Securing TANGO Control System: A brainstorming

Sergi Blanch i Torné

Cryptography & Graphs
Math Department
Universitat de Lleida

September 24th, 2013

Outline

What is an Industrial Control System? (ICS)

Wikipedia's definition (en)

"It is a general term that encompasses several types of control systems used in industrial production, including *supervisory control and data acquisition* (SCADA) systems, *distributed control systems* (DCS), and other smaller control system configurations such as *programmable logic controllers* (PLC) often found in the industrial sectors and critical infrastructures."

What is an Industrial Control System? (ICS)

Wikipedia's definition (en)

"It is a general term that encompasses several types of control systems used in industrial production, including *supervisory control and data acquisition* (SCADA) systems, *distributed control systems* (DCS), and other smaller control system configurations such as *programmable logic controllers* (PLC) often found in the industrial sectors and critical infrastructures."

What is an Industrial Control System? (ICS)

Wikipedia's definition (en)

"It is a general term that encompasses several types of control systems used in industrial production, including *supervisory control and data acquisition* (SCADA) systems, *distributed control systems* (DCS), and other smaller control system configurations such as *programmable logic controllers* (PLC) often found in the industrial sectors and critical infrastructures."

What is an Industrial Control System? (ICS)

Wikipedia's definition (en)

"It is a general term that encompasses several types of control systems used in industrial production, including *supervisory control and data acquisition* (SCADA) systems, *distributed control systems* (DCS), and other smaller control system configurations such as *programmable logic controllers* (PLC) often found in the industrial sectors and critical infrastructures."

What is a Programmable Logic Controllers?

Figure: Example of a PLC controlled system

What is a Programmable Logic Controllers?

This a production line like example!

Figure: Example of a PLC controlled system

What is an SCADA?

Wikipedia's definition (es)

"*Supervisory Control And Data Acquisition* it is a computer software to control and supervise industrial process remotely."

What is an SCADA?

Wikipedia's definition (es)

"*Supervisory Control And Data Acquisition* it is a computer software to control and supervise industrial process remotely."

Examples of an SCADAs

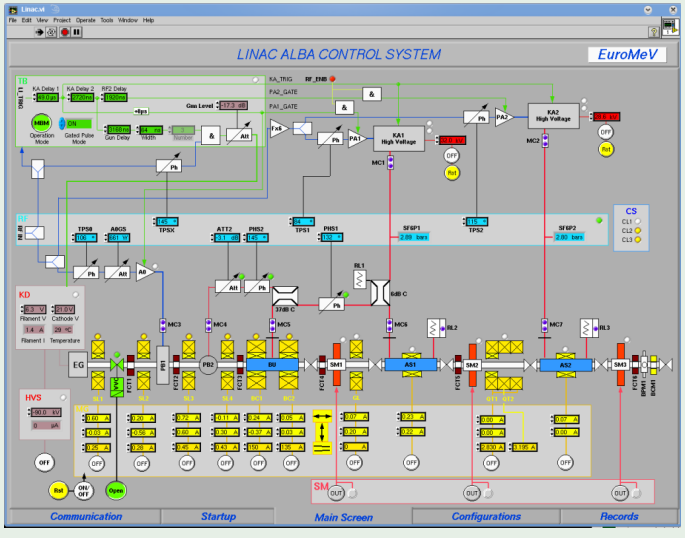


Figure: Labview as SCADA example

What is an Distributed Control System?

Wikipedia's definition (en)

a *Distributed Control System* is the computer software for a manufacturing system, process or any kind of dynamic system, in which the controller elements are not central in location (like the brain) but are distributed throughout the system with each component sub-system controlled by one or more controllers.

What is a distributed system?

Tanenbaum say [1]: *A distributed system is a collection of independent computers that appears to its users as a single coherent system.*

What is a TANGO? (I)

TANGOis an object oriented *Distributed Control System* with active collaborative development from:

Figure: Logos of the Tango Consortium Members

Together with tools like SARDANA, TAURUS, ATK and MAMBO there is a big *Industrial Control System*
Them can act as an SCADA and/or DCS flexibly to the needs.

What is a TANGO? (II)

It's an Distributed Control System

using CORBA as a Middleware (omniORB),
with ØMQ in the event broadcasting.

What means middleware?

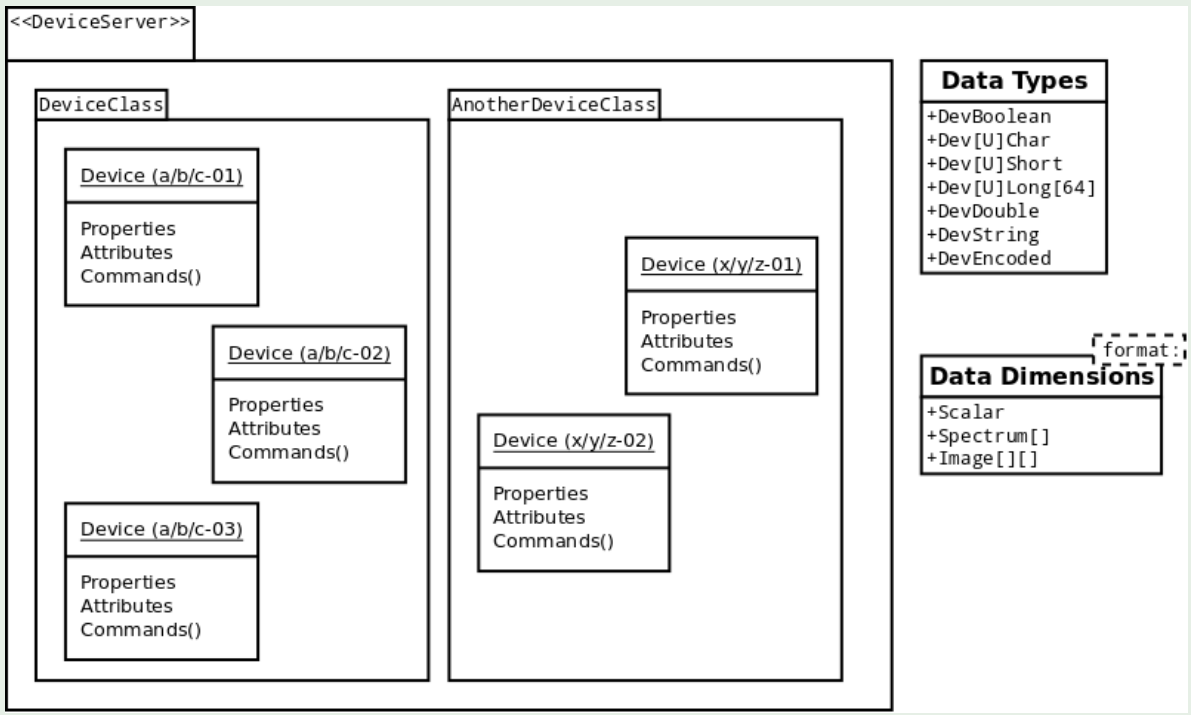
Tanenbaum say [1]: *It is what supports heterogeneous computers and networks while offering a single system view.*

What is a TANGO? (&III)

TANGO parts

- TANGO core ⇒ the Middleware
- TANGO Device Servers ⇒ the agents in the DCS

Device servers, device classes, and devices



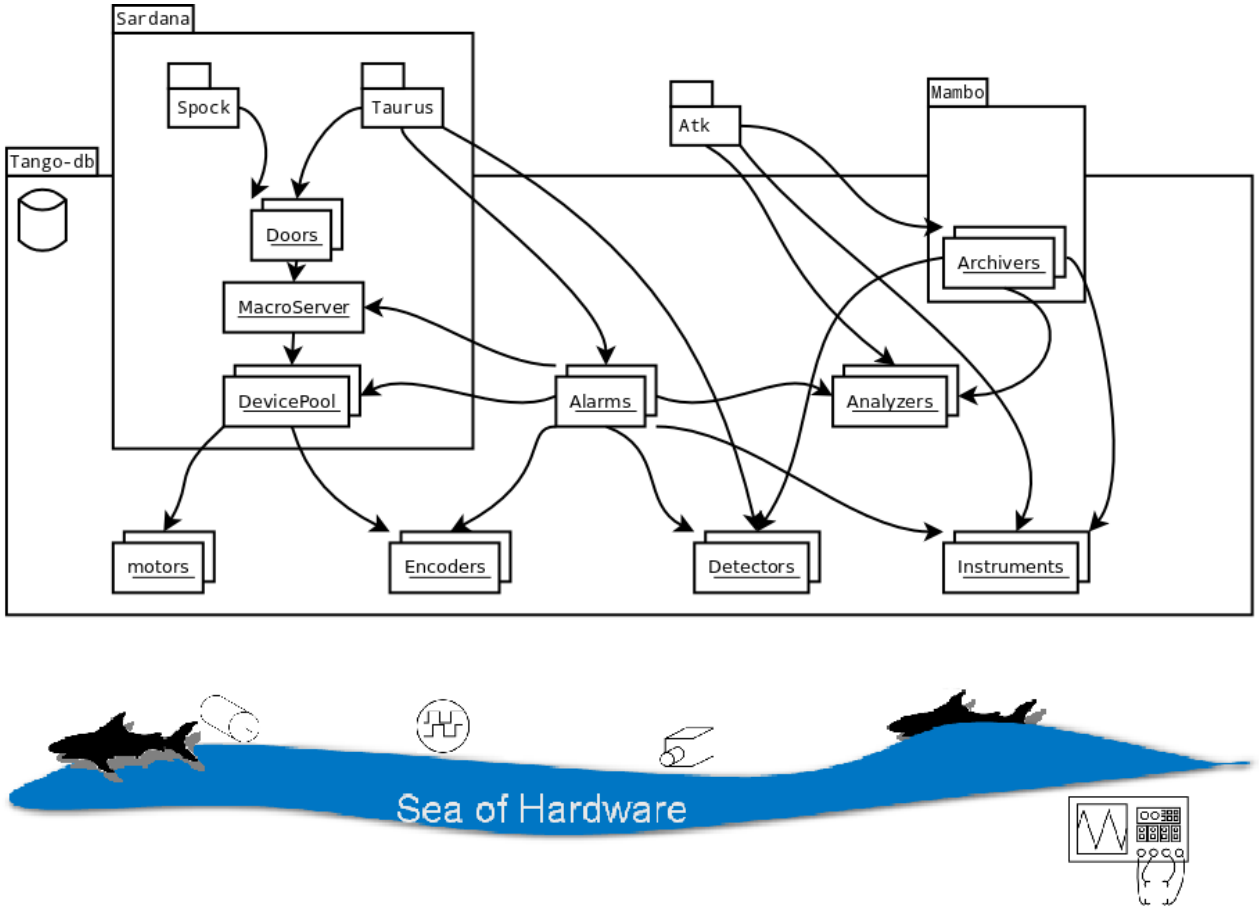
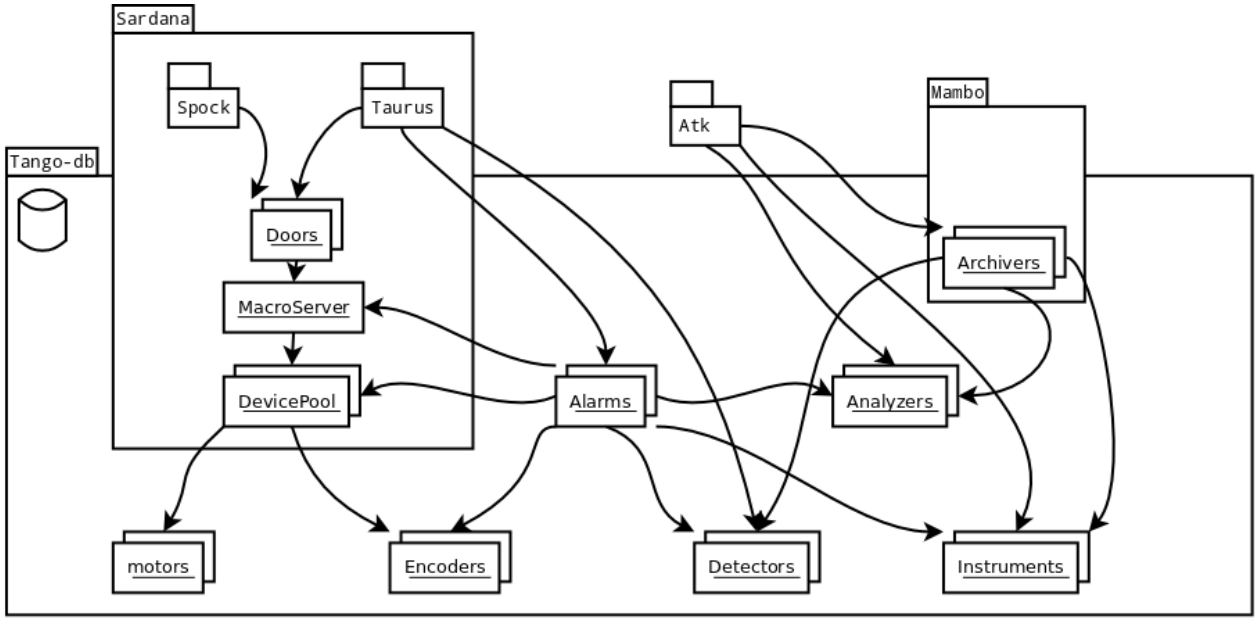


