Can off-the-shelf control systems be compliant with CERN computer security policy?

3rd Control System Cyber-Security Workshop (CS)2/HEP
Grenoble

9.10.2011

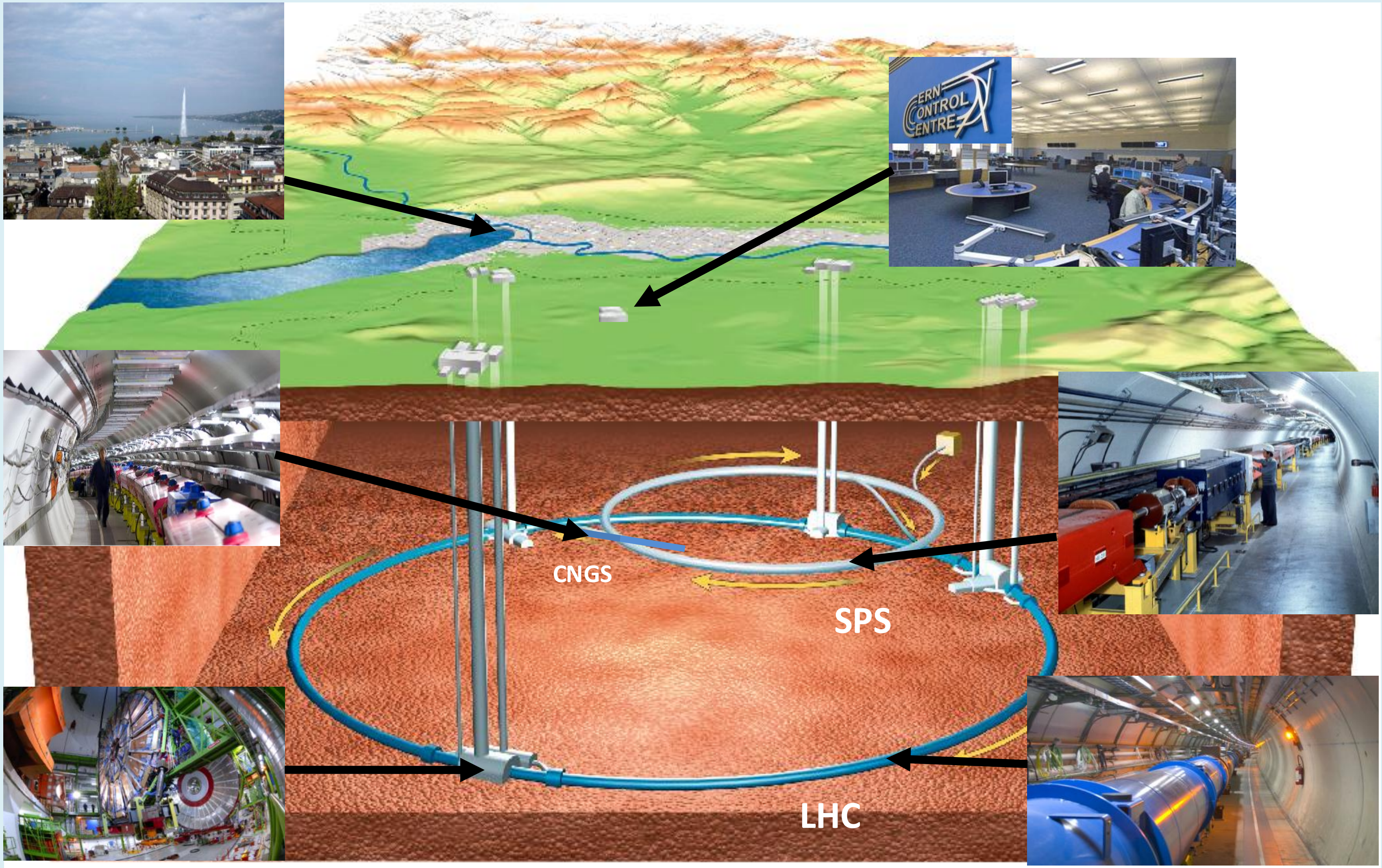
Timo Hakulinen, Pierre Ninin, Francesco Valentini
GS/ASE, CERN, Geneva

EDMS 1161633

Who we are and what we do

- **CERN** group **GS/ASE** is widely responsible for personnel access and safety systems at CERN.
- Focus on safety of the **accelerator complex**, general **site surveillance**, **fire and gas monitoring** (however: excluding radiation monitoring), **alarm systems.**
- **Design and implementation** of new access and safety systems, in particular management of projects and contracts.
- **Operation and maintenance** of existing systems.
- **Consulting** in matters of access and safety systems both internally at CERN and to external laboratories when requested.

