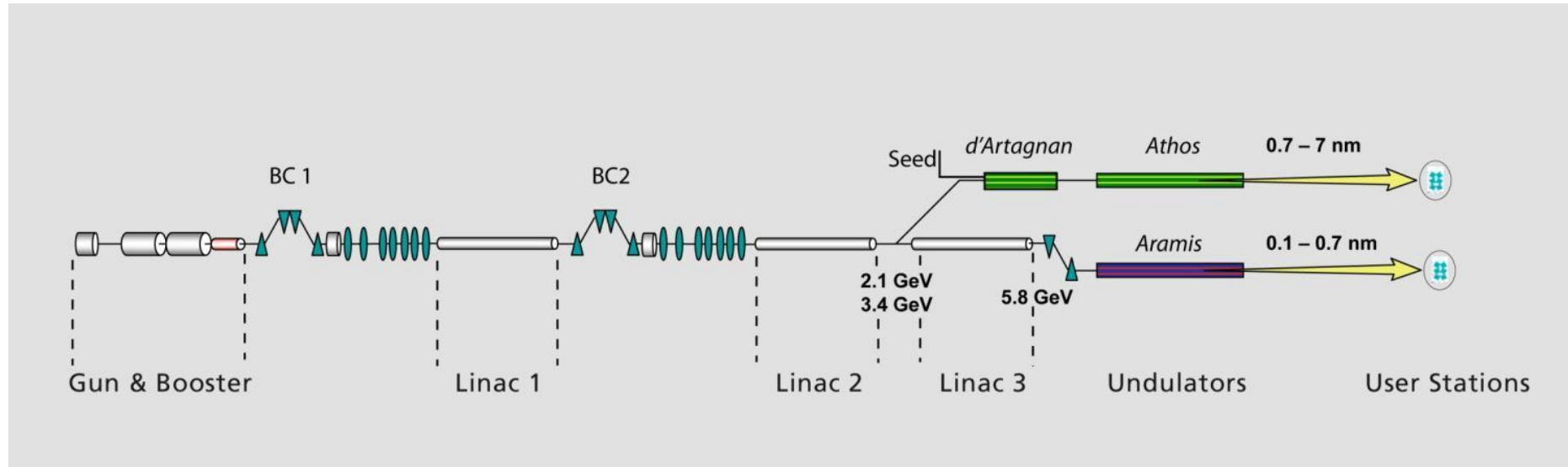
High Intensity Proton Accelerator (HIPA) and PROSCAN



Electron accelerators

Swiss Light Source (SLS) and SwissFEL Injector Test Facility (SITF)





SwissFEL Construction



SwissFEL “Baustelle”



Controls is responsible for the control system

- HIPA Accelerator + ~10 Beamlines
- PROSCAN Accelerator + 4 Beamlines
- SLS + ~20 Beamlines
- SITF (SwissFEL Injector Test Facility) + TRFCB (C-Band RF Structure Test Facility)

Controls Network and Rules

- Control system for accelerators is separated in private machine networks.
- Control system for SLS beamlines is in separated sub-nets, behind a firewall. Users from one beamline cannot influence the control system of another beamline.
- Remote access from the PSI office network to machine and beamline networks is possible through a dedicated ssh gateway.
- Login to ssh gateway is restricted for a well defined list of users and allowed only during facilities shutdown and machine shifts. The „on-call“ service Controls members can get the access on request from the control room. The shift leader operator in the Control room can close the remote network access at any time.

Network Architecture and Hardware

- Controls network is based on PSI standard network topology, hardware with monitoring, documentation and overview.
- Active components are implemented by Network group.
- Passive components (patch panels) are implemented under supervision of Network group and Controls.
- All the devices are documented and kept up-to-date in the Controls Hardware Inventory database.
- Network infrastructure components are installed in locked racks.

