Pierre Charrue (CERN) – Terri Lahey (SLAC)

Technical Network Dependencies and Risk Questionnaire

Status Report

Abstract

Accelerator Control Systems are critical to the operation of modern accelerators. In large control systems, there are often a large number and variety of networked computers. Each computer has its own security issues, and depends upon services running on other computers. In this presentation, we describe an inventory application built to improve the security and reliability of the controls system computers. The inventory tracks multiple security-related attributes of the computers on the CERN Technical Network and analyzes risks, so that we can mitigate risks and plan for future control system enhancements.

Outline

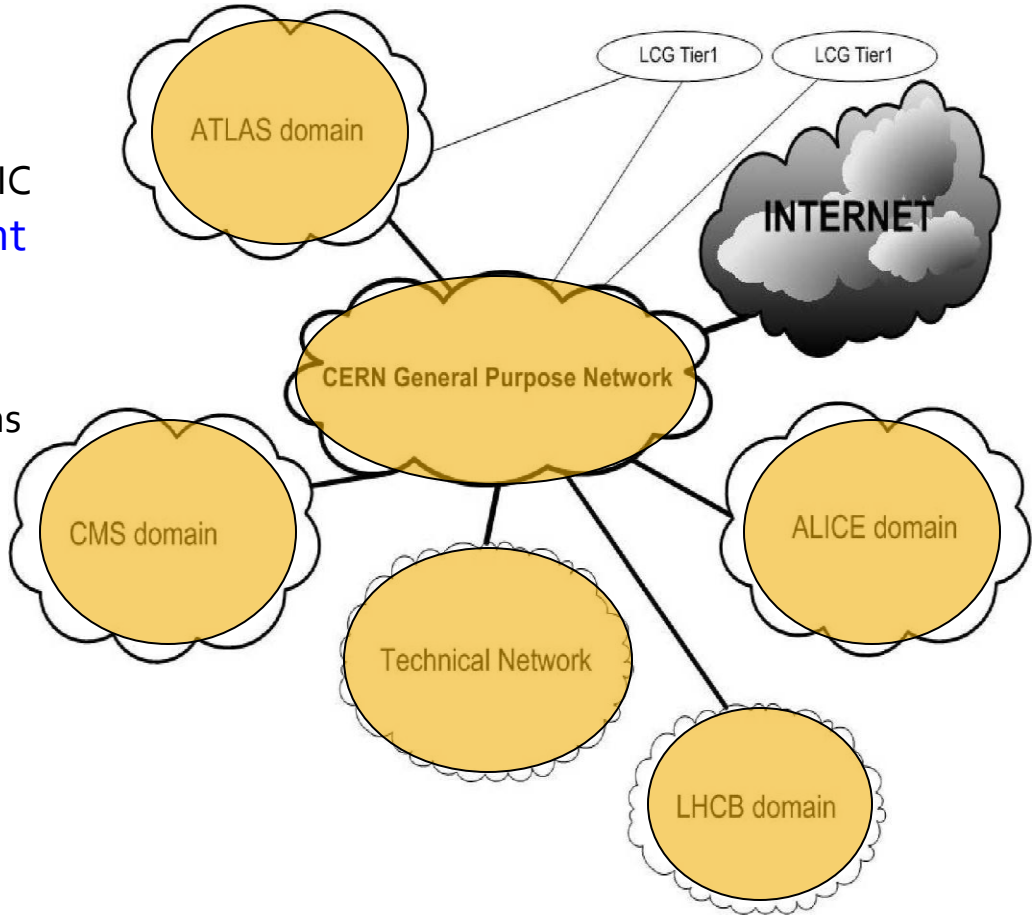
- Networking and Databases
- The TN dependencies and Risk Questionnaire project (TNQ)
- The TNQ in details
- The situation today
- Plans

