Disconnecting Controls

Stefan Lüders
4th CS2HEP @ ICALEPCS2013

CERN Networking

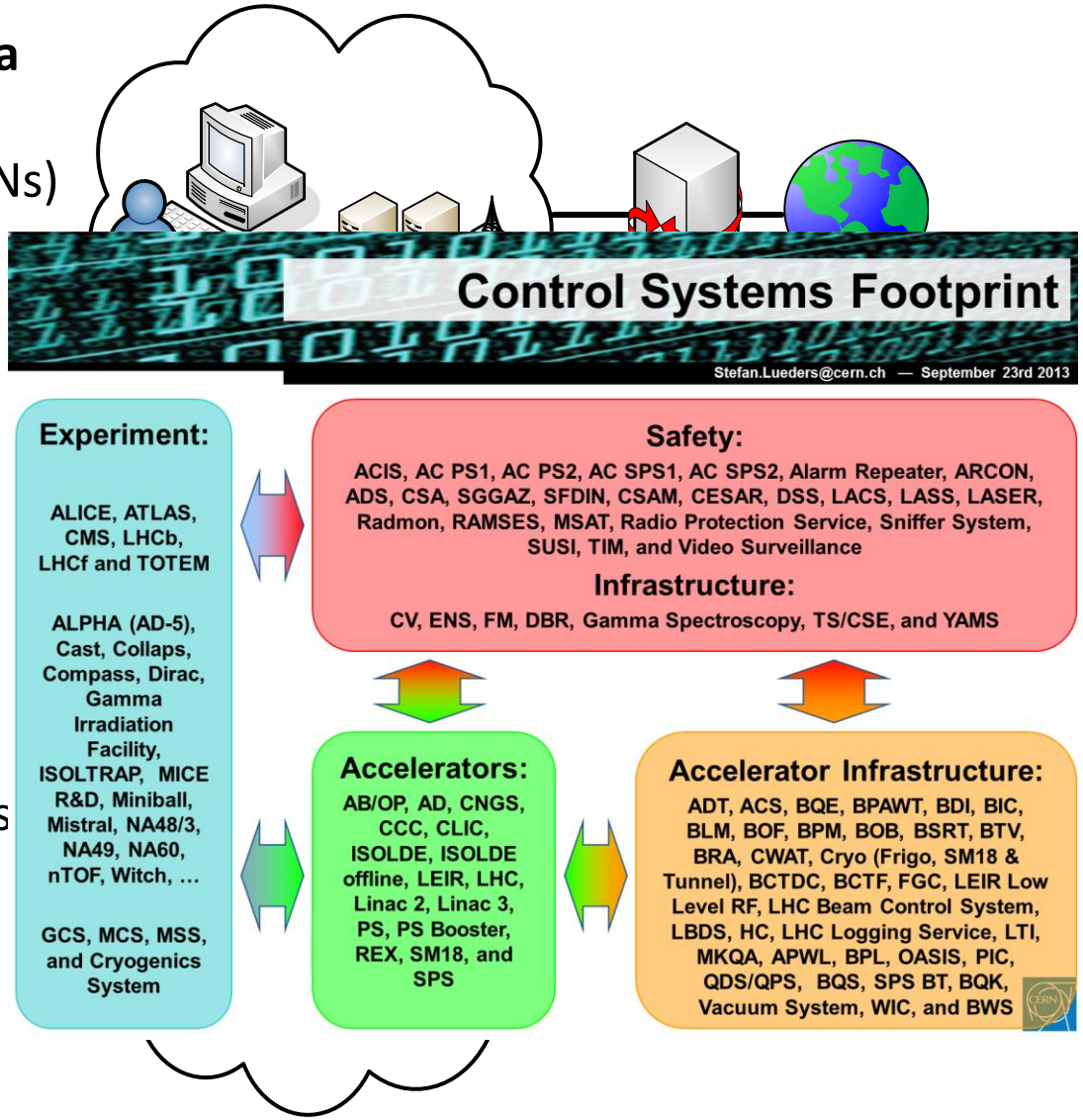
"Controls Network" for

- **Accelerators & infrastructure aka "Technical Network" (TN)**
- (LHC) "Experiment Networks" (ENs)

The Technical Network hosts **>100 different control systems** of different sizes.

Access is **restricted on router level** and based on 1-to-N ACLs.