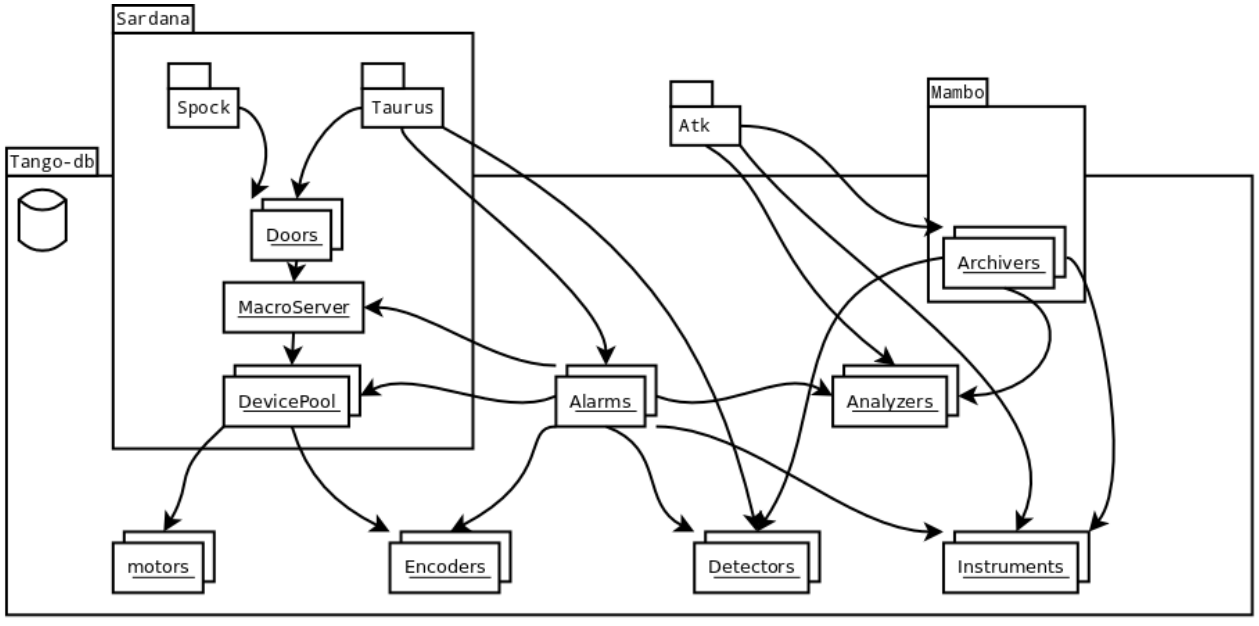
Figure: Tango schematic layout



Communication

- [a]synchronous ⇒ omniORB
- events ⇒ ∅MQ

ematic layout



Communication

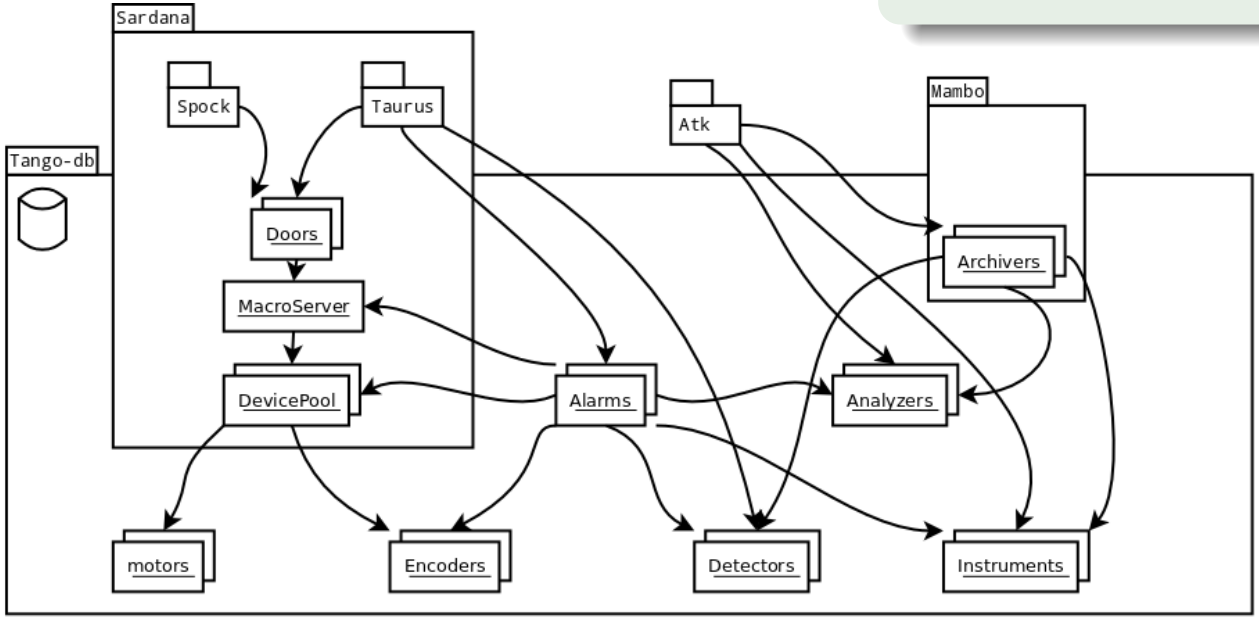
- [a]synchronous ⇒ omniORB
- events ⇒ ∅MQ

Persistent config data

- tango-ds ⇒ MySQL

Archiving

- MAMBO⇒ MYSQL



Communication

- [a]synchronous ⇒ OMNIORB
- events ⇒ ∅MQ

Persistent config data

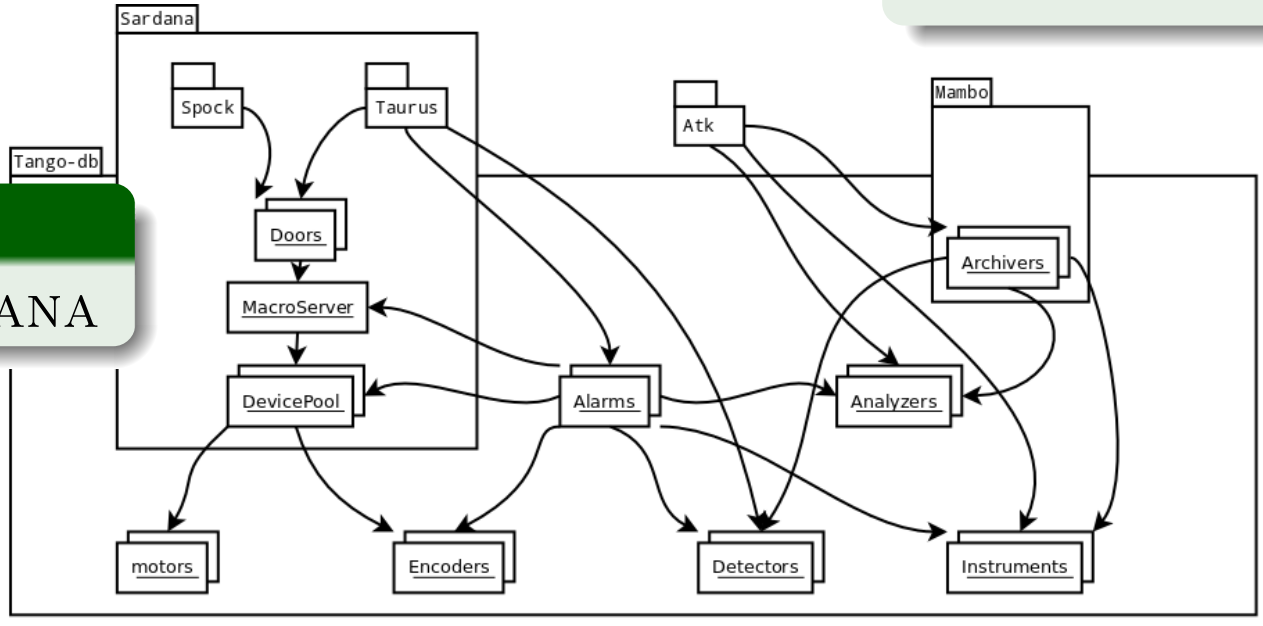
- tango-ds ⇒ MYSQL

Archiving

- MAMBO⇒ MYSQL

Framework

- SARDANA



Communication

- [a]synchronous ⇒ OMNIORB
- events ⇒ ∅MQ

Persistent config data

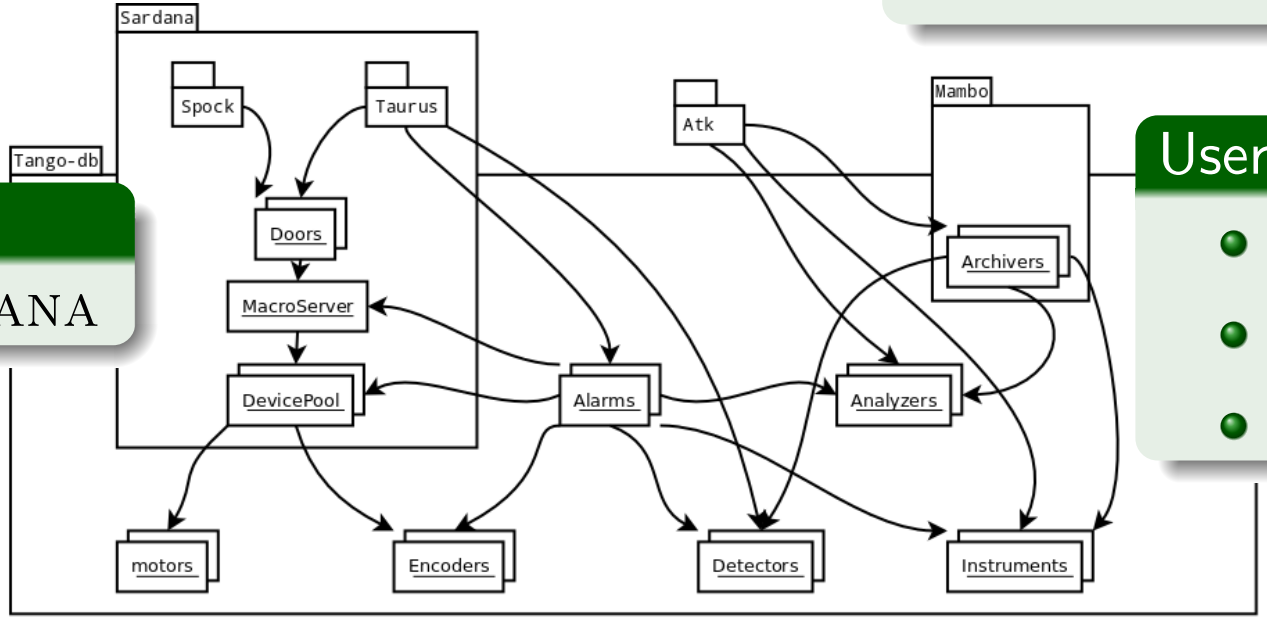
- tango-ds ⇒ MYSQL

Archiving

- MAMBO⇒ MYSQL

Framework

- SARDANA



User access

- TAURUS
- ATK
- SPOCK

Communication

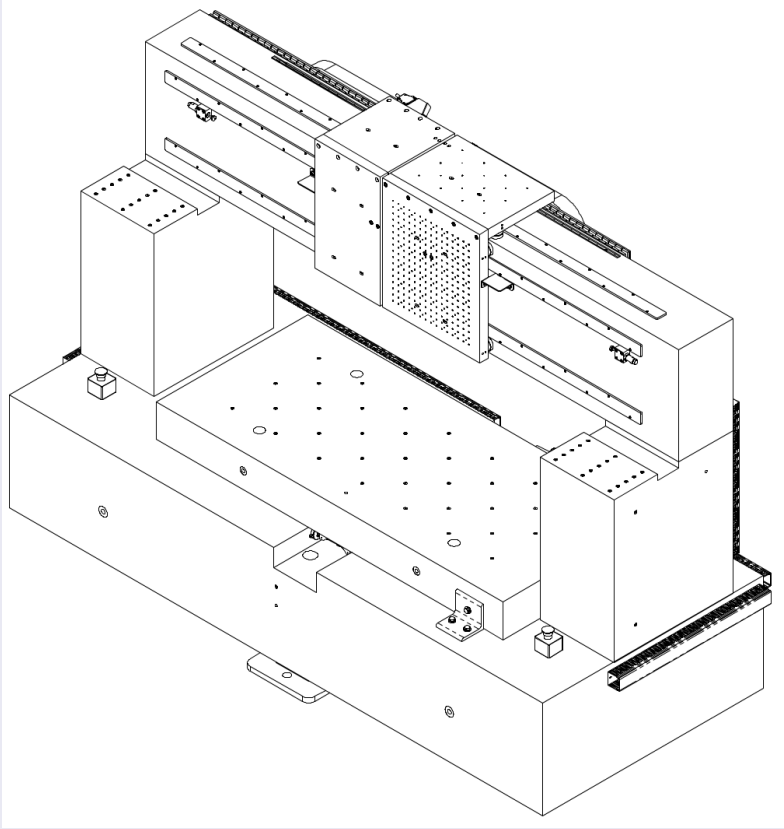
- [a]synchronous ⇒ OMNIORB
- events ⇒ ∅MQ