Outline

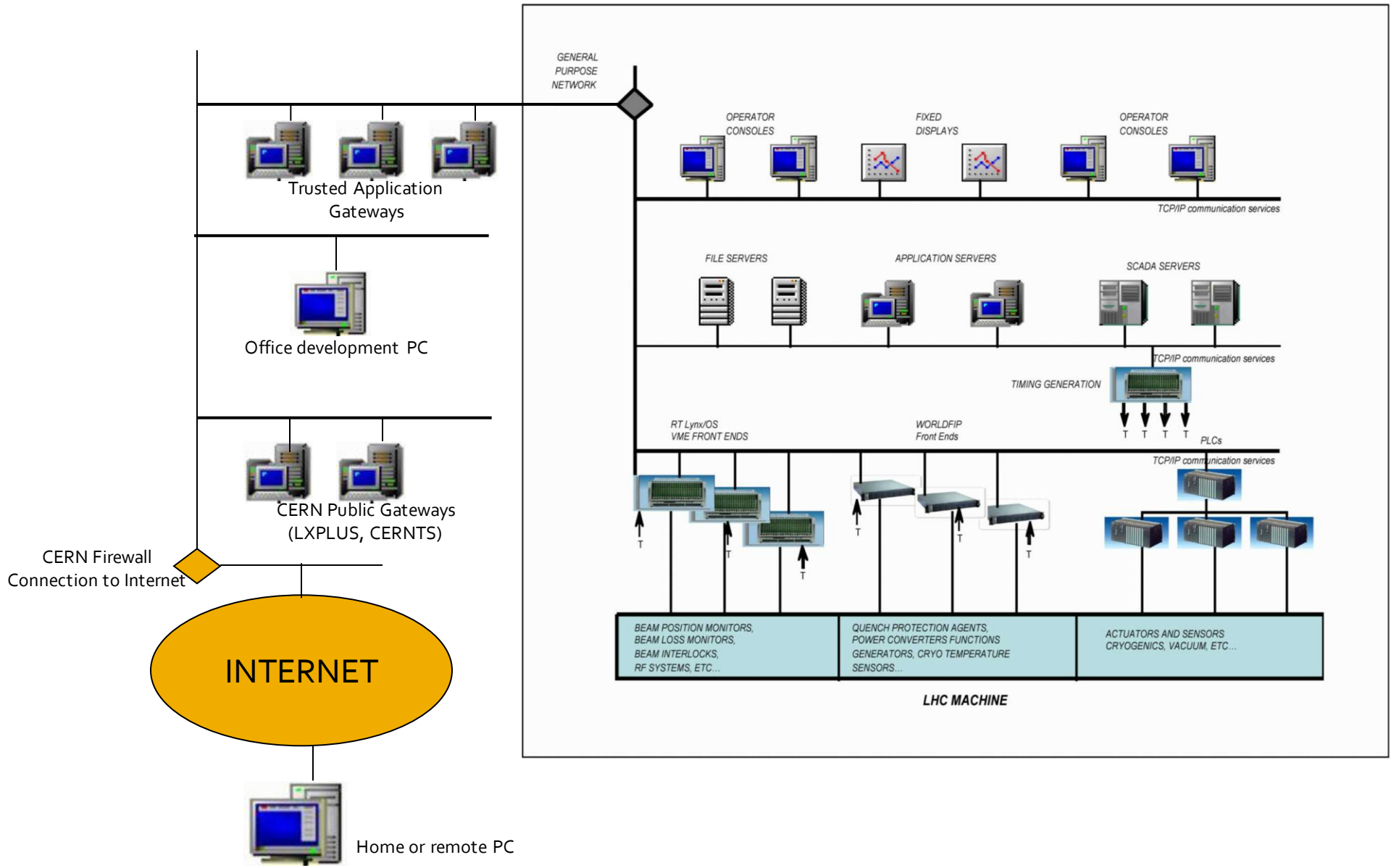
- **Networking and Databases**
- The TN dependencies and Risk Questionnaire project (TNQ)
- The TNQ in details
- The situation today
- Plans

Networking at CERN

- General Purpose Network (GN)
  - For office, mail, www, development, …
  - No formal connection restrictions by CNIC
- Technical Network (TN) and Experiment Network (EN)
  - For operational equipment
  - Formal connection and access restrictions
  - Limited services available (e.g. no mail server, no external web browsing)
  - Authorization based on MAC addresses
  - Network monitored by IT/CS