Proper firewalling is currently **impossible** as inter-network traffic is too complex and to variable.



Depending on the CC

Central CERN IT services are hosted in the CERN Computer Centre (CC).

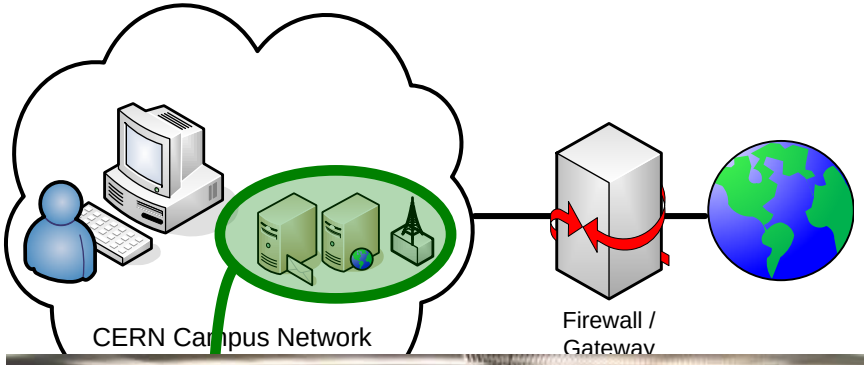
The CC is connected to the CERN campus (office) network (“GPN”).

Controls or DAQ-dedicated services are **hosted locally** on ENs/TN.

Accelerator controls depend on both.

Concept of “Trusting” & “Exposing”:

- **“Trusted” devices are visible to whole TN/EN**
- **“Exposed” devices are visible to whole GPN**