Persistent config data

- tango-ds ⇒ MYSQL

Optics Lab: Nanometer Optical Measuring

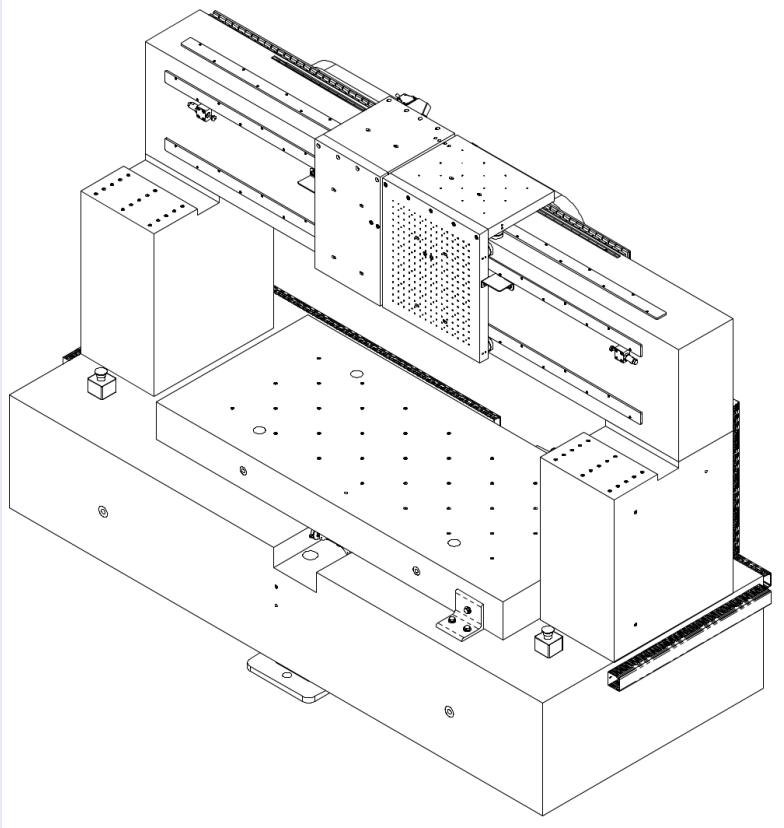
Drawing of the optics lab NOM-Long Term Profiler



Images provided by Dr.Josep Nicolas

Optics Lab: Nanometer Optical Measuring

Drawing of the optics lab NOM-Long Term Profiler

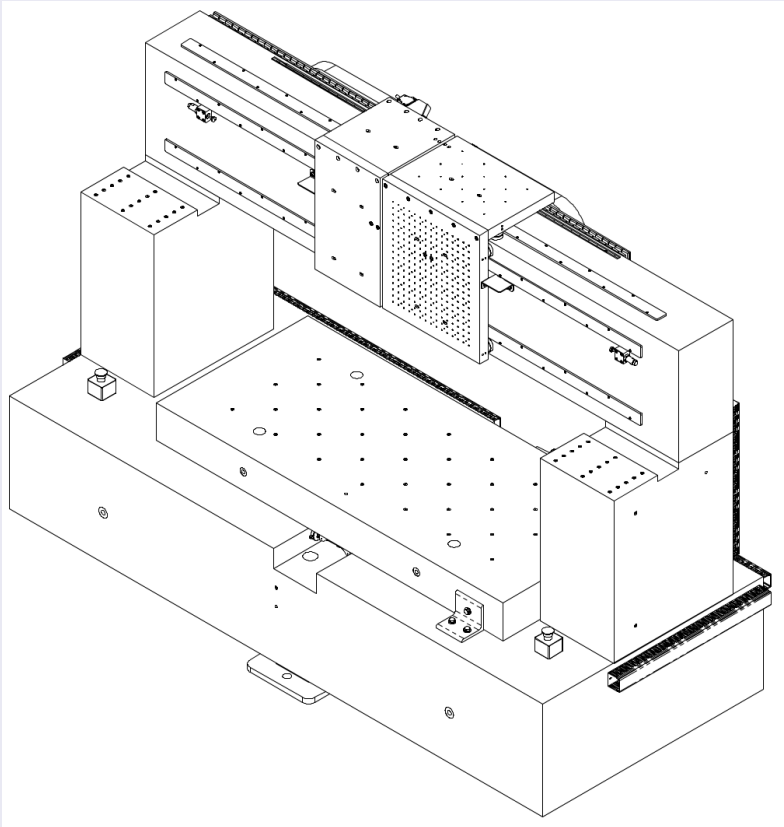


From the clean room

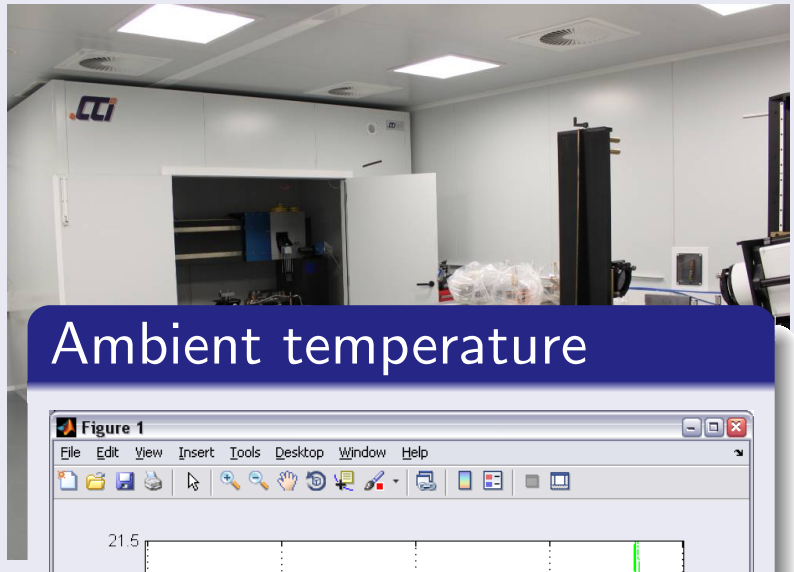
Images provided by Dr.Josep Nicolas

Optics Lab: Nanometer Optical Measuring

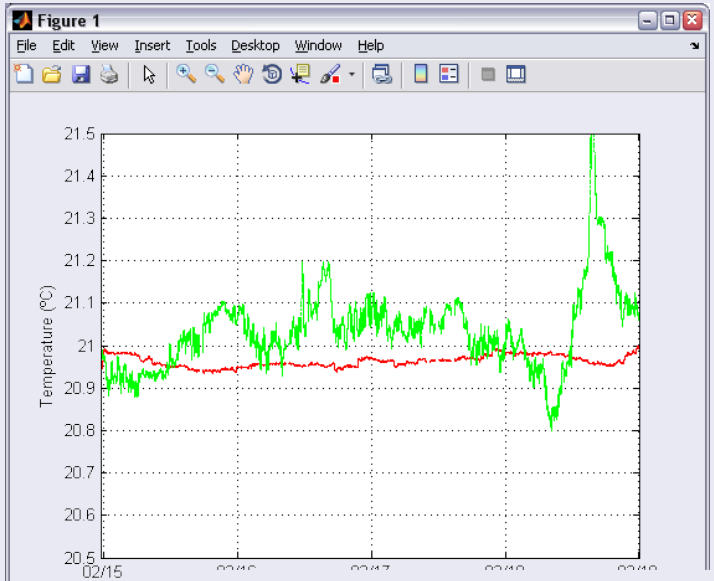
Drawing of the optics lab NOM-Long Term Profiler



From the clean room



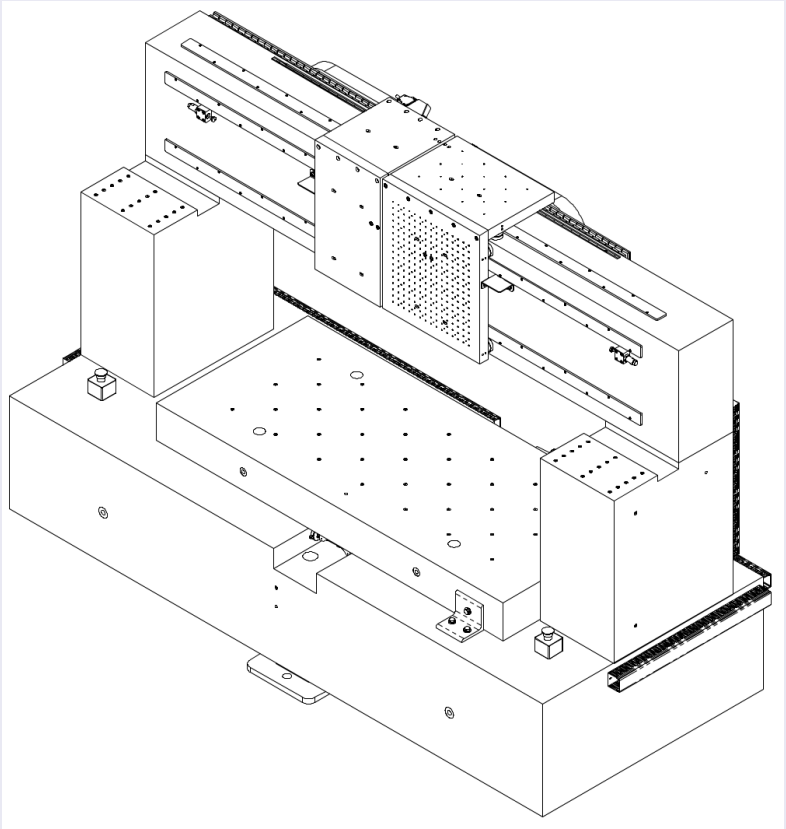
Ambient temperature



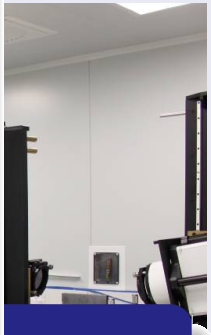
Images provided by Dr.Josep Nicolas

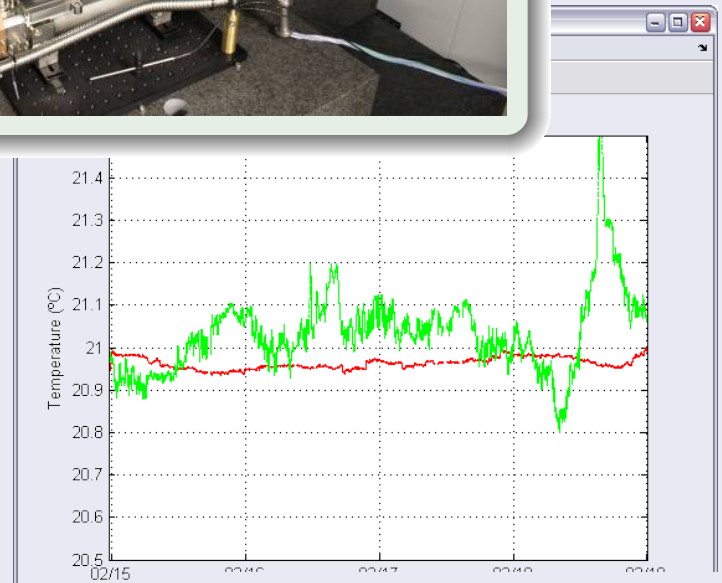
Optics Lab: Nanometer Optical Measuring

Drawing of the optics lab NOM-Long Term Profiler



Mirror position

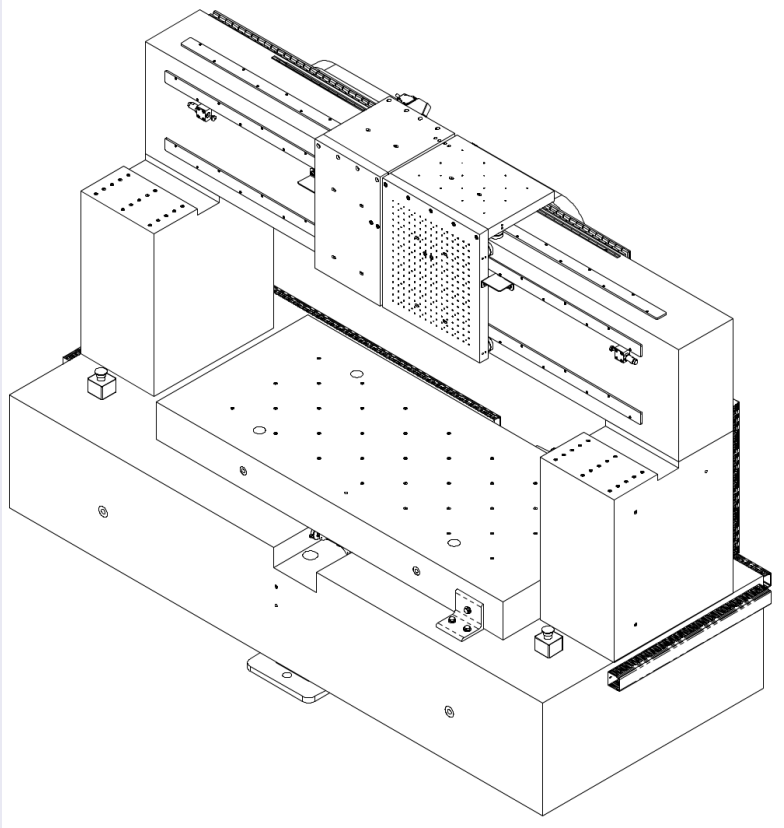




Images provided by Dr.Josep Nicolas

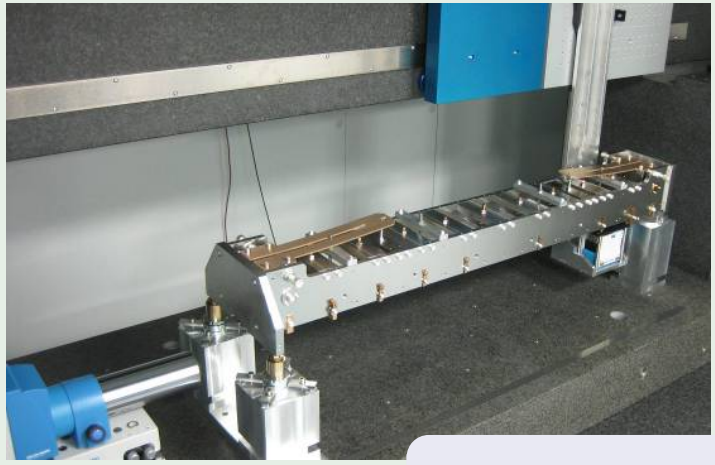
Optics Lab: Nanometer Optical Measuring

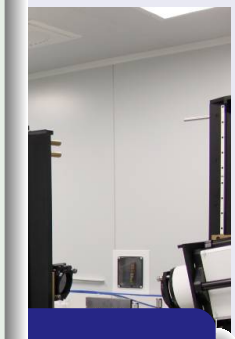
Drawing of the optics lab NOM-Long Term Profiler