Our playground



The environment we live in

- Networks:
  - CERN General Purpose Network (GPN), Technical Network (TN), experiment networks.
  - Our private (safety-related) networks.
  - Internet.
- Services provided by CERN:
  - Windows service (Domain, DFS).
  - Linux service (AFS).
  - Software installation services (CMF, YUM)
  - Oracle service.
  - Authentication services (Single Sign-on, Kerberos, LDAP).
  - Web services (Windows and Unix based).
  - Security patches, scans, and monitoring.
- Policies governing use:
  - CERN computing rules (general usage, computer security).
  - CNIC (Computing and Network Infrastructure for Controls) rules for controls networks.

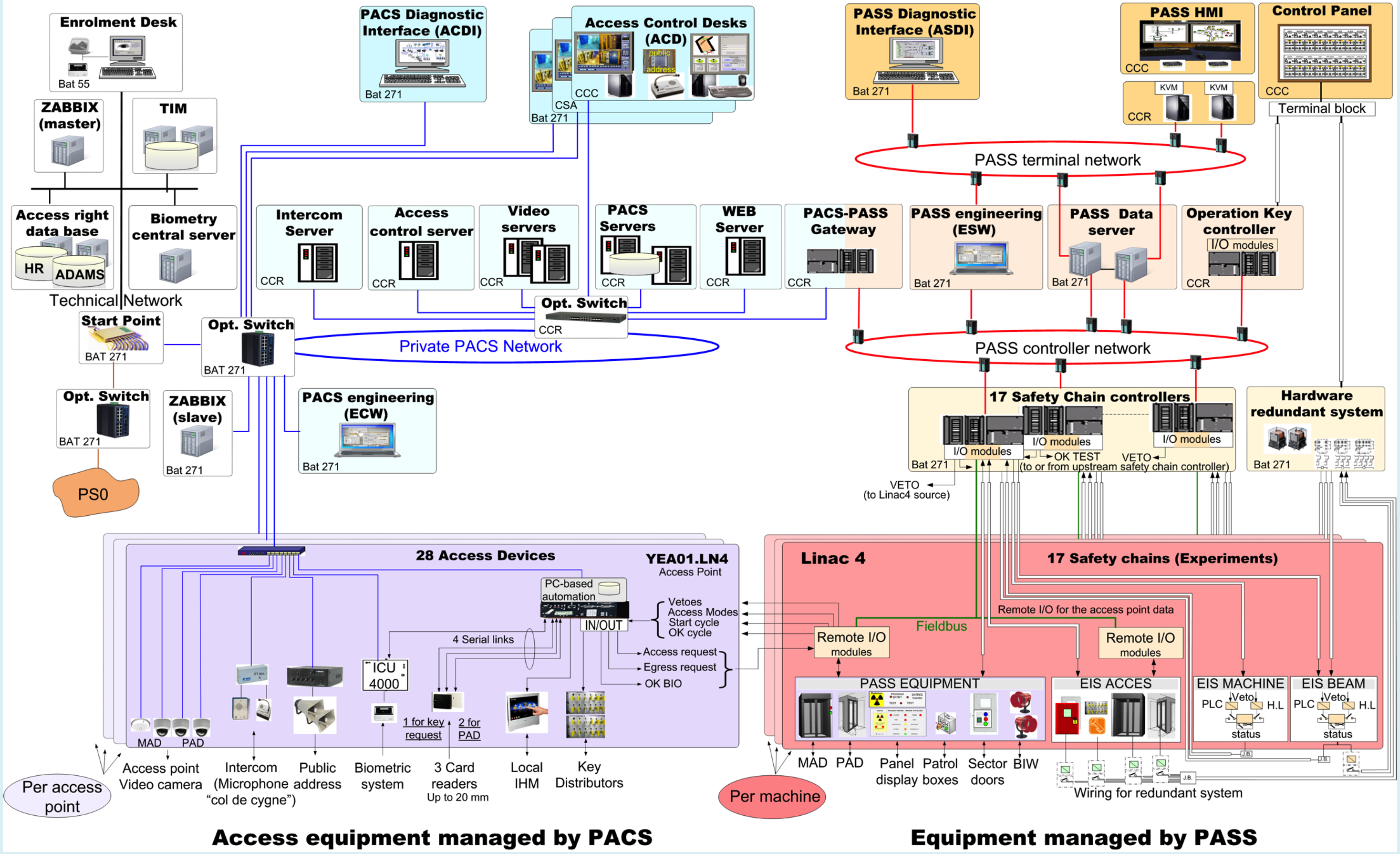
Access and safety systems by GS/ASE

- **LACS** (LHC Access Control System) – who enters LHC and when?
- **LASS** (LHC Access Safety System) – is it safe for beam or access?
- **PACS** (PS Access Control System) – idem for PS (a renovated system to be implemented during shutdown 2013-2014).
- **PASS** (PS Access Safety System) – idem …
- **SPS PSS** – integrated personnel safety system for SPS.
- **SUSI** (Surveillance des Sites) – who enters CERN sites and areas other than the accelerators.
- **CSAM** (CERN Safety Alarm Monitoring) – alarms for the fire brigade.
