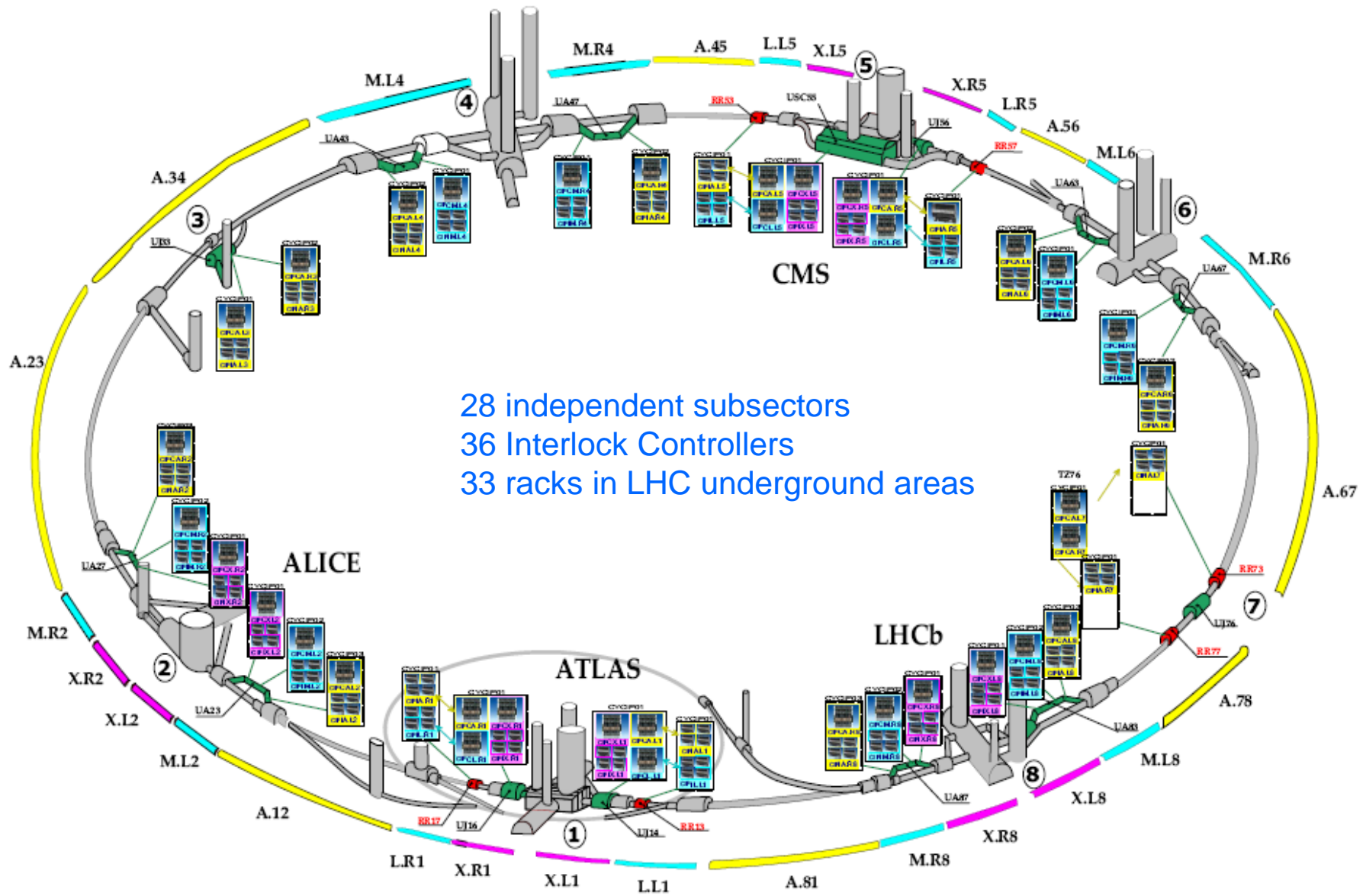# Secure configuration for the Powering Interlock Controller

J. Blanco   AB/CO/MI   29 January 2007

28 independent subsectors
36 Interlock Controllers
33 racks in LHC underground areas

Layout

PVSS
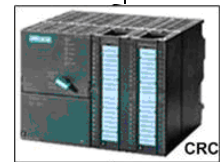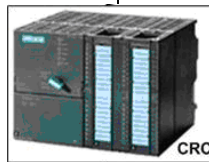
DB

Startup & Monitoring

Layout DB
Configuration DB
CVS

Ethernet

PLC

PLC

PLC

Circuit Protection
BIC Interface

PROFIBUS

PROFIBUS

. . .