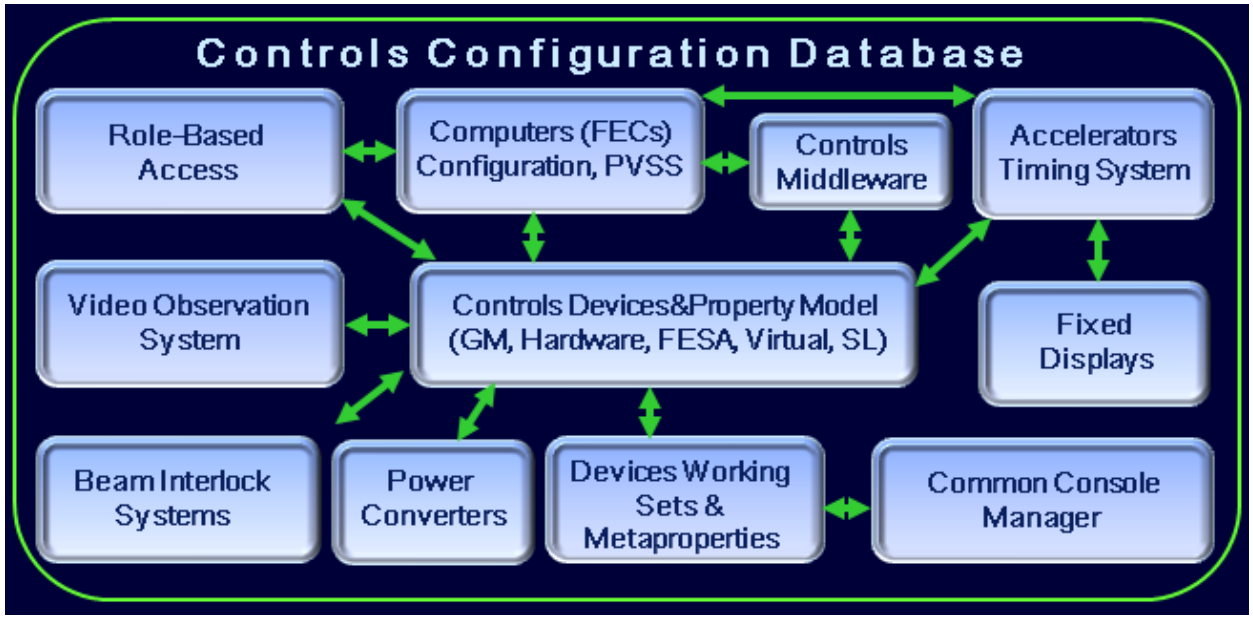
The Technical Network



Databases - CCDB

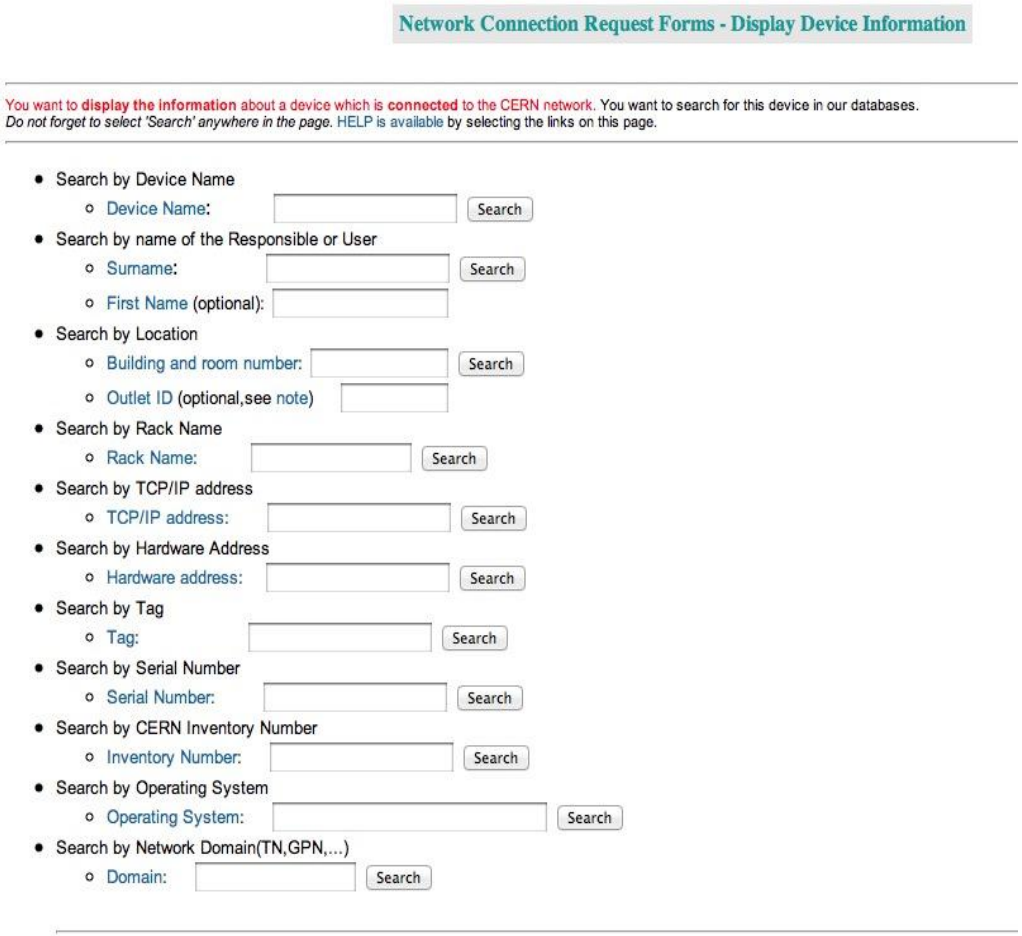
- The CCDB contains a detailed description of all Controls hardware and software entities with:
  - Name
  - Type
  - Description
  - Location
  - And several configuration definitions such as timing, alarms, in operation, …
- Each device used in the controls infrastructure has an entry in the CCDB
- Access in read and write is protected by a CERN identification

The Controls Configuration Database



Databases - Netops

- Any device that has an IP address MUST be defined in the NETOPS database
- All devices in the NETOPS database has:
  - A main user
  - A responsible
  - A location
  - A hardware address
  - A name
  - An IP number
- Prior to be connected to the CERN network, a device has to be declared in the NETOPS database
- Access to the NETOPS database is protected by a CERN identification



Outline

- Networking and Databases
- **The TN dependencies and Risk Questionnaire project (TNQ)**
- The TNQ in details
- The situation today
- Plans

Project Goals and scope

- **Improve the security** and hence the reliability of the Accelerator Control Infrastructure.
- **Identify the most critical** security risks in the Control System so we can fix them.
- **Identify solutions** to improve the security, so that we can pursue funding and implementation
- The **scope** covers **all devices connected to the TN**, their **Operating Systems** and the **software** described in the CCDB (mainly FrontEnd device servers and Operation Console Applications)