Switches Documentation

Switch

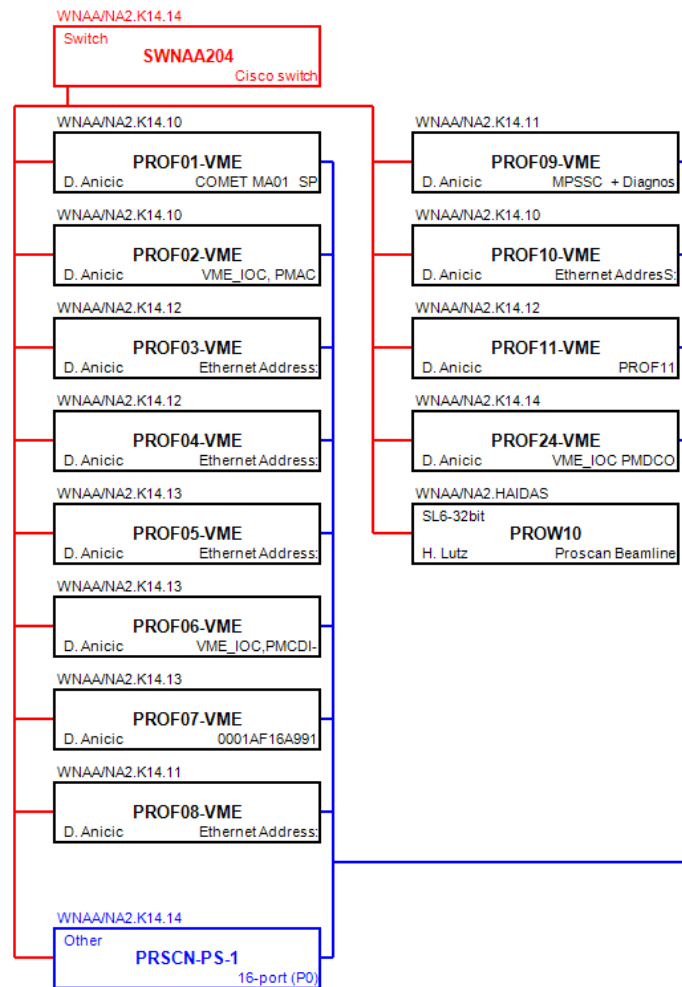
Filter: PROSCAN

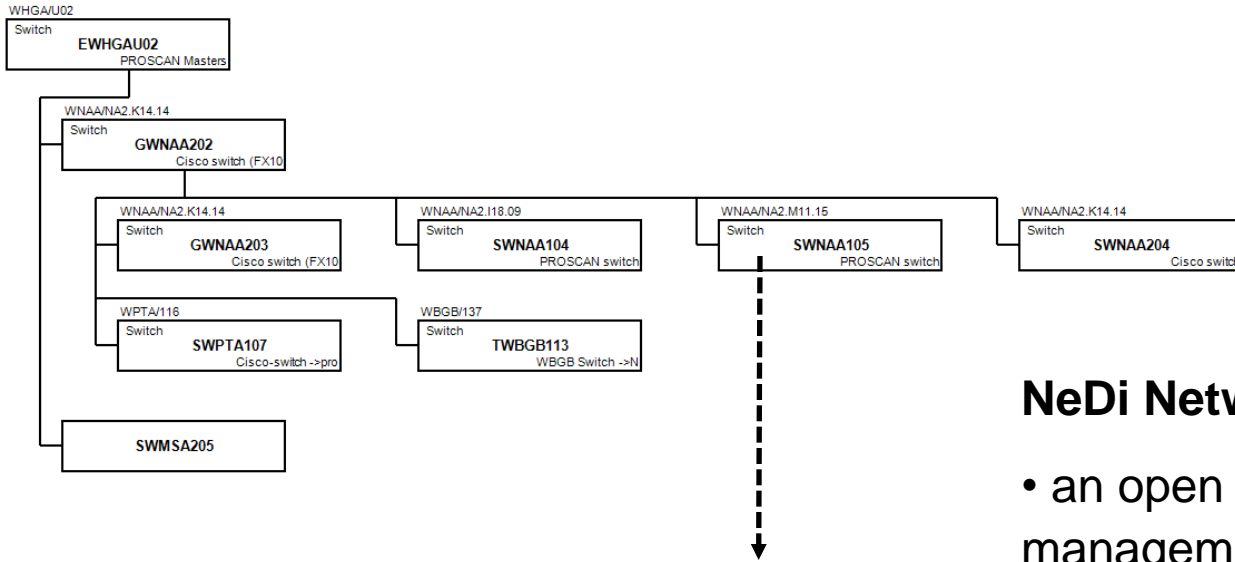
Switch	Description	Location	Host	Location
Diagram EWHGAU02	PROSCAN Masterswitch	Installed/WHGA/U02	GWNAA202 GWNAA203	Installed/WNAA/NA2.K14.14 Installed/WNAA/NA2.K14.14
Diagram GWNAA202	Cisco switch (FX100)	Installed/WNAA/NA2.K14.14	SWNAA104 SWNAA105 SWNAA204 SWPTA107 TWBGB113	Installed/WNAA/NA2.I18.09 Installed/WNAA/NA2.M11.15 Installed/WNAA/NA2.K14.14 Installed/WPTA/116 Installed/WBGB/137
Diagram SWNAA104	PROSCAN switch	Installed/WNAA/NA2.I18.09	PROF17-VME PROF18-VME PROF20-VME PROF23-VME	Installed/WNAA/NA2.I18.09 Installed/WNAA/NA2.I18.01 Installed/WNAA/NA2.I18.08 Installed/WNAA/NA2.I18.03
Diagram SWNAA105	PROSCAN switch	Installed/WNAA/NA2.M11.15	PROF12-VME PROF13-VME PROF14-VME PROF16-VME	Installed/WNAA/NA2.M12.14 Installed/WNAA/NA2.M12.16 Installed/WNAA/NA2.M12.16 Installed/WNAA/NA2.M12.14
Diagram SWNAA204	Cisco switch	Installed/WNAA/NA2.K14.14	PROF01-VME PROF02-VME PROF03-VME PROF04-VME PROF05-VME PROF06-VME PROF07-VME PROF08-VME PROF09-VME PROF10-VME PROF11-VME PROF24-VME PROW10 PRSCN-PS-1	Installed/WNAA/NA2.K14.10 Installed/WNAA/NA2.K14.10 Installed/WNAA/NA2.K14.12 Installed/WNAA/NA2.K14.13 Installed/WNAA/NA2.K14.13 Installed/WNAA/NA2.K14.11 Installed/WNAA/NA2.K14.11 Installed/WNAA/NA2.K14.10 Installed/WNAA/NA2.K14.12 Installed/WNAA/NA2.K14.14 Installed/WNAA/NA2.HAIDAS Installed/WNAA/NA2.K14.14