- **Sniffer** – gas detection and alarm.
- **SIP** (Site Information Panels) – display relevant info at access points.
- **TIM** (Technical Infrastructure Monitoring) – access status data of control equipment.
- Safety systems developed by us but operated by others: **SSA** (Atlas), **Ramses** (radiation monitoring).

What kind of systems?

- Access and safety systems are quite heterogeneous:
  - Servers (Windows / Linux)
  - Operator posts (PCs at control rooms / access service)
  - Panel-PCs (local displays / information panels)
  - PLCs / UTLs (local special purpose control units)
  - Video cameras / recorders
  - Biometry units (iris-scan)
  - Interphones (at access points and operator rooms)
  - Card readers
  - Key distributor units
  - Databases / web-servers
- Many different manufacturers.
- Most of these units directly network connected.
- Mainly in TN but also some equipment in GPN and the most important systems have their own private networks.

Example: PS access and safety system



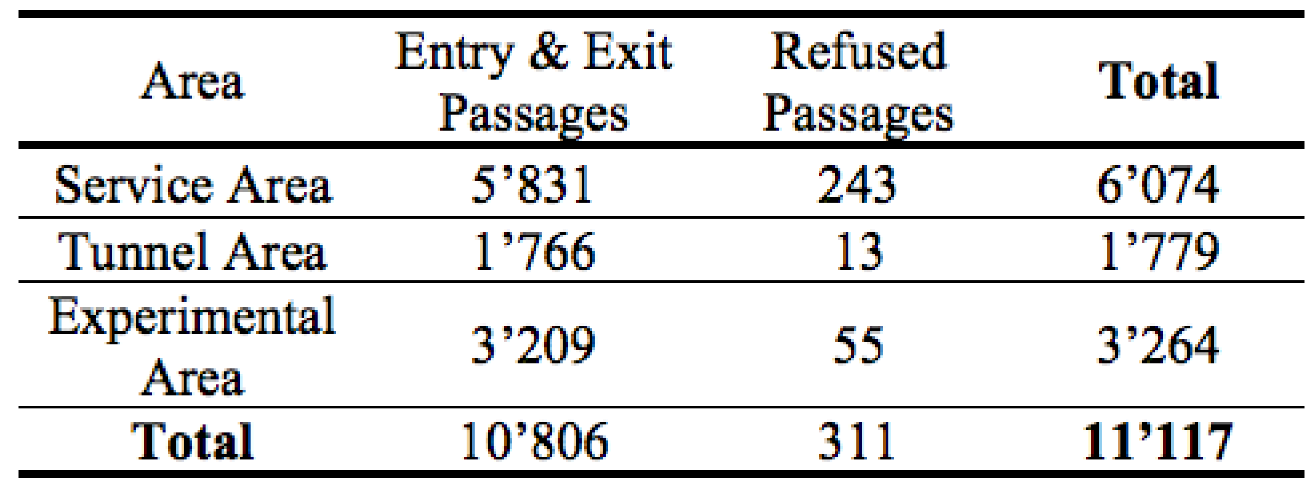
Access equipment managed by PACS

Equipment managed by PASS

Requirements on our systems

- Mission critical safety systems (LASS, PASS): System malfunction will stop beam.
- Highly visible and actively solicited: Access to sites and accelerators ➔ very high availability necessary.