Project phases and deliverables

1. **Phase I**
   - Make an inventory of service/system and their dependencies
   - Implement a questionnaire to collect the A&T sector data
   - Implement a Data Base with a web interface to enter the data
   - Populate the database
   - Extract the security risks from A&T sector data

2. **Phase II**
   - Mitigate these risks with management and derive the actions needed to address them
   - Propose action in management
   - Proceed with implementation of agreed actions

Project phases and deliverables

- Create database and web-based application using existing tools used by CERN:
  - ORACLE including PLSQL & APEX
  - Benthic (golden, goldview, pledit)
- Work with LHC Controls Security Panel (LCSP), includes representatives from all A&T sector departments and central IT
- Work with IT networking, CERN Security Officer, and Controls Database Experts

Inventory and Dependencies

- A **questionnaire** has been created to identify
  - Service/System [is made of Device and DataStore]
  - Device [has Operating System, Users, location, Application]
  - User [has name, password]
  - Application [has language, version, review]
  - Other attributes .. (see an extract next slide)

- For each **attribute** its **risk** is evaluated
  - Low, Medium, High/Unknown, Inherited

Responsibility	The service/system owner is responsible for the correctness of this data. Any deliberate mis-information will be reported to the corresponding department head.								
Scope	The scope is focussing on "Cyber-Assets". Physcial security, e.g. access restrictions or protections against power cuts, is not considered.								
Ownership	The CSO is owning this data.								
Version	SL V0.9 20091028								
Context	**Group**	**Item**	**Question**	**Low risk**	**Medium risk**	**High risk**	**Unknown risk**	**Inherited risk**	**Risk to be determined manually**
Service/System	General	Name	What is the name of this service/system ?	Name					
		Owner	What is the name of the system owner ?				Unknown	[Account]	
		Date	When was this questionnaire filled out ?	Date (Year/Month)					
		Provider	By whom was this questionnaire filled out ?					[Account]	
	Devices		Provide a list of all devices connected to the Ethernet					List of [Device]	
	Data Stores		Provide a list of all data stores containing service/system data, documentation, information, ...					List of [Device]	
	Dependencies							[Dependencies]	
	Procedures							[Procedures]	
	Security Risk Assessment							[Security Risk Assessment]	
	Training							[Training]	
Device	General	Name	What is the name of this device ?	Name					
		WebReq	Provide the link in the network database (http:\\network.cern.ch)	Automatic Link		Not existent			
		WebReq correctness	Is the WebReq information correct ?	Yes		No			
		LayoutDB	Provide the link in the layout database (http:\\????.cern.ch)	Automatic Link		Not existent			
	Operating System		Which operating system is this device running ?				Unknown		Name; Version
		Patch/upgrade means	How is this O/S upgraded/patched ?	CMF centrally	CMF locally	Manually; never	Unknown		
		Patch/upgrade frequency	When has this device been upgraded/patched the last time ?	This month	Last 3 months	Last 6 months or more; never	Unknown		
		Link to CMF	CMF: please provide a link to CMF	Automatic Link		None			
	Anti-Virus		Which anti-virus software is this device running ?			None	Unknown		Name; Version
		Patch/upgrade means	How is the virus signature file updated ?	CMF centrally	CMF locally	Manually; never	Unknown		
		Patch/upgrade frequency	When was the last update ?	This month	Last 3 months	Last 6 months or more; never	Unknown		
	Logging		Where is this device logging important system/security parameters ?			No	Unknown	List of [Data Store]	
		Review	Who is reviewing this logging data ?				Unknown	List of [Account]	
		Review frequency	How often is this data reviewed ?	Real-time (via alerts), Daily	Weekly	Monthly or more; never	Unknown		
	ACLs		Is this device applying IP access control lists ?			No		Yes	
		IPs	Provide a list of devices permitted access	None		All	Unknown	List of [Devices]	
	Firewall		Is this device restricting firewall openings ?			No		Yes	
		IPs	Provide a list of devices permitted access	None	All, but port filtered	All	Unknown	List of [Devices]	
		TCP ports	Which are the open TCP ports ?	None; SSH, RDP, HTTPS, NTP	HTTP, SNMP	FTP, TELNET, RLOGIN, SHELL, EPMAP, NETBIOS	Unknown		List of other ports
		UDP ports	Which are the open UDP ports ?	None; SSH, RDP, HTTPS, NTP	HTTP, SNMP	FTP, TELNET, RLOGIN, SHELL, EPMAP, NETBIOS	Unknown		List of other ports
	Open Shares		Which are externally accessible folders ?	None				List of [Data Store]	
	Network		To which network is this device connected ?	TN/EN	LCG	GPN, EXT			Other
		Controls Sets	Is this device protected by Controls Sets ?	Yes		Not			

Courtesy S.Lueders

Outline

- Networking and Databases
- The TN dependencies and Risk Questionnaire project (TNQ)
- **The TNQ in details**
- The situation today
- Plans