Diagram SWPTA107	Cisco-switch ->provs6,7,8,11,12	Installed/WPTA/116	PROF27-VME PROF28-VME PROF29-VME PROW11 PROW12 PROWS6 PROWS7 PROWS8 PRSCN-PS-4	Installed/WPTA/112/PT2.112.01 Installed/WPTA/112/PT2.112.05 Installed/WPTA/113/PT2.3.6 Installed/WPTA/O2 Installed/WPTA/G2 Installed/WPTA/111 Installed/WPTA/111 Installed/WPTA/111 Installed/WPTA/111 Installed/WPTA/112/PT2.112.04
Diagram TWBGB113	WBGB Switch ->NA.K14.14[3-4]	Installed/WBGB/137	PROSCAN-SOFTIOC02 PROWS0	Installed/WBGB/013 Installed/WBGB/135

Host Diagrams

Draw Host Diagram

Element: Sort by:

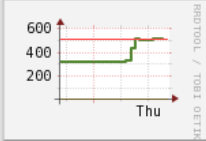




NeDi Network Discovery

- an open source tool for network management and monitoring
- used by the PSI Network group
- integrated in the Hardware Inventory Database tool, so that Controls can get monitoring information about switches in the Controls networks

NEDI - Ports on the switch

Filter	Filter	Filter	Filter	Filter	Filter
Port	Graph	Info	Speed	FD	Hosts
Graph Fa0/1		FastEthernet0/1	100M	-	1
Graph Fa0/2		FastEthernet0/2	100M	-	1
Graph Fa0/3		FastEthernet0/3	100M	-	1