PROFIBUS

matrix

matrix

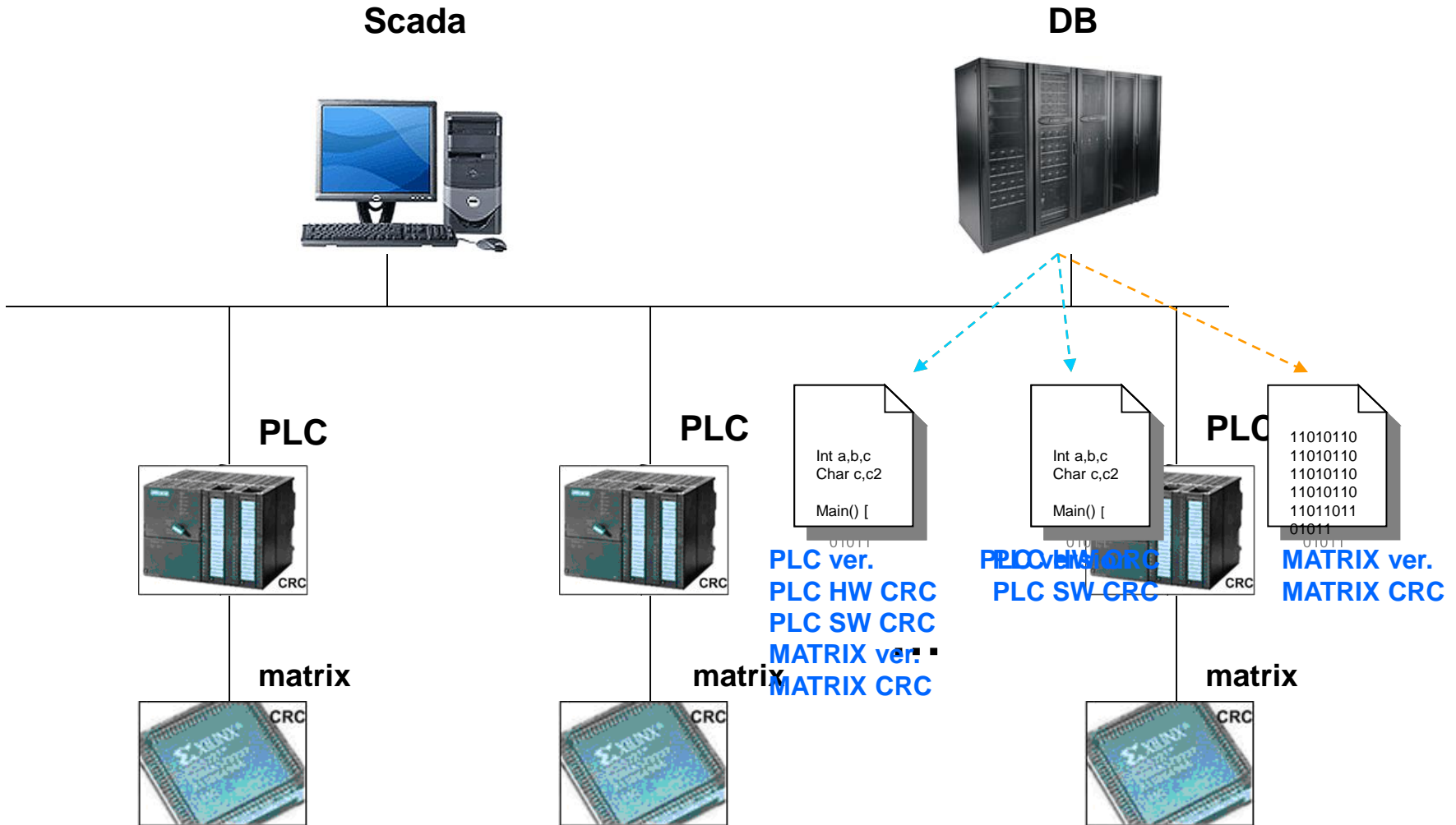