Example: LHC access statistics of 5 days (Aug 29 – Sep 2):



Area	Entry & Exit Passages	Refused Passages	Total
Service Area	5’831	243	6’074
Tunnel Area	1’766	13	1’779
Experimental Area	3’209	55	3’264
Total	10’806	311	**11’117**

Risks related to computer security

- Technical
  - A security breach may bring down an important control system ➔ beam loss, personnel safety compromised, data loss.
- Financial
  - Wasted time and money due to outage and to run analysis and mitigation procedures.
- Legal
  - CERN may even be legally responsible in some cases (copyright violation, failure to prevent misuse).
- Reputation
  - Very bad PR for CERN.

Some pertinent CERN policies

- Password quality and expiration
  - Check while changing the password.
  - Expiration can be sometimes deactivated.
- Security patching
  - Patching policy controllable by administrators.
- Security scans
  - Automatic on every device – opt-out in problem cases.
- OS versions
  - A set of centrally supported versions – rest tolerated if supported by the vendor.
- USB sticks
  - Restrictions in controls networks – use case necessary if needed.
- Internet access from TN
  - Generally blocked – use case necessary if needed.

What kind of systems (redux)?

- What is “off-the-shelf” to us?
  - Integrated systems built for us but with commercially available standard components (hardware and software).
  - Minimum in-house development.
  - PLC’s, controllers, communication equipment, etc.
  - Commercial SCADA, configuration and monitoring software.
- SCADA software running on Windows:
  - WinCC: Only Siemens-validated OS + patches.
  - PCVue: Only ARCinfo-validated OS + patches.
  - Factorylink: No longer supported on current OS’s.
  - ➔ Not free to change at will.
- PLC’s and the like:
  - Siemens (different generations), Schneider (idem.), Wago.
  - UTL’s of the Evolynx access control system.
  - Various special purpose controllers.
  - ➔ Some of these are non-robust and not readily fixable.

Some typical problem cases

- Security scan problems (NMAP):
  - Biometry units disconnecting from server ➔ access to LHC not possible by the affected access points.
  - Disturbance of remote I/O units ➔ LHC Material access devices (MAD) unavailable, not possible to pass material by the affected access points.
  - Crash of DAQ card accessing LASS gateway ➔ safety system status information not available + LHC access mode change not possible.
  - At first these problems took a while to debug, now we know what to check first…
- Security patching:
  - After a patch, local security policies on panel-PCs got auto-tightened ➔ certain network connections started failing.
  - New Web-browser versions have a habit of breaking applications in sometimes non-obvious ways.
  - For LHC access system we run patched systems on our test bench for a month before committing to prod – however, cannot spot everything.
- Password issues:
  - Expiration of service passwords: Many scripts and binaries to change.
  - Password quality control problems: Hardcoded "simple" passwords no longer pass the test.
  - Vendor default passwords: Some are visible on the vendor's web-site.
- Unsupported OS versions:
  - Old hardware requires old SCADA requires old OS ➔ may require full system revamp.

What to do when stuff breaks?

- Devices having trouble with security scans can be excluded.
- It may be possible to reverse misapplied security patches – and if not, reinstall (this can be a big ouch).
- How about systems running antiquated OS's?
  - It may not be feasible to upgrade at a given time (operational constraints, may provoke other upgrades, cost, …).
  - Can the machine be otherwise secured: firewall, virtual machine, disconnect from network?
- What to do with unpatchable embedded systems / hardcoded passwords / other vendor goofs?
  - Same story as above – also, kicking the vendors surprisingly futile!
- System isolation behind a private network segment:
  - Pretty brainless but if it becomes necessary…
  - Math exercise: a (hypothetical) system upgrade 500 kCHF / 1 year, private network 50 kCHF / 1 week.

So, what’s the answer then?

Q: Can these kinds of systems remain compliant with CERN security policy?

A: Have to! However, adaptation/interpretation of the policies may be necessary in some cases.

Miscellaneous suggestions

- A way to control security scans to sensitive equipment.
- Ability to query security scan data of equipment (schedules, history, results) to be able to correlate with monitoring data.
- A way to coordinate validation of system robustness during commissioning.
- Test platform, where equipment can be stress-tested and qualified in a controlled environment.
- Conformity spec of CERN security measures to be given to equipment and system vendors – a detailed laundry list of things to take into account.

Conclusions

- **Clearly**: strict policies directing use of computing resources and limiting misuse are necessary.
- **However**: these policies may/will clash with poorly designed/implemented or legacy systems.
- **Unfortunately**: some of those systems cannot be easily fixed.
- **Therefore**: mitigation will be necessary on a case by case basis.

Thank you!

Questions?