TN Questionnaire - Principles

- There is **no duplication of data**
- CCDB, NETOPS & HR data are linked and not copied into TN questionnaire
  - NETOPS
    - Computer definitions, including network domains
    - Set Definitions
  - CCDB
    - Software: DSC, Applications, Class Software (eg.FESA)
    - Software Families
  - HR people information

TNQ Principles (2 of 3)

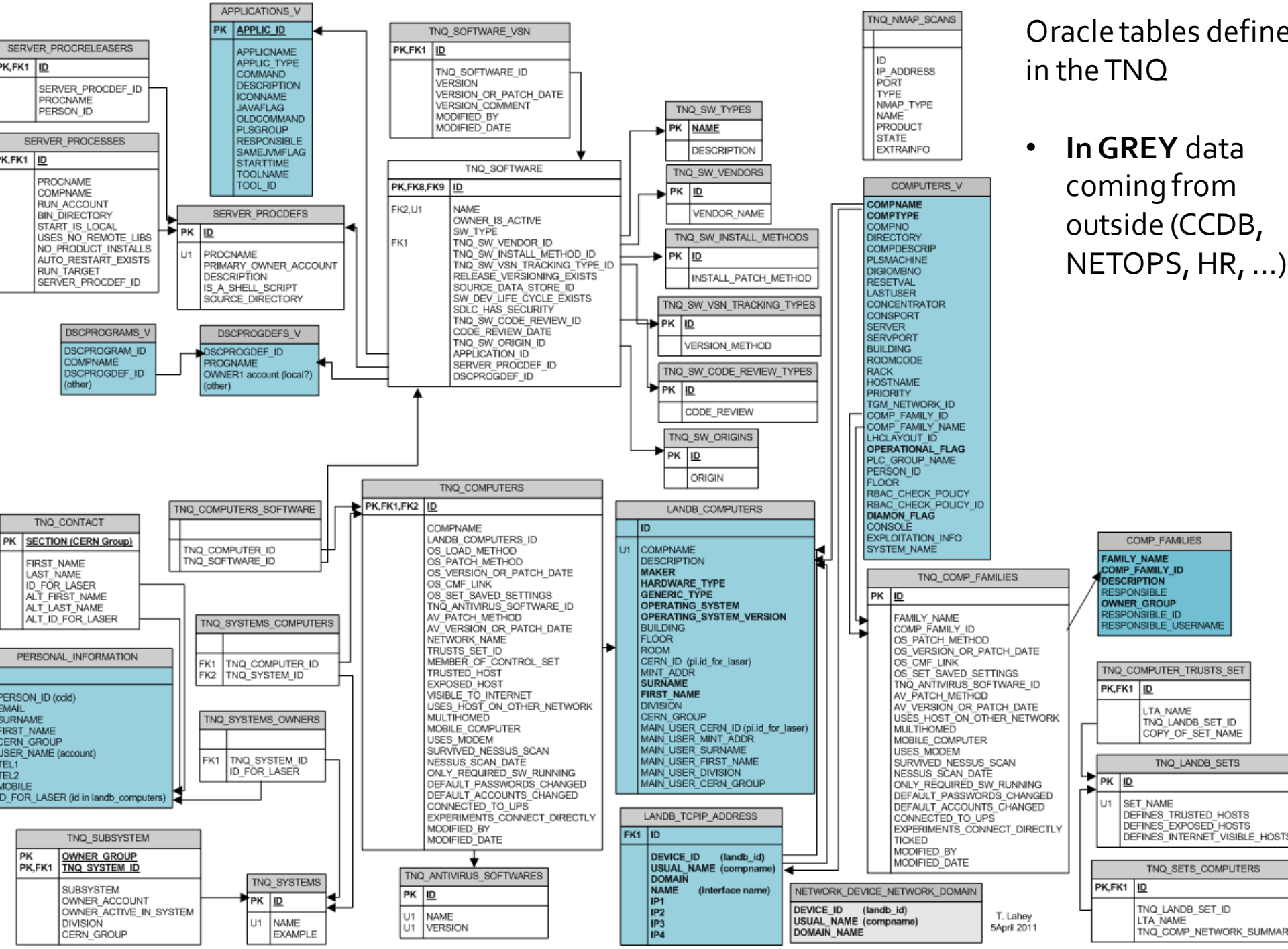
- Extreme care has been taken to **ease the work of the end-user** entering data
  - Use existing data
  - Derive TNQ data from existing data
  - automate wherever possible
  - simplify data entry
    - Apply the same changes to groups of devices by "group & owner" (template or copy) to avoid data entry for each individual devices
- Also improves data reliability

TNQ Principles (3 of 3)

- **Connectivity** between the TNQ and CCDB/NETOPS Databases:
  - Button to launch LANDB or CCDB window to edit or check data
    - LANDB: computers and sets
    - CCDB: computers and software
- Track which items have **not been updated**, so we can
  - identify remaining work
  - display only those items that need update