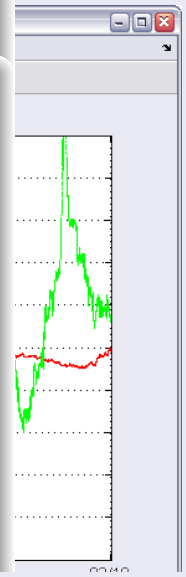


Mirror position

Inverted configuration





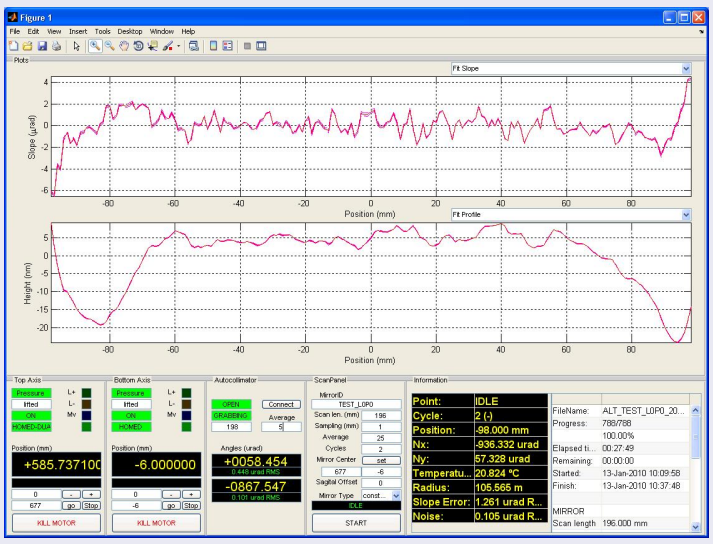


Images provided by Dr.Josep Nicolas

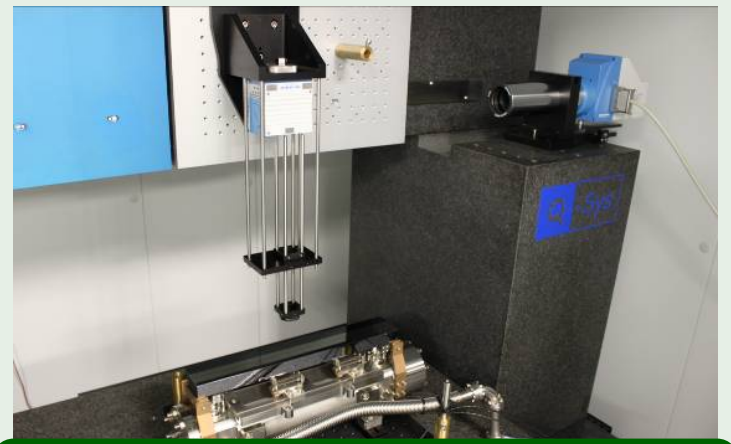
Optics Lab: Nanometer Optical Measuring

Drawing of the optics lab NOM-Long Term Profiler

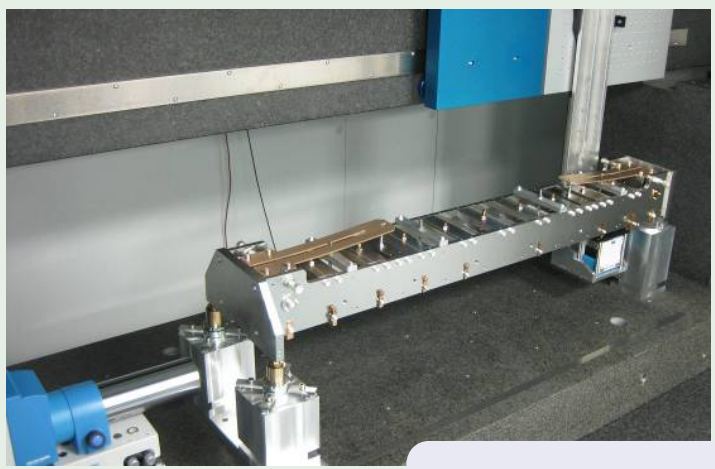
Matlab GUI

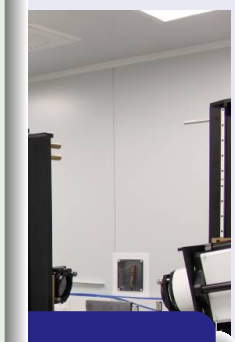


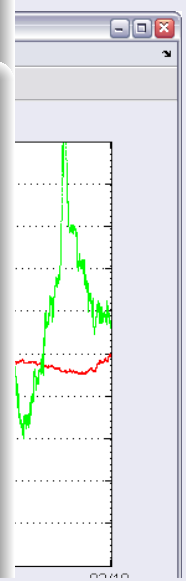
Mirror position



Inverted configuration





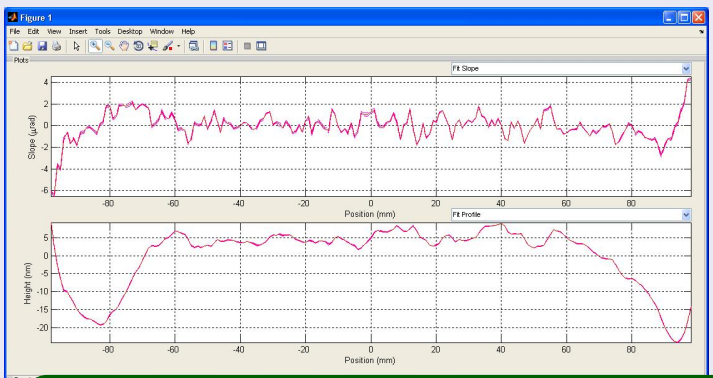


Images provided by Dr.Josep Nicolas

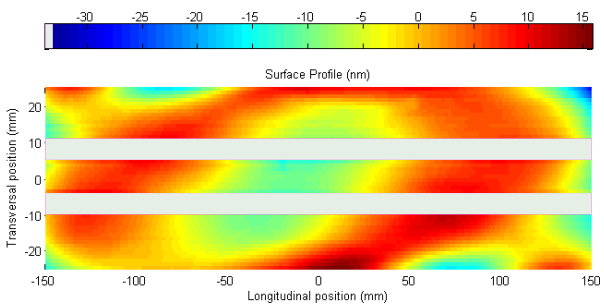
Optics Lab: Nanometer Optical Measuring

Drawing of the optics lab NOM-Long Term Profiler

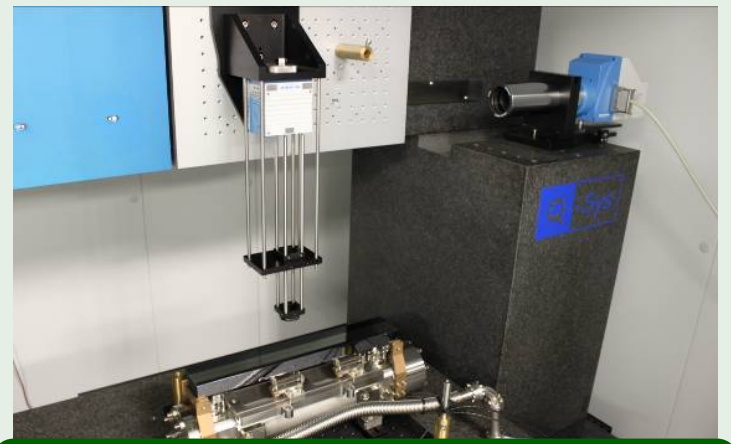
Matlab GUI



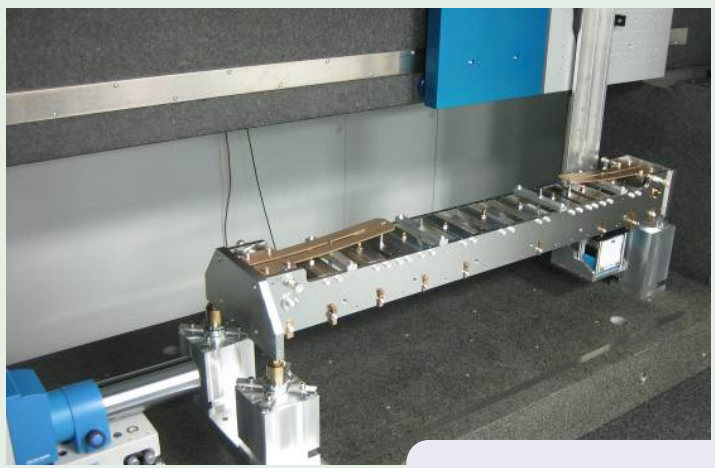
Surface example



Mirror position



Inverted configuration

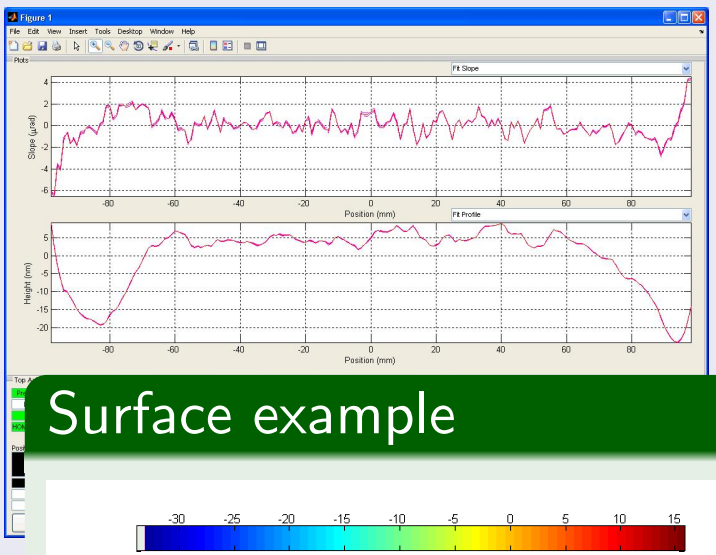


Images provided by Dr.Josep Nicolas

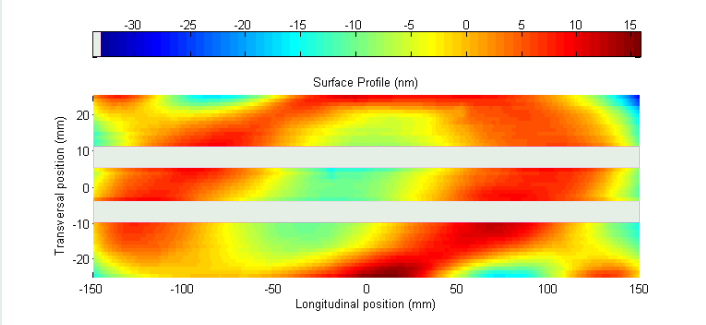
Optics Lab: Nanometer Optical Measuring

Drawing of the optics lab NOM-Long Term Profiler