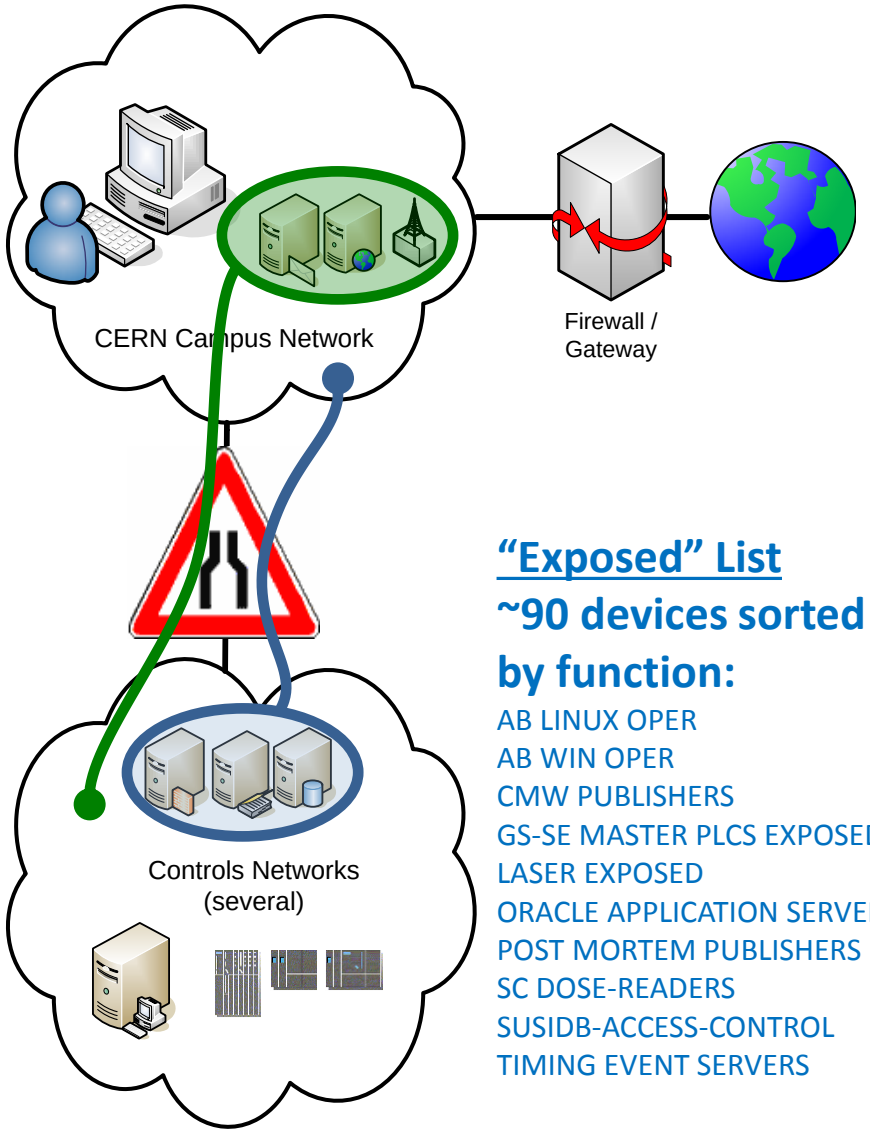


The Full Listing

“Trusted” Bypass List

~1200 devices sorted by function:

AB FEC DEV
AB FESA DEV
AB LINUX DEV
AB MISC DEV
AB PO FECS
AB WIN DEV
BE OPERATIONS
BE VM DEVELOPMENT
DIP GPN HOSTS
EN-CV TEMPORARY PATCHING
EN-ICE APPLICATION GATEWAYS
GS-ASE CSAM - NO TN
GS-ASE-AAS SERVERS - NO_TN
GS-SE PLC SERVERS TRUSTED BY TN
ISOLDE NO TN
IT BACKUP SERVERS
IT CC AFS
IT CC CDB
IT CC CONSOLE SERVICE
IT CC CVS
IT CC SVN
IT DB ACCELERATOR
IT DB MANAGEMENT
IT DB WEB
IT LICENCE SERVERS
IT LINUXSOFT
IT NICE CMF SERVICES
IT SECURITY BACKENDS
IT TELEPHONE SERVERS
LCR FOR 936
LCR FOR BI
LCR FOR BT
LCR FOR CCR
LCR FOR ICE
LCR FOR RF
LCR FOR STI
LCR FOR VACUUM
NICE_CA
NICE_DFS
NICE_DOMAINCONTROLLERS
NICE_MAIL_MX
NICE_PRINTING
NICE_TS_INFRASTRUCTURE
NICE_XLDAP
PH EXPERIMENTS
SC GPRS
TN APPLICATION GATEWAYS
TN INTERNET PUBLISHERS
TN WEB SERVERS
TS-CV SERVERS - NO_TN
TS-EL SERVERS - NO_TN
TS-FM SERVERS - NO_TN
TS-HE GPRS



“Exposed” List

~90 devices sorted by function:

AB LINUX OPER
AB WIN OPER
CMW PUBLISHERS
GS-SE MASTER PLCS EXPOSED TO GPN
LASER EXPOSED
ORACLE APPLICATION SERVERS
POST MORTEM PUBLISHERS
SC DOSE-READERS
SUSIDB-ACCESS-CONTROL
TIMING EVENT SERVERS

TN Disco Test

Cut the cable between GPN and TN.