TN Questionnaire – Phase 1

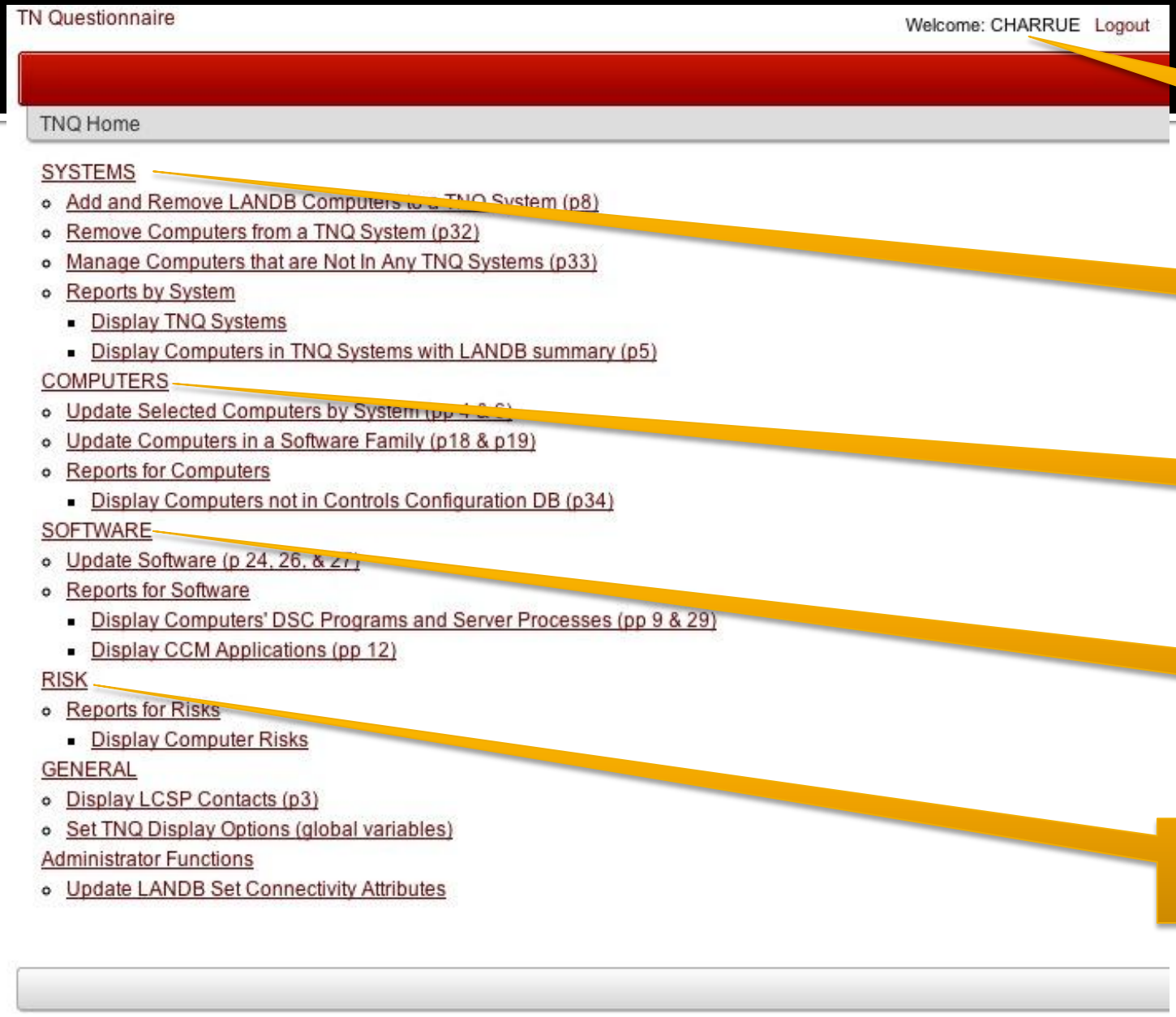
- Using standard **ORACLE-APEX**, a **web-based questionnaire** has been developed in close collaboration with the DM section
- 3 **major to**pics:
  - **Systems** (BI, BT, CRYO, OP, RF, …)
  - **Computers** (FrontEnd, PLC, Console, …)
  - **Software** (FESA servers, CCM application, …)
- A lot of data is taken directly or derived from the **CCDB and NETOPS databases**



Oracle tables define in the TNQ

- **In GREY** data coming from outside (CCDB, NETOPS, HR, …)