Local access

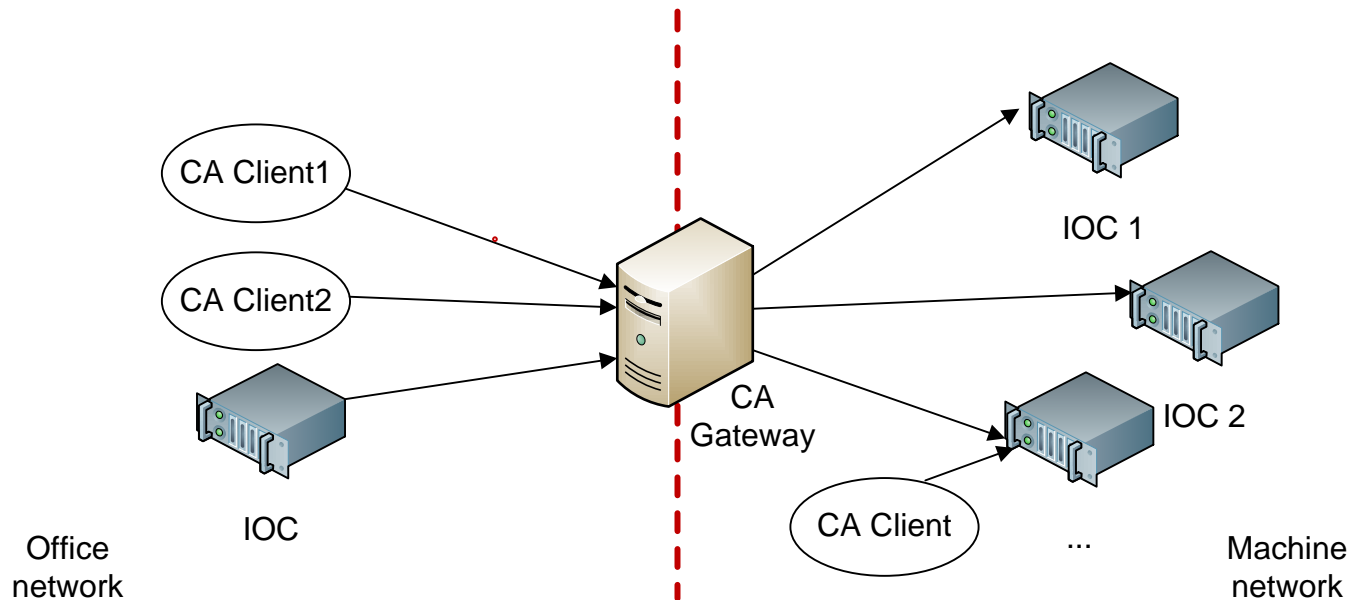
- Connected devices must be registered in the PSI central DNS.
- No direct wireless access to the private machine networks

Remote access to a private machine network

- Access only from the PSI net through the gateways
- No direct access from one machine network to another
- No access to users home directories

Channel Access Gateway

- Control system protocol (EPICS channel access) cross the network via a channel access gateway.
- Allows access control and filtering.
- It saves resources (network bandwidth, memory consumption) on IOCs because it reduces the number of direct client connections and shares data and connections between the clients.



- Computers (operator consoles, camera servers, etc.) are purchased as a PSI standard hardware and installed by the Controls IT group.
- Installation and configuration is done by using a centralized installation and configuration mechanism.
- OS supported: Linux and Windows
- Controls servers (NFS and VmWare clusters, computing nodes, etc.) are located in server rooms accessible only by system administrators.
- All the related information about computers is registered in the Controls Hardware Inventory DB.

Installation and Configuration

Linux PCs

- Scientific Linux (SL) distribution is used at PSI
- PSI Central Computing Division is in charge for SL core and rpm packages
- We use Redhat ***kickstart*** mechanism to deploy the base SL and ***puppet*** to configure computers according the Controls requirements

Windows PCs

- OS installation according the PSI Central computing division standard mechanism
- Extra software is installed by the Controls IT

- Protecting physical network ports, identify the authorized hardware connected to the private machine network
- Windows systems:
 - restricted OS installation, updates, limitation of mounted disk drives,
 - control system installation and distribution
 - IOCs configuration, installation and deployment
- Controls system security versus necessary users flexibility (data transfer, user's software, etc.)
- New and non standard hardware and software
- Systems stability, versus maintenance, updates, users change requests
- Scientists...

Acknowledgments

PSI Central Computing Security group

PSI Central Computing Network group

References

S. Lüders et al., “CNIC Security Policy for Controls”,
2011;<https://edms.cern.ch/document/584092>

http://www.hpc-ch.org/wp/wp-content/uploads/2010/06/KS_Puppet_VM_20100520_printout.pdf

<http://www.sls.psi.ch/controls/software/controls-software.pdf>

Two types of login accounts have been provided for both Linux and Windows computers:

- personal accounts - provide access to any system on the accelerator network (not attach network drives)
- group accounts (operator accounts) - only active on core systems necessary for operations

Linux: facility operator accounts used on Controls consoles mainly located in the Control room. It must not be used for software development or installation.

Windows: global measuring accounts used for long-term logins for service computers, oscilloscopes, etc..