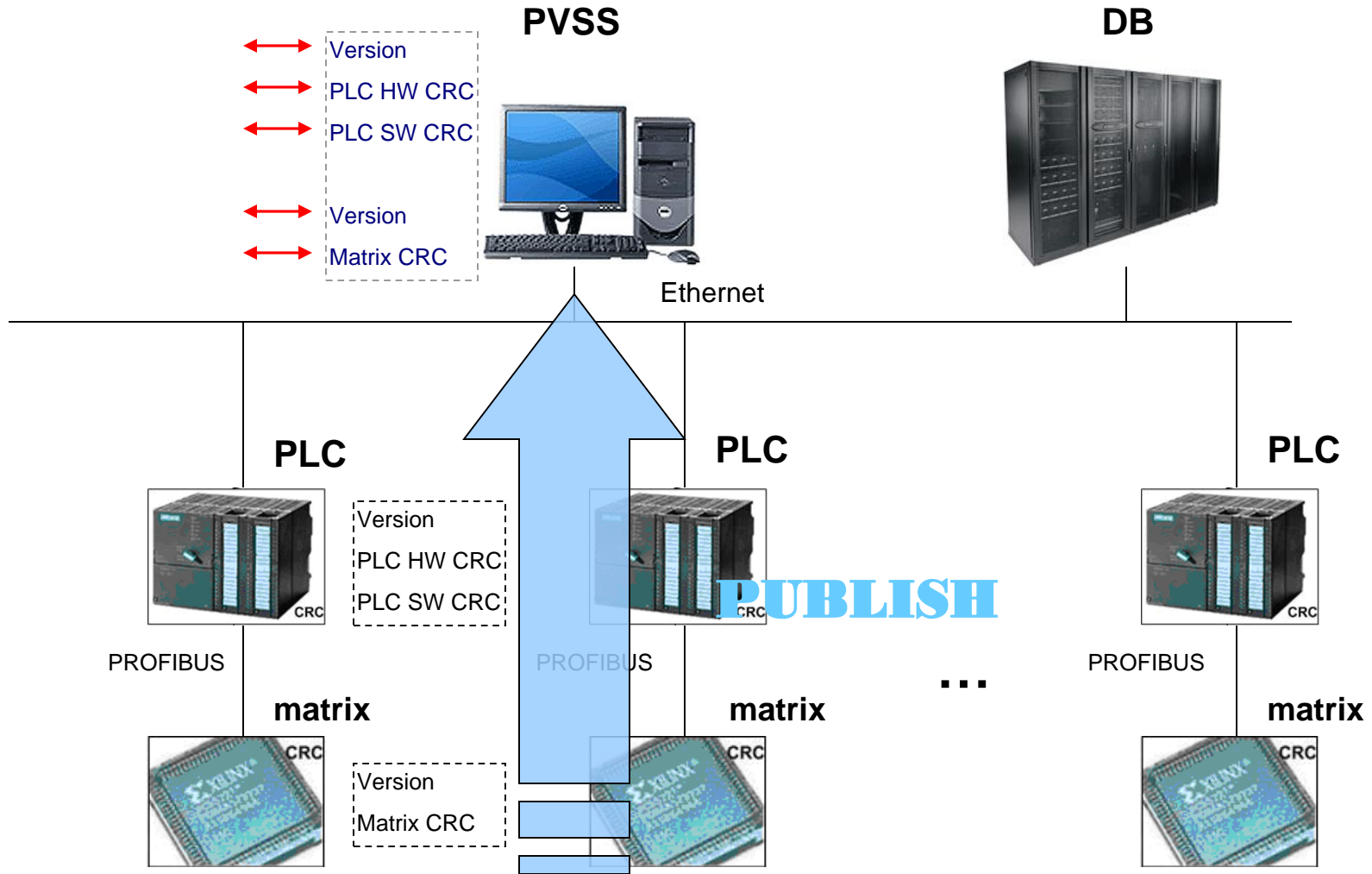**matrix**