TN Questionnaire – Phase 1



NICE identification

SYSTEMS

COMPUTERS

SOFTWARE

RISK REPORTS

Systems

- 33 Systems have been identified so far
- Coordinating with CCDB system names

System Name	Subsystem	Example	CERN Group	Primary LCSP Co
Ion Sources & Survey System	-	(PLCs & PVSS)	BE-ABP	SCRIVENS Richa
BI - Beam Instrumentation	-	Beam Loss Monitors (BLM), Beam Position Monitors (BPM), Beam Synchronous Timing (BOB), Beam Synchrotron Radiation Telescope (BSRT), Beam TV Monitor (BTV), Beam-Beam Rate Monitor (BRAN), DC Beam Current Monitor (BCTDC), Fast Beam Current Monitor (BCTF), Longitudinal Density Monitor (APWL), Schottky Monitor (BQS), Tune Kicker (BQK), and Wire Scanner (BWS), Based Band Tune Measurement (BQE), Beam Abort Gap Monitor (BPAWT), Beam Orbit Feedback (BOF), Ionisation Profile Monitor (BGI), Longitudinal Desity Monitor (APWL), Luminescence Profile Monitor (BPL), BLRSPS	BE-BI	JENSEN Lars
CERN Wide Accelerator Timing (CWAT)	-	-	BE-CO	CHARRUE Pierre
Consoles: CCC and other consoles	-	-	BE-CO	CHARRUE Pierre
FE Computer Services	-	Crates, FE Computer Booting & Initialization, PLC, Ethernet/WorldFIP gateways, Remote Reset, Terminal Services, NTP/DNS, DHCP/BOOTP	BE-CO	CHARRUE Pierre
Servers	-	File, CMW, Application, Alarm, LSA, DIAMON, Video, PVSS/other SCADA, Oracle (Application & DataBase), TCPIP services, Web & other Servers, Testbed PC gateways, LO & Console Management	BE-CO	CHARRUE Pierre
BE/OP Systems	-	Management of Critical Settings (MCS); some PLCs	BE-OP	ALEMANY FERNANDEZ Rey Maria
RF, LLRF Controls, and RF diagnostics	-	LHC LowLevel RF (LHC LLRF), Accelerator Superconducting Cavities (ACS), Accelerator Injection Transversal Dumper (ADT), Accelerator Cavities Normal conducting (CAN) oscilloscopes and (RF) network analysers, RF signal switching system (ACS/ADT diagnostic)	BE-RF	BUTTERWORTH Andrew

TNQ for Systems

- TNQ actions on the Systems:
  - Add and Remove LANDB Computers *(TN and Trusted)* to a TNQ System
  - Remove Computers from a TNQ System
  - Manage NETOPS Computers that are Not In Any TNQ Systems
  - Reports by System
    - Display TNQ Systems
    - Display Computers in all TNQ Systems with LANDB summary

TNQ for Computers

- TNQ actions for computers:
  - Update Selected Computers by System
    - Answer questions for one computer
    - Filter list of computers & apply answers to list of computers (*)
    - Also useful for interactive reports
  - Update All Computers in a Software Family
    - Answer questions for family & apply answers to all computers (*)
    - Also useful for interactive reports
  - Reports for Computers
    - Display Computers not in Controls Configuration DB

Computer Questionnaire

Launch LANDB Window | Display Selected Computer in CCDB Window

TNQ Questionnaire Computer — Cancel | Apply Changes to TNQ Computer

Id 670
Computer Name cwe-2001-ctfb
LAN[illegible] Computers ID 155470
How is the Operating System[illegible]ded? Over Ethernet
What method is used to patch the Operating System? [illegible] Repository – YUM Auto Update, Manual Reboot
Date of Last Installed Operating System Version or Patch
Select Anti-Virus Software NONE
How is the anti-virus signature file updated? Not Applicable
If On-Demand, Enter Date of Last Installed Anti-Virus Signature File

Launch buttons to NETOPS or CCDB

Is this a Mobile Computer (eg. special unit configured for mobile)? No
Does this computer connect to the network via a Modem? No
Do you apply Local Configurations after Installing the Operating System? Yes
Are Only the Required Software & Services Installed? No
Have Vendor Default Passwords been Changed? Yes
Have Vendor Default Accounts been Changed? Yes
Do Experiments Rely Directly on this Computer (eg. not on DIP)? No
Last Modified By TLAHEY
Last Modified Date 23-MAR-11