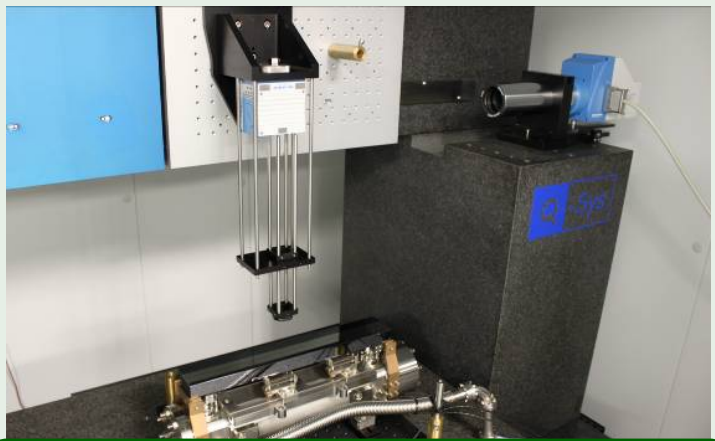
Matlab GUI



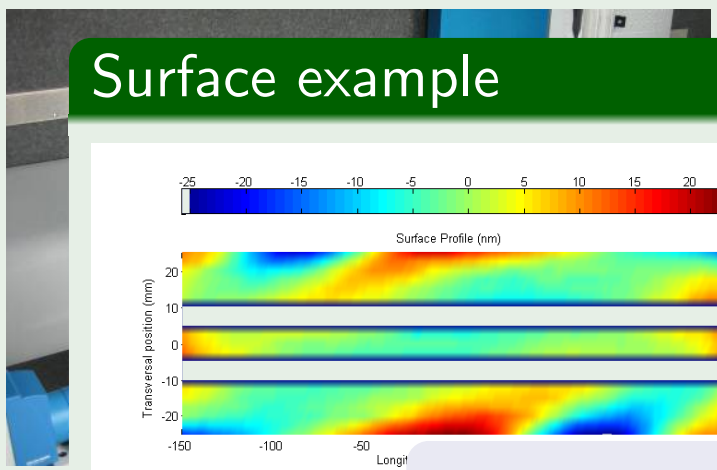
Surface example



Mirror position



Inverted configuration



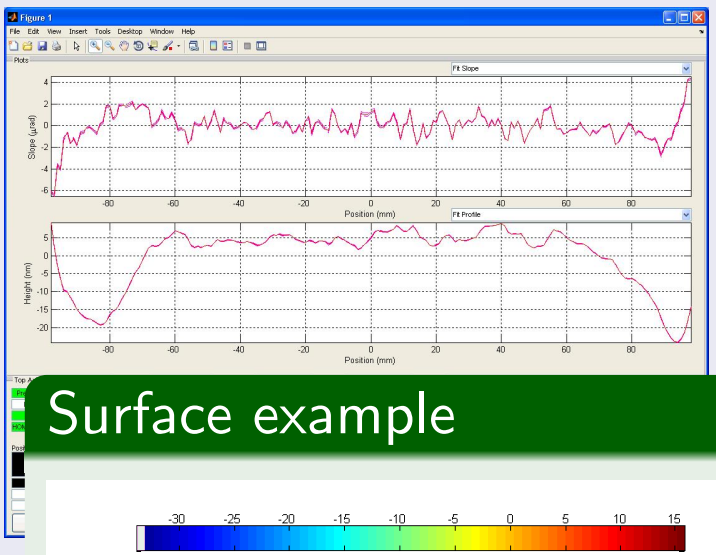
Surface example

Images provided by Dr.Josep Nicolas

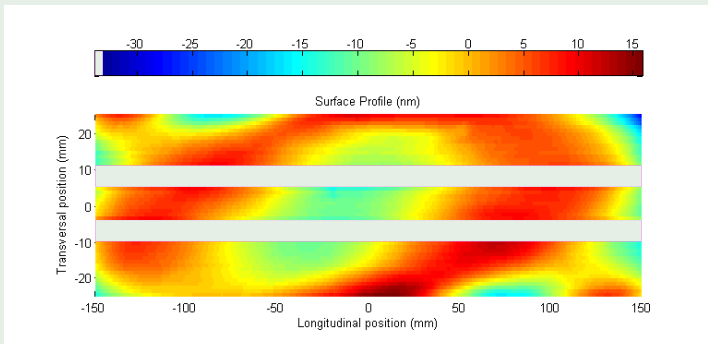
Optics Lab: Nanometer Optical Measuring

Drawing of the optics lab NOM-Long Term Profiler

Matlab GUI



Surface example

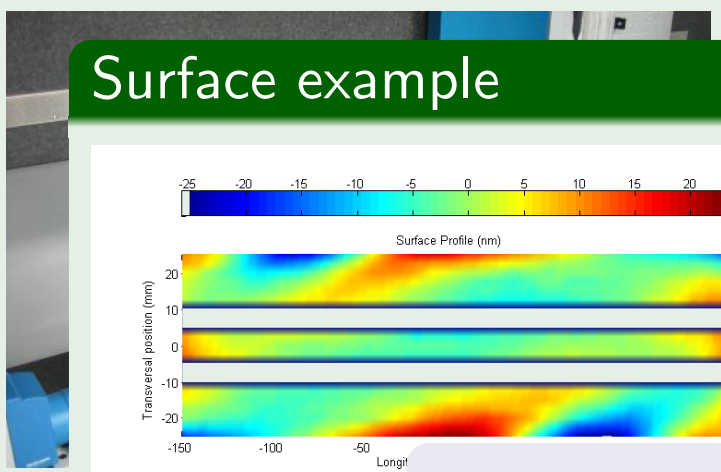


Mirror position

TANGOinformation

- 3 Hosts
- 28 Devices
- 12 DServers
- 19 DClasses

Inverted configuration

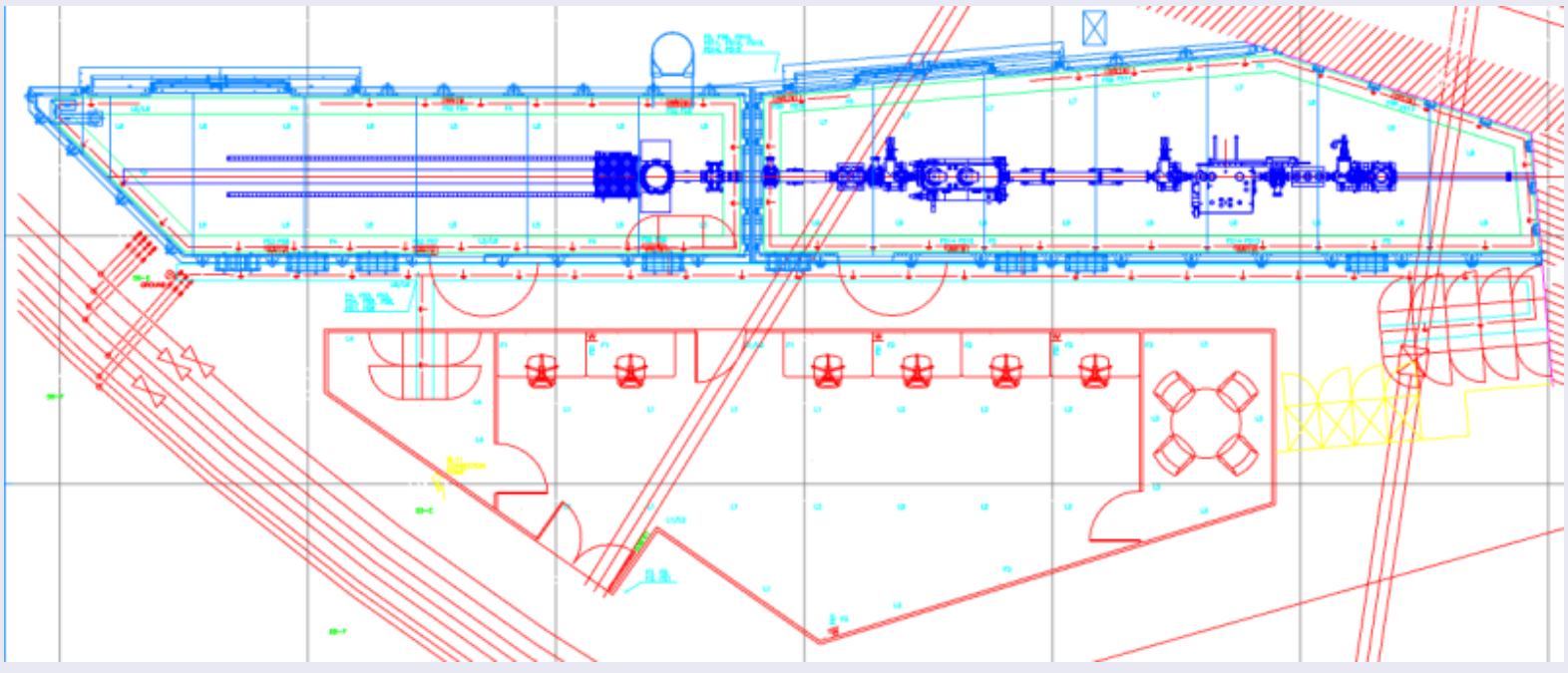


Surface example

Images provided by Dr.Josep Nicolas

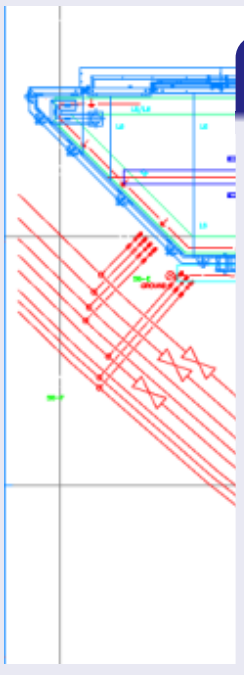
A beamline

layout of BL11

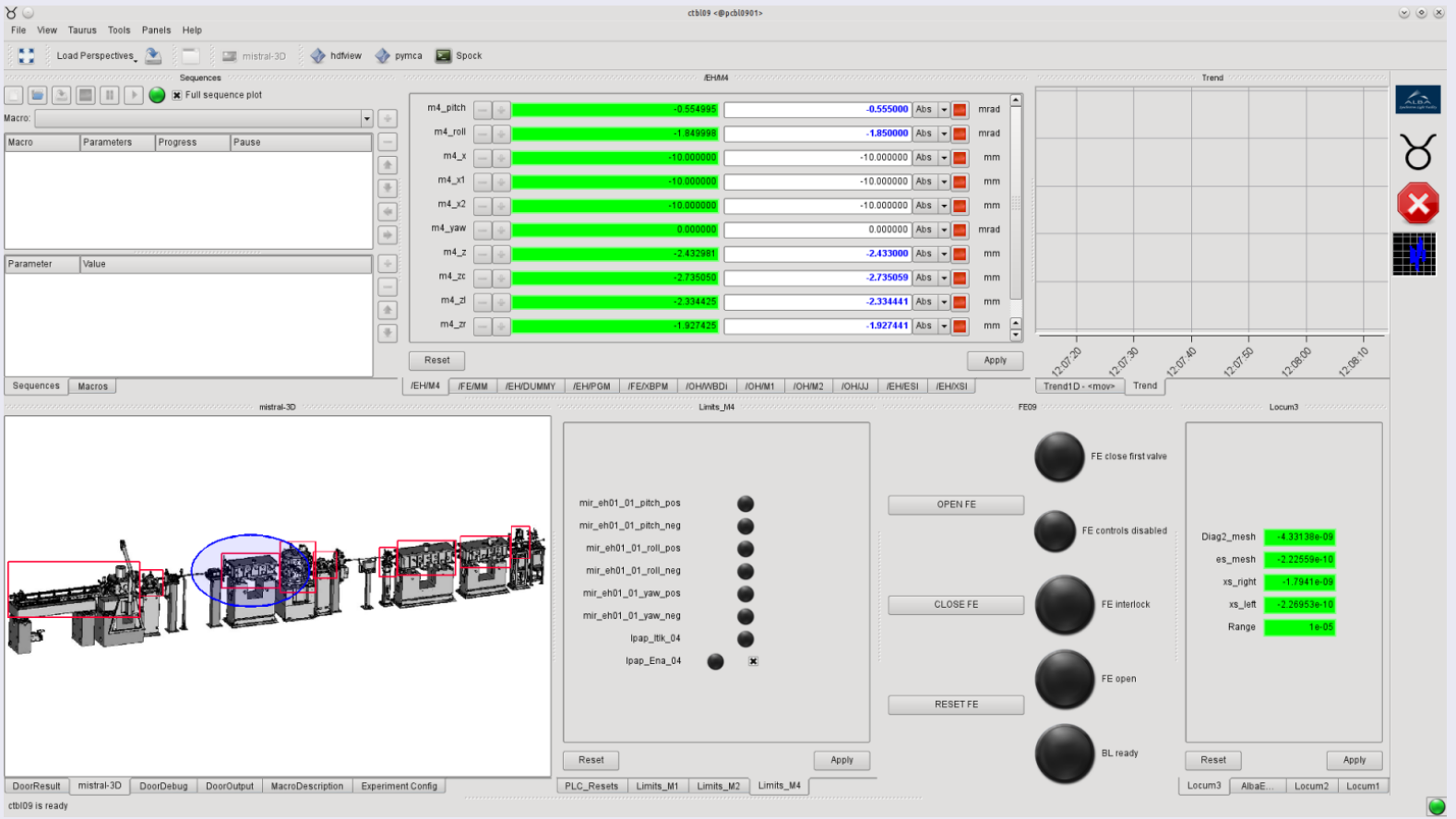


A beamline

layout of BL11

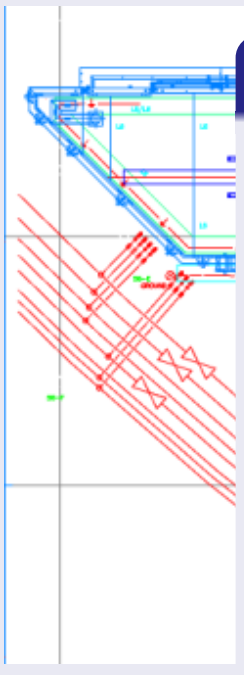


SARDANA's gui in BL09

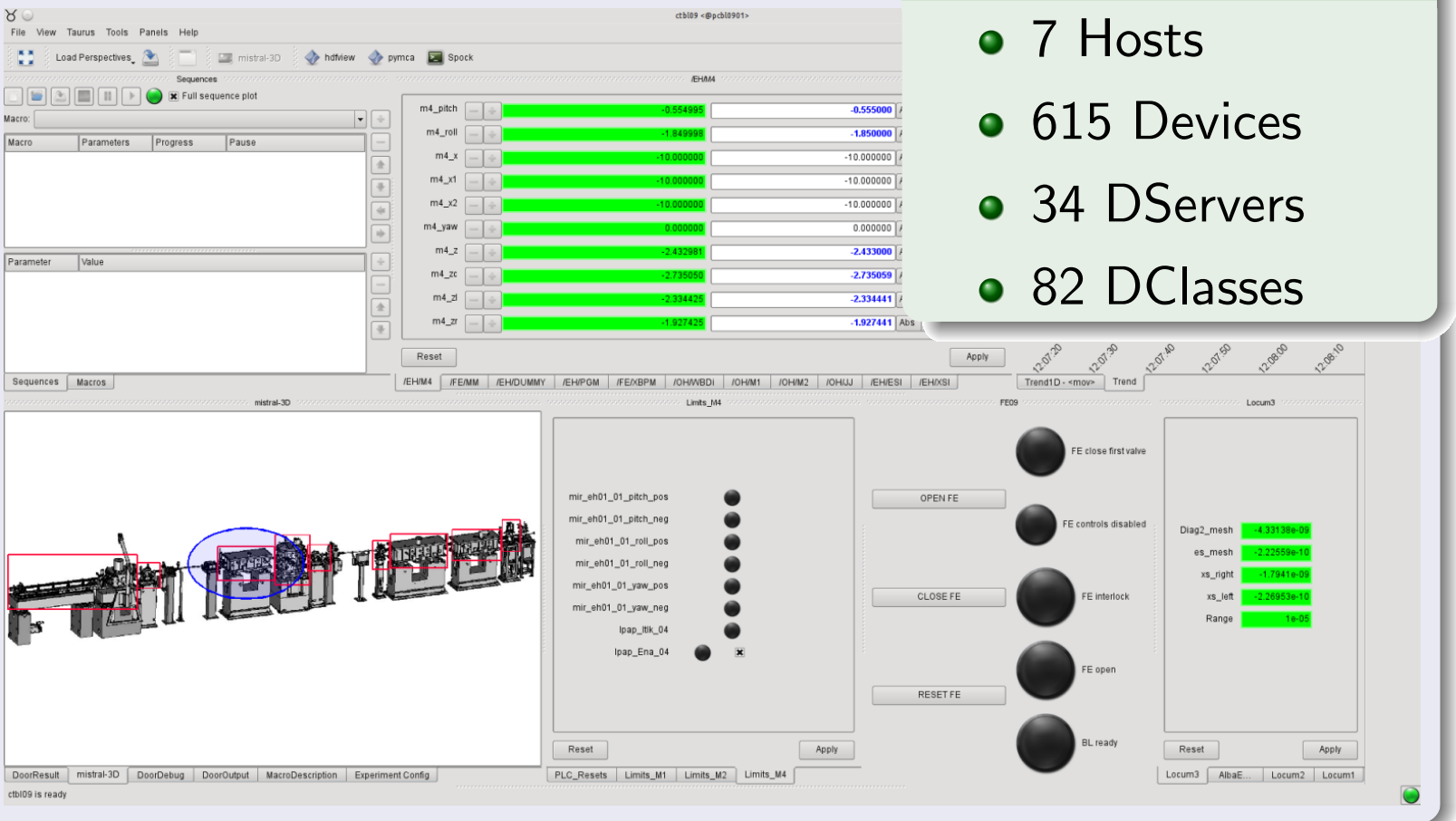


A beamline

layout of BL11



SARDANA's gui in BL09

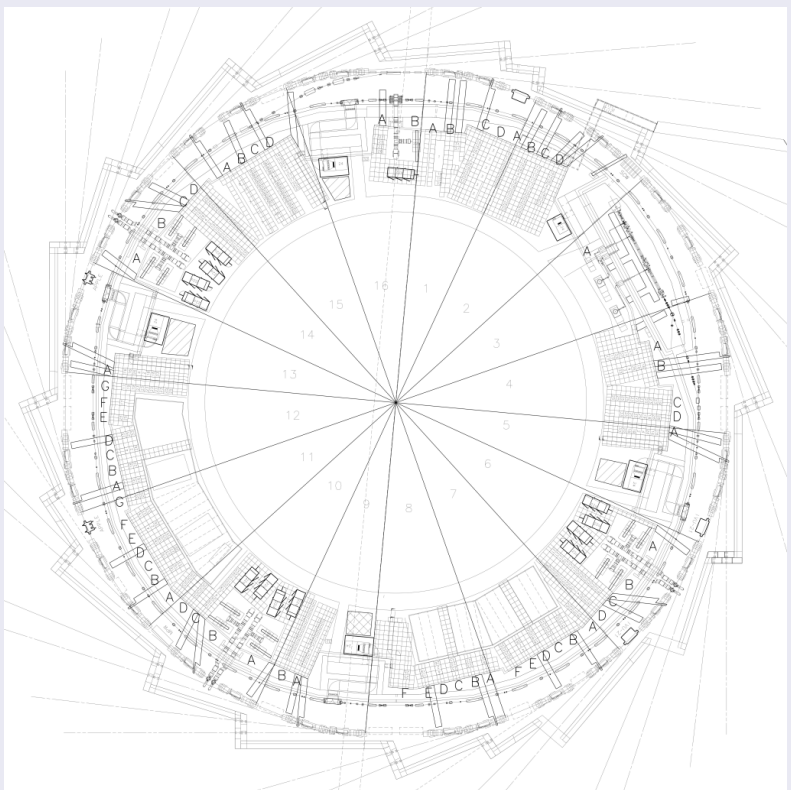


TANGOinformation (bl13)