Redundant, fast
BIC Interface

Aims

- **Help operations & experts to**
  - Avoid inversion of configuration data between PLC's
  - Assure version integrity between all the software components (PLC, PVSS, Matrix)
  - Assure integrity of configuration data between all the system components (PLC, PVSS, Matrix)
  - Assure the trust of the files downloaded from the DB server
  - Safely change operational parameters without changing hardware configuration

- **Does not protect against**
  - Manual post-editing of configuration data

Implementation

Scada

DB

PLC

PLC

PLC

```
Int a,b,c
Char c,c2

Main() [
01011
```

```
Int a,b,c
Char c,c2

Main() [
01011
```

```
11010110
11010110
11010110
11010110
11011011
01011
```

PLC ver.
PLC HW CRC
PLC SW CRC
MATRIX ver.
MATRIX CRC

PLC ver.
PLC SW CRC

PLC HW CRC

MATRIX ver.
MATRIX CRC

matrix

matrix

matrix

Supervision application config file

- The PVSS application is responsible for the consistency of all the configuration data as well as the coherency of the program versions for the CPLD-PLC-PVSS

- It contain

  - Version number of the config file.

  - The CRC's for the PLC and CPLD

  - The versions of the PLC and CPLD code.

- The overall coherency will depend on the correctness of the PVSS configuration file.

Verification process

PVSS

DB

Version
PLC HW CRC
PLC SW CRC

Version
Matrix CRC

Ethernet

PLC

Version
PLC HW CRC
PLC SW CRC

PROFIBUS

matrix

Version
Matrix CRC

PLC

PUBLISH

PROFIBUS

matrix

...

PLC

PROFIBUS

matrix

Actions

- Enable/Disable 'Give Permit' command at PVSS level.

Checking Parameters

- Every time a Faceplate of a PIC is opened in the SCADA systems all 5 parameters are verified.

- Before a '*give permit"* command is sent, the 3 PLC related parameters (HW CRC, SW CRC, Version) are checked. The 2 CPLD parameters (CRC, Version) are verified only if the last verification is older than a maximum of 1 hour.

- Every time a '*give permit all"* is sent all the parameters are verified.

CVS repository

- After download from database, all configuration data will be archived in CVS
- Validation during hardware commissioning

CERN — European Organization for Nuclear Research

Click on a directory to enter that dire

Current directory: [pico - PIC Confi

File
Parent Directory
CIP.TZ76.AL7/
CIP.TZ76.AR7/
CIP.UA23.AL2/
CIP.UA23.ML2/
CIP.UA23.XL2/
CIP.UA27.AR2/
CIP.UA27.MR2/
CIP.UA27.XR2/
CIP.UA43.AL4/
CIP.UA43.ML4/
CIP.UA47.AR4/
CIP.UA47.MR4/
CIP.UA63.AL6/
CIP.UA63.ML6/

CERN — European Organization for Nuclear Research

CIP_Config_Data/CIP.UA83.XL8/

Click on a directory to enter that directory. Click on a file to display its revision history and to get a chance to display diffs between revisions.

Current directory: [pico - PIC Configuration Files] / CIP_Config_Data / CIP.UA83.XL8

File	Rev.	Age	Author	Last log entry
Parent Directory				
PIC_UA83_XL8.zip	1.1	7 weeks	jblancos	PLC program Version 1.7 PLC config Version: 2.0 Remarks: Cryo Comm PLC-PLC spec...
PIC_UA83_XL8_No_PSoff.zip	1.1	7 weeks	jblancos	PLC program Version 1.7 PLC config Version: 2.0 Remarks: Cryo Comm PLC-PLC spec...
matrixcode_CIP_UA83_XL8.jed	1.1	8 weeks	jmarieth	Add of the matrix compiled code
matrixmask_CIP_UA83_XL8.txt	1.1	2 months	jmarieth	*** empty log message ***
plcD_CIP_UA83_XL8.txt	1.2	2 months	jmarieth	New version number for PLC_SW (2.0) and CPLD (15) New URL for [html page]
plc_CIP_UA83_XL8.txt	1.2	2 months	jmarieth	New version number for PLC_SW (2.0) and CPLD (15) New URL for [html page]
pvss_CIP_UA83_XL8.txt	1.4	5 weeks	jmarieth	New header field containing the list of PC connected to the PIC

Show only files with tag: All tags / default branch ▼ Module path or alias: CIP_Config_Data/0 Go

- Adding equipment or electrical circuits
  - Probability very low.
  - Imply changes in the PC, QPS and PIC.
  - Imply changes in the Hardware part of the config data → re-commissioning must be done.
- Removing equipment or electrical circuits defined as Auxiliary (corrector circuits)
  - High probability.
  - PC powering that circuit should be switched off and the interlock cable should be disconnected.
  - No config file modifications needed.
- Removing equipment or electrical circuits defined as Essential (main circuits)
  - Low probability.
  - Should be redefined as auxiliary → SW part of PLC config file needs to be modified as well as the MATRIX mask.

- **Change the 'POWERING SUBSECTOR OFF' flag**
  - Low probability.
  - Update the Software part of the PLC config file.
  - Quick functional test of the modification from the CCC sufficient

- **Change the 'BEAM DUMP' FLAG**
  - Medium-low probability.
  - Update the Software part of the PLC config file.
  - Change the MATRIX mask of the CPLD.
  - Quick functional test of the modification from the CCC sufficient

Conclusions

- ES summarizing the design issues finalized and will soon be distributed for engineering check

- Similar ideas implemented for PLC systems as MCS for VME front-ends to
  - Later integration into MCS?

- Assist operations with configuration management and changes of operational parameters

- Bernard, Frederic.   (AB/CO)

- Harrison, Robert.   (AB/CO)

- Zerlauth, Markus.   (AB/CO)