Computer Data from LANDB and Layout/CCDB

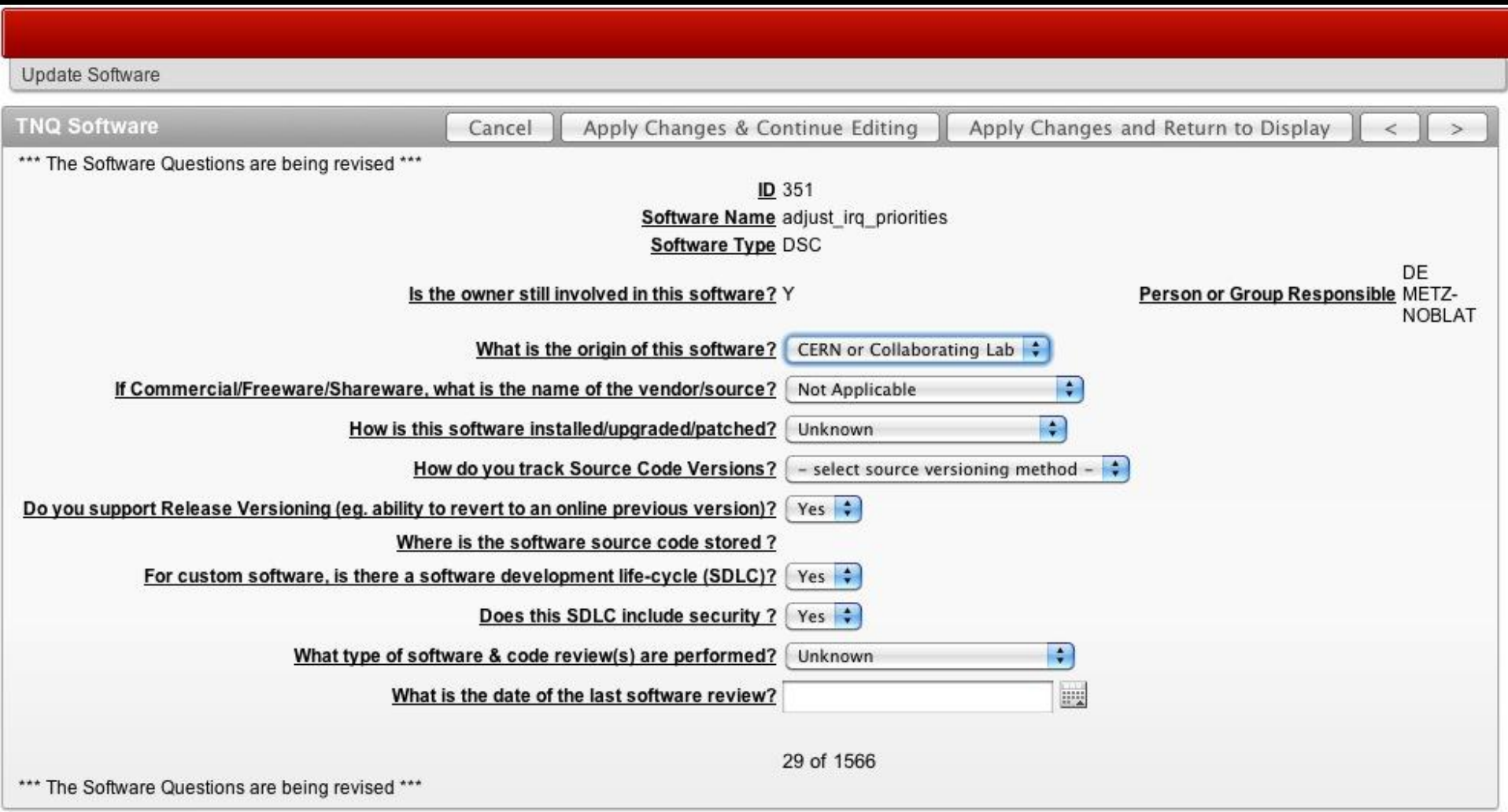
Building	Operating System	Operating System Version	Network Name	Member Of Control Set	Trusted Host	Exposed Host	Visible To Internet	Multihomed	Connected To Ups
2001	LINUX	SLC5	TN	N	N	N	N	N	(null)

1 - 1

TNQ for Software

- TNQ actions for software:
  - Update Software
  - Reports for Software
    - Display Computers' DSC Programs (CCDB)
    - Display Server Computers' Processes (snapshot)
    - Display CCM Applications (CCDB)
  - Automate lists of Software
    - Adding list of FESA and other class software
    - Automating lists of Server Processes
    - Add other existing lists of software, as identified

Software Questionnaire



Outline

- Networking and Databases
- The TN dependencies and Risk Questionnaire project (TNQ)
- The TNQ in details
- **The situation today**
- Plans

Current state of the TNQ

- The TN questionnaire is in production since mid April'11 and system owners started to populate data into the questionnaire
- In addition, a **positive side effect** is that NETOPS and CCDB databases are being cleaned
- Report summaries display problems that are simple to find and fix. LCSP member found
  - Computers assigned to the wrong group/person or with wrong description
  - Computers where responsible/user group are empty, likely no reassignment when someone left CERN is
  - Unexpected computer definitions, eg. 2nd IP address
  - We can find computers that are obsolete or in the wrong NETOPS set
- This cleaning of the CCDB or NETOPS is eased by the **buttons to launch the existing editors**
- Remember that the TNQ does NOT write in CCDB or NETOPS

Future Plans

- Define more RISK assessments
  - Combine risk factors, eg. computers visible to TN and their update dates/methods
- Adding more features
  - Create reports of computers with special network routing
  - Create reports of computers with difficult access (in tunnel)
- Network Scans
  - Load data from Network scans
  - Use it to compare expected open ports
- Derive more data
  - Summary from Central Management of windows/linux: Date Patches applied, Patches needed, Reboot Needed

Summary

- The TN Questionnaire is ready in production
  - Uses data from other database to reduce work and improve data reliability
  - Eases update by applying answers to groups of computers, etc.
- The LCSP members are now entering the data to populate the TN Questionnaire DB
- While entering data, LCSP is Reviewing and Cleaning up existing data
- We have plans for adding more Features to the TN Questionnaire
- Extract and present first Risk assessments in the coming months and propose mitigation actions