- 7 Hosts
- 615 Devices
- 34 DServers
- 82 DClasses

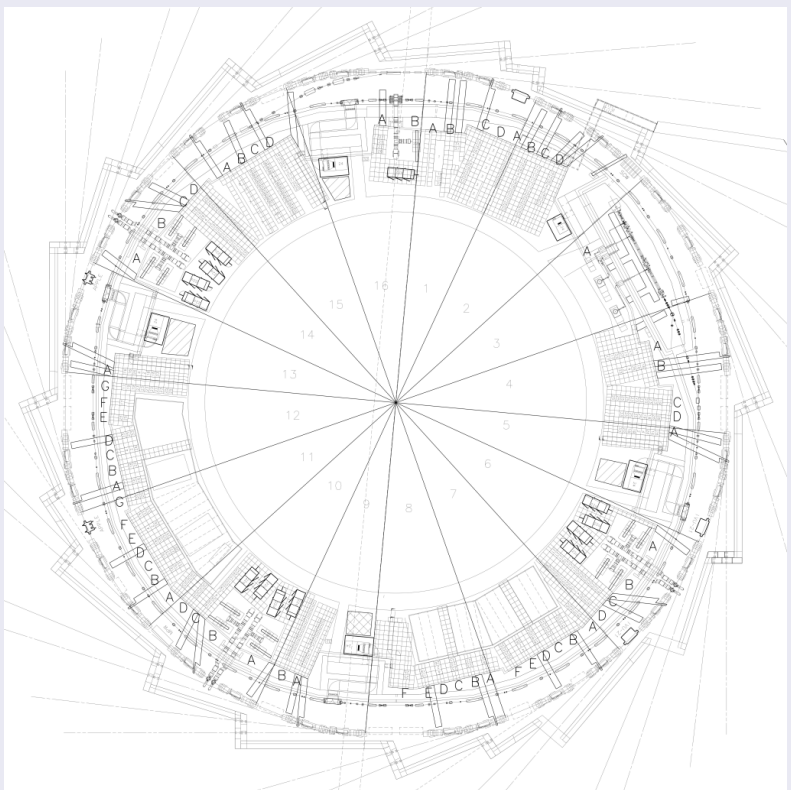
Control a synchrotron accelerator

Alba's overview

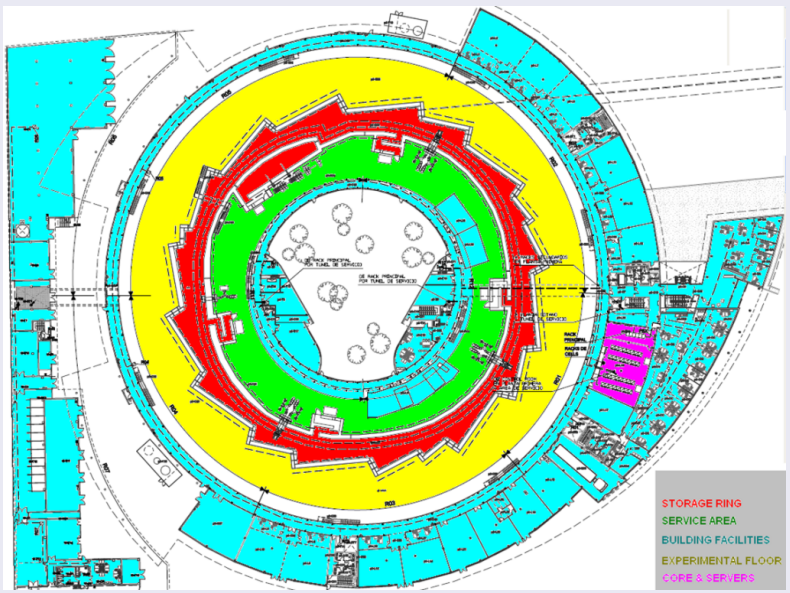


Control a synchrotron accelerator

Alba's overview

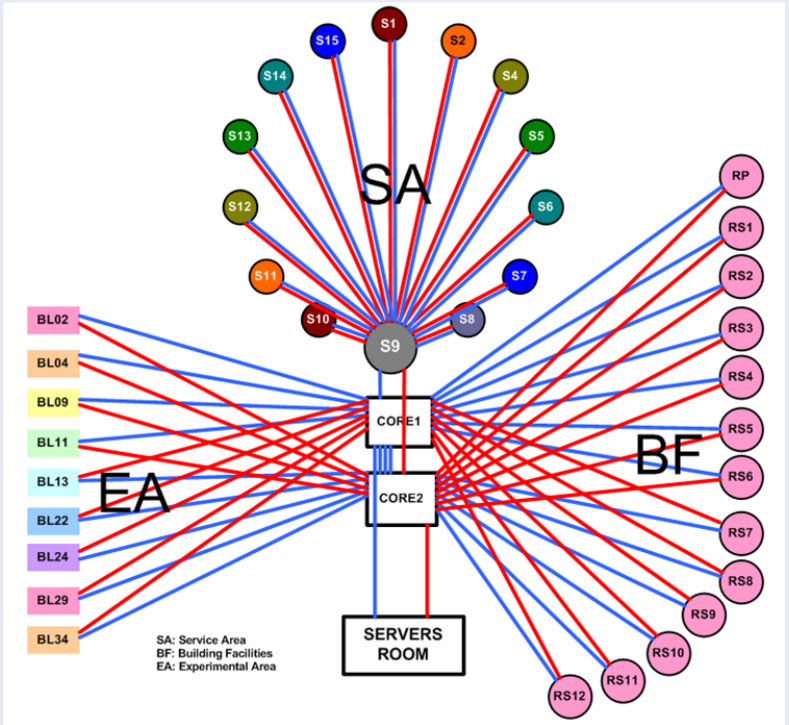


Alba's main network

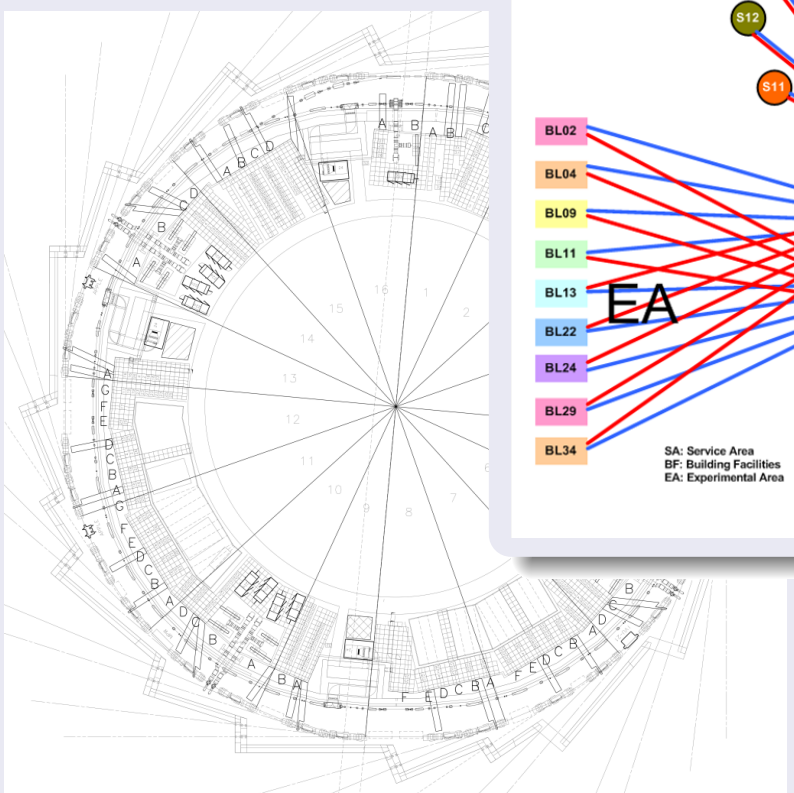


Control a synchrotron accelerator

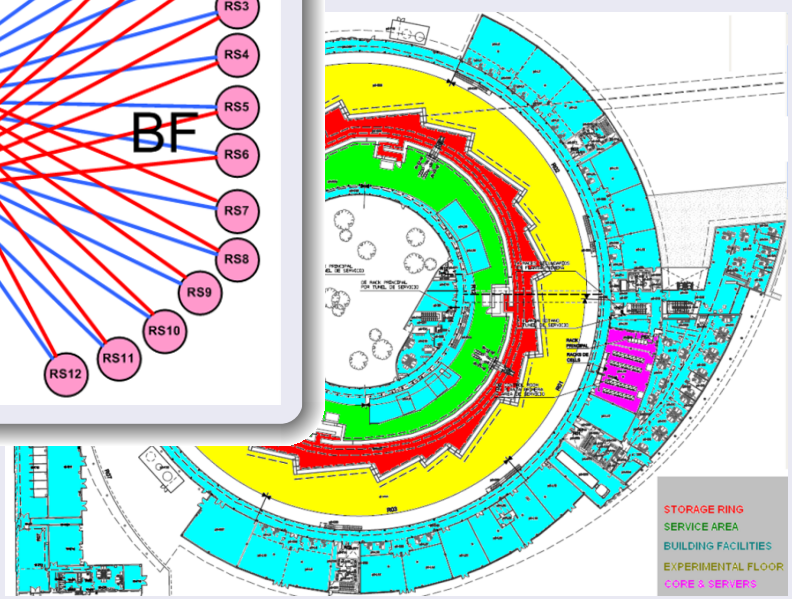
Alba's network layout



Alba's overview

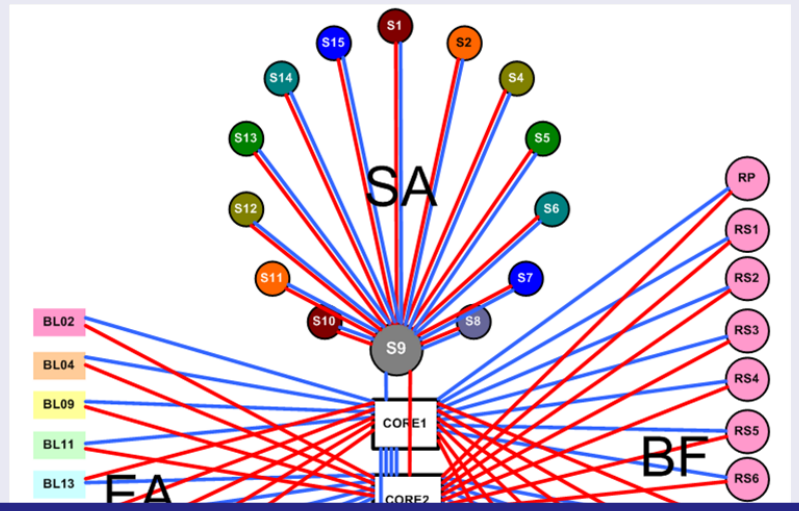


network



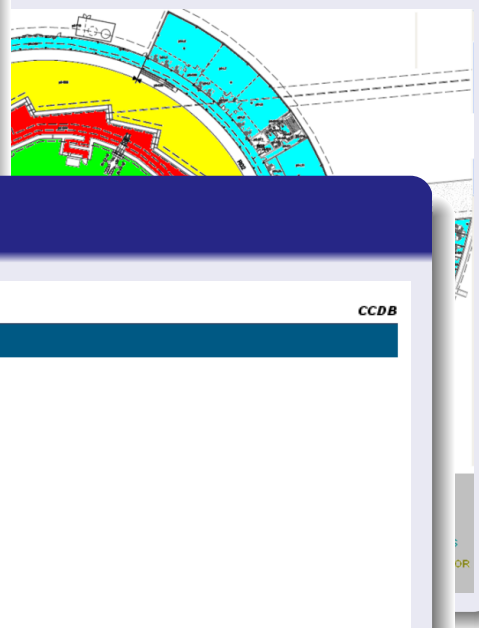
Control a synchrotron accelerator

Alba's network layout

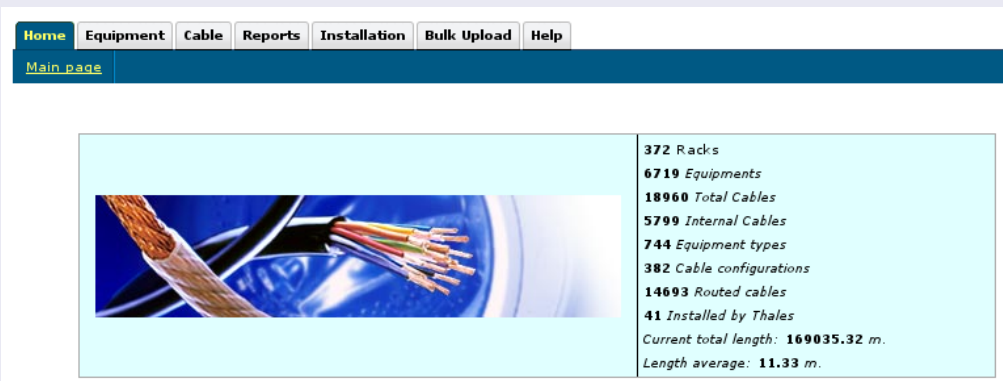


Alba's overview

network



Alba's Cabling Database

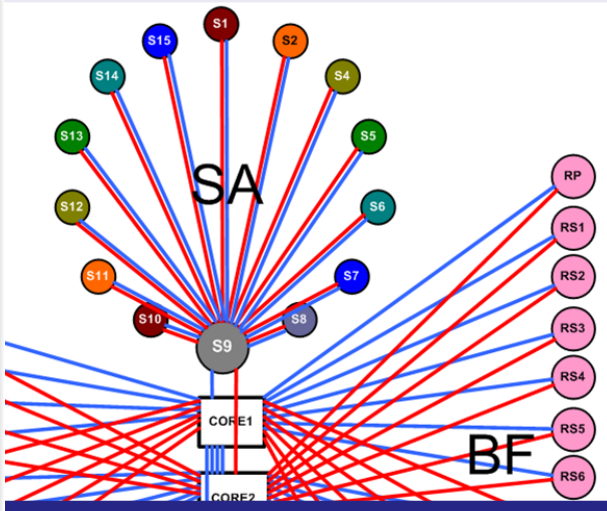


Control a synchrotron accelerator

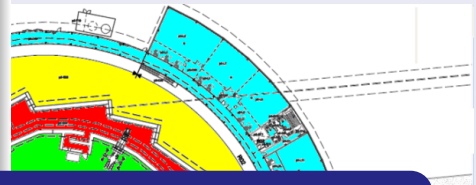
Alba's subsystems

- Timming
- Vaccum
- Power supplies
- Radio frequency
- Diagnostics
- EPS and PSS
- Fronted and IDs

Alba's network layout



network



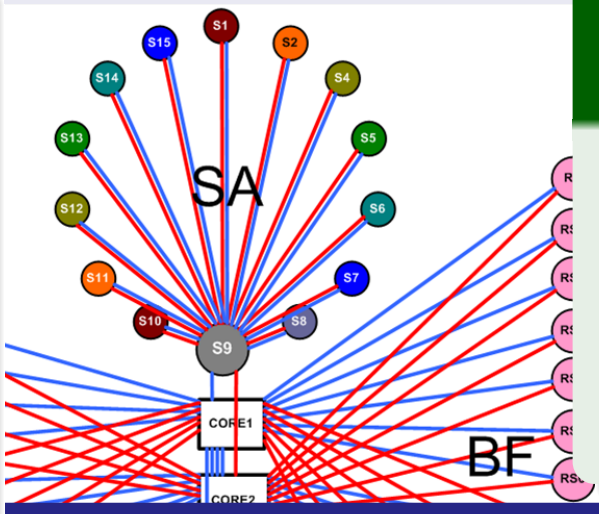
base

Control a synchrotron accelerator

Alba's subsystems

- Timming
- Vaccum
- Power supplies
- Radio frequency
- Diagnostics
- EPS and PSS
- Fronted and IDs

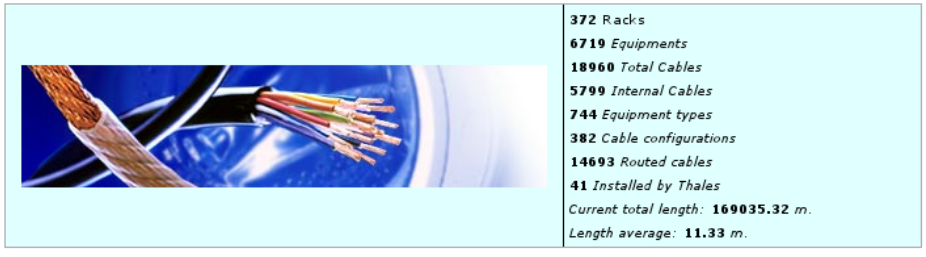
Alba's network layout



TANGOinformation (bl13)

- 139 Hosts
- 4259 Devices
- 85 DServers
- 1551 DClasses

base



Other possibilities

Images found in google, not license checked

Other possibilities

- Factory production lines

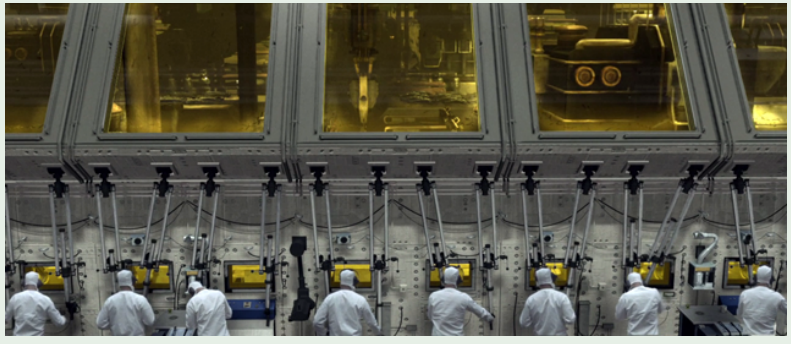
Production lines

Images found in google, not license checked

Other possibilities

- Factory production lines
- Critical factories

Production lines



Images found in google, not license checked

Other possibilities

- Factory production lines
- Critical factories
- Electronic traffic lights and tools

Images found in google, not license checked

Other possibilities

- Factory production lines
- Critical factories
- Electronic traffic lights and t

Electronic road panels

Images found in google, not license checked

Other possibilities

- Factory production lines
- Critical factories
- Electronic traffic lights and t

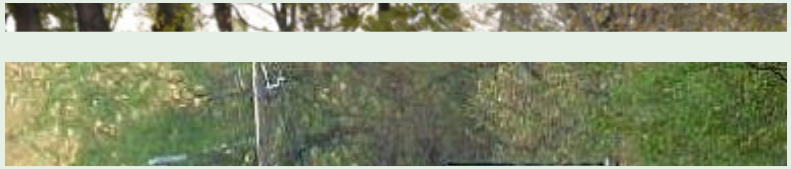
Electronic road panels

Images found in google, not license checked

Other possibilities

- Factory production lines
- Critical factories
- Electronic traffic lights and t

Electronic road panels



Images found in google, not license checked

Other possibilities

- Factory production lines
- Critical factories
- Electronic traffic lights and tools
- Energy industry

Images found in google, not license checked

Against the transparencies