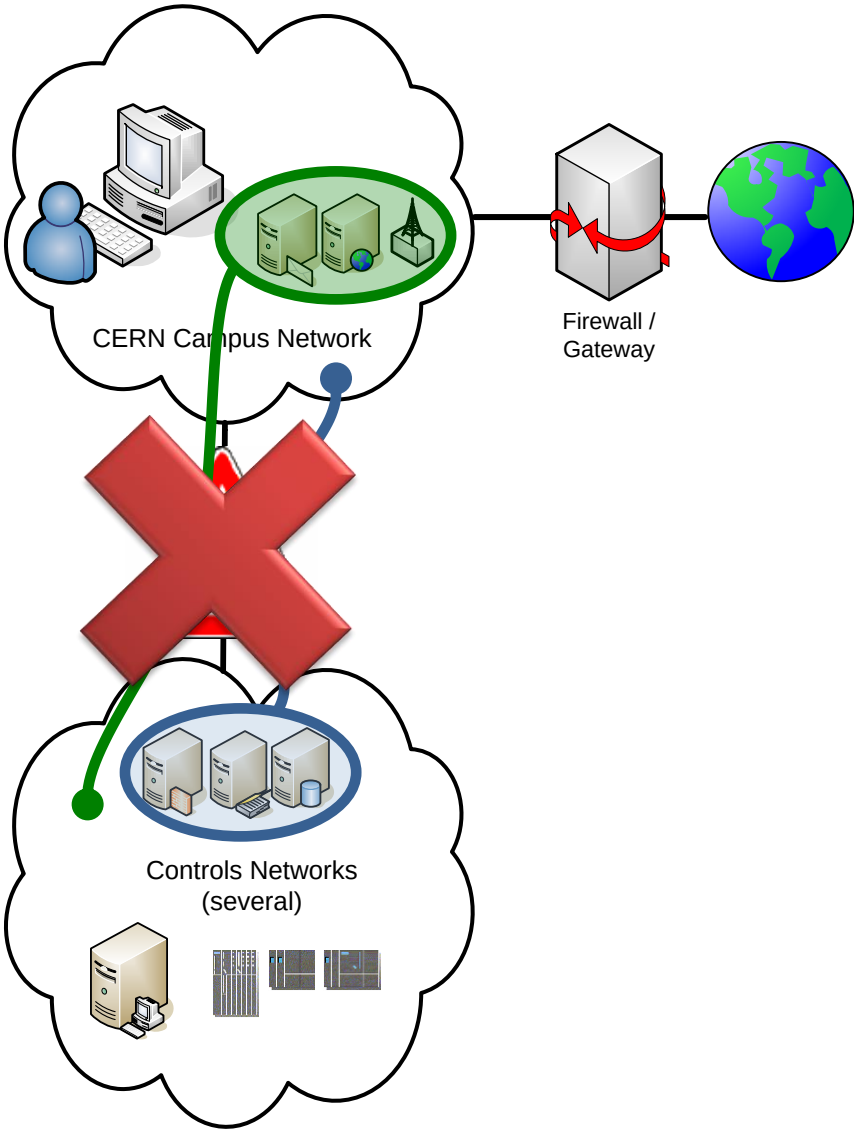
Control systems should be able to **continue running.**

Objectives:

- **Reassure people** that disconnection does not do harm;
- **Understand extent of dependency** on external services;
- **Confirm autonomy**;
- **Confirm** that disconnection is **valid preventive action** in case of major security incidents e.g. in the CC.

Downer:

This is LS1 – many systems were in maintenance mode…



Findings

We did not screw up: No system failed nor mal-functioned.

As expected,

- Remote maintenance / access was inhibited
- Data bases / web pages / file stores in the CC weren't accessible
- Some systems had to run in degraded mode

However, unexpectedly, we observed

- **Too long boot/log-in time of Windows PCs** due to long time outs of start-up and login-scripts (e.g. affecting Cryo, Vaccum, RAMSES)
- **Hidden dependencies on AFS** e.g. when log-in into Linux PCs (probably related with Kerberos) and for PVSS fwAccessControl
- **GUI blocking issue in RBAC** related with NICE SOAP AuthN, e.g. for TIM Viewer (and, thus, PS/SPS tunnel accesses), LASER/DIAMON/OASIS GUI (in particular for CTF3)

In addition

Smaller surprises:

- Hidden dependency in BI RBAC fetching software from a GPN development PC
- BE MONI server crashed (cause unknown; probably AFS related)
- HP Proliant server monitoring failed

Expected, but potentially nasty:

- **IMPACT** not able to sync new requests to the ACS
- **Missing license servers** e.g. Mathlab (CTF3) and Mathematica (Tomoscopes) not able to start.
- **Dependency on DHCP and PXEboot** (need to be retested)
- **Dependencies on CERN SSO/winservices-soap** for certain web applications e.g. for ACC Control Configuration DataBase and TIM

The remaining rest:

- TIM DB, Spectrum network monitoring, RAMSES touch panels, guardians CCTV, access cards & biometry (ZORADB vs. HRDB)

Next Steps

Currently, we're trying to **mitigate issues** related with Windows Start-Up/Log-In and Linux AFS dependency (and a few others).

By-end-2013, we plan to **re-conduct the TN Disco Test** with mitigations in place **as well as in June 2014** with systems operational, online, and beam in PS/SPS.

In 2014, we would like to understand **possible operation levels at TN/GPN disconnection:**

- Scenario 1: Immediately stop any beam and put accelerators in a safe mode
- Scenario 2: Keep operation as usual; stop only if disco last more than NN mins
- Scenario 3: Depending on machine mode, either stop LHC beam (e.g. if not yet in physics) or keep physics mode until EIC/experiments detect non-safe situation
- Scenario 4: (other scenarios as defined by the accelerator sector)

Once defined, we would need to **provide cost estimates** of mitigations and fixes, implement, and validate.