Access	Hide differences in data representation and how a resource is accessed
Location	Hide where a resource is located
Migration	Hide that a resource may move to another location
Relocation	Hide that a resource may be moved to another location while in use
Replication	Hide that a resource is replicated
Concurrency	Hide that a resource may be shared by several competitive users
Failure	Hide a faulure and recovery of a resource
Persistence	Hide whether a (software) resource is in memory or on disk

Against the transparencies

Access	Hide differences in data representation and how a resource is accessed
Location	Hide where a resource is located
Migration	Hide that a resource may move to another location
Relocation	Hide that a resource may be moved to another location while in use
Replication	Hide that a resource is replicated
Concurrency	Hide that a resource may be shared by several competitive users
Failure	Hide a faulure and recovery of a resource
Persistence	Hide whether a (software) resource is in memory or on disk

Security threads

All those transparencies shows at least on security issue

Basics on *information security*

1. Confidentiality
2. Integrity
3. Availability
4. Authenticity
5. Non-repudiation

Basics on *information security*

1. Confidentiality
   - Information must be disclosed only to the authorized.
2. Integrity
3. Availability
4. Authenticity
5. Non-repudiation

Basics on *information security*

1. Confidentiality
   - Information must be disclosed only to the authorized.
2. Integrity
   - Only authorized can set in the system.
3. Availability
4. Authenticity
5. Non-repudiation

Basics on *information security*

1. Confidentiality
   - Information must be disclosed only to the authorized.
2. Integrity
   - Only authorized can set in the system.
3. Availability
   - Information must be accessible for those who are authorized.
4. Authenticity

5. Non-repudiation

Basics on *information security*

1. Confidentiality
   - Information must be disclosed only to the authorized.
2. Integrity
   - Only authorized can set in the system.
3. Availability
   - Information must be accessible for those who are authorized.
4. Authenticity
   - Information must only be emitted by the authorized.
5. Non-repudiation

Basics on *information security*

1. Confidentiality
   - Information must be disclosed only to the authorized.
2. Integrity
   - Only authorized can set in the system.
3. Availability
   - Information must be accessible for those who are authorized.
4. Authenticity
   - Information must only be emitted by the authorized.
5. Non-repudiation
   - Forbid validity changes on the information emitters.

Basics on *information security*

1. Confidentiality
   - Information must be disclosed only to the authorized.
2. Integrity
   - Only authorized can set in the system.
3. Availability
   - Information must be accessible for those who are authorized.
4. Authenticity
   - Information must only be emitted by the authorized.
5. Non-repudiation
   - Forbid validity changes on the information emitters.

Those first 5 are the basics of the Information Security

Basics on *information security*

1. Confidentiality
   - Information must be disclosed only to the authorized.
2. Integrity
   - Only authorized can set in the system.
3. Availability
   - Information must be accessible for those who are authorized.
4. Authenticity
   - Information must only be emitted by the authorized.
5. Non-repudiation
   - Forbid validity changes on the information emitters.
6. Auditory
   - trace who access where
     (extremely useful for a security breach analysis).

Attacks

Passive

- Eavesdropping

Attacks

Passive

- Eavesdropping

Active

- Men-in-the-middle
- Spoofing: mask and falsify data
- Noise-Interruption-poisoning: Block transmissions
  - Includes [D]DoS
- Modification/Fabrication: agent impersonate

Attacks

Passive

- Eavesdropping

Active

- Men-in-the-middle
- Spoofing: mask and falsify data
- Noise-Interruption-poisoning: Block transmissions
  - Includes [D]DoS
- Modification/Fabrication: agent impersonate

Counter-measures

- Intrusion detection and recovery

Security threads, policies and mechanisms

TANGO needs the 's', like https, stmps, imaps, telnet (ssh),...

Security threads, policies and mechanisms

TANGO needs the 's', like https, stmps, imaps, telnet (ssh),...

- Thread model:
  From "Security engineering" [2],
  based on where the thread usually comes from

Security threads, policies and mechanisms

TANGO needs the 's', like https, stmps, imaps, telnet (ssh),...

- Thread model:
  From "Security engineering" [2],
  based on where the thread usually comes from
  - Hospital
  - Bank
  - Military base

Security threads, policies and mechanisms

TANGO needs the 's', like https, stmps, imaps, telnet (ssh),...

- Thread model:
  From "Security engineering" [2],
  based on where the thread usually comes from
  - Hospital
  - Bank
  - Military base
- References also in "Cryptography Engineering" [3].

Security threads, policies and mechanisms

TANGO needs the 's', like https, stmps, imaps, telnet (ssh),...

- Thread model:
  From "Security engineering" [2],
  based on where the thread usually comes from
  - Hospital
  - Bank
  - Military base
- References also in "Cryptography Engineering" [3].
- 'Practical paranoia' from "Practical cryptography" [4]:

Security threads, policies and mechanisms

TANGO needs the 's', like https, stmps, imaps, telnet (ssh),...

- Thread model:
  From "Security engineering" [2],
  based on where the thread usually comes from
  - Hospital
  - Bank
  - Military base
- References also in "Cryptography Engineering" [3].
- 'Practical paranoia' from "Practical cryptography" [4]:
  - Identify threads
  - Evaluate attack capabilities

Security threads, policies and mechanisms

TANGO needs the 's', like https, stmps, imaps, telnet (ssh),...

- Thread model:
  From "Security engineering" [2],
  based on where the thread usually comes from
  - Hospital
  - Bank
  - Military base
- References also in "Cryptography Engineering" [3].
- 'Practical paranoia' from "Practical cryptography" [4]:
  - Identify threads
  - Evaluate attack capabilities

Do not left all your security in ISO/IEC 27000-series!

Security levels

European commission *fiche 17*
"Exchange of EU classified information" [5]

- Open or Unclassified
- Confidential
- Secret
- Top-Secret

Security levels

European commission *fiche 17*
"Exchange of EU classified information" [5]

- Open or Unclassified
- Confidential
- Secret
- Top-Secret

Sub-classifications

Elements in a group can have internal subsets. Agents with "Top-secret" access only under one subsystem, but "Confidential" under another.

Authentication (I)

- Agent authentication
- User authentication (PAM in Unix)

In TLS what is authenticated is the server, almost never the client.

Authentication (I)

- Agent authentication
- User authentication (PAM in Unix)

In TLS what is authenticated is the server, almost never the client.

Rights

Who have rights to do any read/write action
Access Control Levels: would be similar than linux permissions
But multilevel and both directions.

Authentication (I)

- Agent authentication
- User authentication (PAM in Unix)

In TLS what is authenticated is the server, almost never the client.

Rights

Who have rights to do any read/write action
Access Control Levels: would be similar than linux permissions
But multilevel and both directions.

Tools

- Elliptic curve cryptosystem for TLS (RFC4492 [6])
- This one allow any curve (prime&char2) in WRF[a], unlike RFC6637 [7]

[a] Weierstrass Reduced Form

Encryption

- Encrypt *what has send* to an agent and its *answer*
- Encrypt *events* emitted

Encryption

- Encrypt *what has send* to an agent and its *answer*
- Encrypt *events* emitted

- Transmissions from *single booleans* to *arrays of tenths of thousands of 64bit* elements.
- Neither forget the frequency that they can be transmitted.

Encryption

- Encrypt *what has send* to an agent and its *answer*
- Encrypt *events* emitted

- Transmissions from *single booleans* to *arrays of tenths of thousands of 64bit* elements.
- Neither forget the frequency that they can be transmitted.

Tools

- Elliptic curves cryptosystem for *key exchange*

Encryption

- Encrypt *what has send* to an agent and its *answer*
- Encrypt *events* emitted

- Transmissions from *single booleans* to *arrays of tenths of thousands of 64bit* elements.
- Neither forget the frequency that they can be transmitted.

Tools

- Elliptic curves cryptosystem for *key exchange*
- (generalized) Rijndael (data transmission & event broadcasting)

Encryption

- Encrypt *what has send* to an agent and its *answer*
- Encrypt *events* emitted

- Transmissions from *single booleans* to *arrays of tenths of thousands of 64bit* elements.
- Neither forget the frequency that they can be transmitted.

Tools

- Elliptic curves cryptosystem for *key exchange*
- (generalized) Rijndael (data transmission & event broadcasting)
  - Smaller block size requested
  - Bigger block size would be better than block cipher modes (CBC, CFB, CTR)

Encryption

- Encrypt *what has send* to an agent and its *answer*
- Encrypt *events* emitted

- Transmissions from *single booleans* to *arrays of tenths of thousands of 64bit* elements.
- Neither forget the frequency that they can be transmitted.

Tools

- Elliptic curves cryptosystem for *key exchange*
- (generalized) Rijndael (data transmission & event broadcasting)
  - Smaller block size requested
  - Bigger block size would be better than block cipher modes (CBC, CFB, CTR)
- Stream ciphers

ECC authentication & encryption

ECC authentication & encryption

Using different curves

- Each security level requires its curve size ($\mathbb{F}_p$)

ECC authentication & encryption

Using different curves

- Each security level requires its curve size ($\mathbb{F}_p$)
- Different *subsystems* must use different curves. (even if they have same level)

ECC authentication & encryption

Using different curves

- Each security level requires its curve si
- Different *subsystems* must use different curves.
  (even if they have same level)

Certicom's curves [8]

They are not enough.
(Superset NIST curves).

ECC authentication & encryption

Using different curves

- Each security level requires its curve si
- Different *subsystems* must use different curves. (even if they have same level)

Certicom's curves [8]

They are not enough. (Superset NIST curves).

Tools

Auditable EC generation algorithm.

ECC authentication & encryption

Using different curves

- Each security level requires its curve si
- Different *subsystems* must use different curves. (even if they have same level)

Certicom's curves [8]

They are not enough. (Superset NIST curves).

Cryptosetup

Institution (re)set

Tools

Auditable EC generation algorithm.

ECC authentication & encryption

Using different curves

- Each security level requires its curve si
- Different *subsystems* must use different curves. (even if they have same level)

Certicom's curves [8]

They are not enough. (Superset NIST curves).

Cryptosetup

Institution (re)set

Tools

Auditable EC generation algorithm.

Collateral help

This would help to avoid to share same curve between too many. Thread that the X9.62 [9] advice.

Database access

- TANGO-db is the "phone guide" of the system also stores persistent data, like the properties

Database access

- TANGO-db is the "phone guide" of the system
  also stores persistent data, like the properties
- It is necessary to record over the properties:
  - Who and when modifies
  - Who and when reads (read should be also protectable)

Database access

- TANGO-db is the "phone guide" of the system
  also stores persistent data, like the properties
- It is necessary to record over the properties:
  - Who and when modifies
  - Who and when reads (read should be also protectable)
- Should be possible to restrict areas of the "phone book"
  - It doesn't have much sense to say where an agent runs if you don't have right to talk with it
  - this must not replace agent request for authentication of the requester.

Database access

- TANGO-db is the "phone guide" of the system
  also stores persistent data, like the properties
- It is necessary to record over the properties:
  - Who and when modifies
  - Who and when reads (read should be also protectable)
- Should be possible to restrict areas of the "phone book"
  - It doesn't have much sense to say where an agent runs if you don't have right to talk with it
  - this must not replace agent request for authentication of the requester.

Tools

- Homomorphic encryption/Ordered cryptography

5 Reference Papers

- Zero-knowledge proof
- Session key exchange
- Symmetric and stream ciphers
- Homomorphic encryption

(free) Paper sources

- International Association for Cryptologic Research (e-print & archiver)
- arxiv (open access e-print archiver)
- vixra (alternative open e-print archiver)
- citeseer (scientific search engine)
- scholar (Google's indexer)
- dblp (bib reference)

Zero-knowledge proof for authentication

- S.Martínez, "*Protocolos de seguridad para sistemas de identificación por radiofrecuencia*". PhD Thesis UdL, march 2011. Directed by: Concepció Roig and Magda Valls.[10]
- BSI TR-03110:"*Advanced security mechanisms for machine readable travel documents.*".[11]

key exchange

- R. Tomàs, "*Volcans d'isogenies de corbes el·líptiques: Aplicacions criptogràfiques en targetes intel·ligents*". PhD Thesis UdL, march 2011. Directed by: Josep M. Miret and Daniel Sadornil.[12]
- BSI TR-03111:"*Elliptic curve cryptography, version 2.0*" .[13]
- S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, and B. Moeller, "*Elliptic curve cryptography (ecc) cipher suites for transport layer security (tls)*" May 2006. RFC4492. [6]

Elliptic curves

- J. Valera, "Volcales de ℓ-isogenias de curvas elípticas," Sistemas Informáticos. Escola Politècnica Superior. Universidad de Lleida, Sept 2011. Directed by: Josep M. Miret. [14]
- A. Rostovtsev and E. Rostovtsev and A. Stolbunov "Public-Key Cryptosystem Based On". 2006 [15]
- R. Moreno, Subgrupos de Sylow de las curva ellíipticas definidas sobre cuerpos finitos. PhD thesis, Universitat Politècnica de Catalunya, 2005. Directed by: Anna Rio and Josep M. Miret. [16]

Ongoing:

- S. Blanch-Torné and R. Moreno and F. Sebé and J. Varela "Security risk associated with multiple users sharing the same elliptic curve". Draft [17]

Symmetric ciphers

- "*Specification for the advanced encryption standard (aes).*" Federal Information Processing Standards Publication 197, 2001.[18]
- J. Daemen and V. Rijmen, "*The Design of Rijndael*". Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2002. [19]
- J. Schaad and R. Housley, "*Advanced Encryption Standard (AES) Key Wrap Algorithm.*" Sept. 2002. RFC3394 [20]

Ongoing:

- S. Blanch-Torné and R. Moreno and F. Sebé and M. Valls "Generalised Rijndael". Draft [21]

Stream ciphers

- TODO: "*More information required!*"
- Key Derivation Functions
- Wikipedia (en)
  - Rabbit (RFC4503)
  - VEST
- Chacha20

Private database query system

- D. B. nad Craig Bentry, S. Halevi, F. Wang, and D. J. Wu, "*Private database queries using somewhat homomorphic encryption*," International Association for Cryptologic Research, June 2013.

Reference journals

- TODO: "*More information required!*"

Reference conferences & workshops

- Icalepcs: International Conference on Accelerator and Large Experimental Physics Control Systems
- No-bugs: New Opportunities for Better User Group Software
- CHES: Cryptographic Hardware and Embedded Systems
- SAC: Selected Areas in Cryptography
- Crypto, Eurocrypt, & Asiacrypt
- Tango Meeting

References I


A. S. Tanenbaum and M. van Steen, *Distributed systems, Principles and Paradigms*.
Prentice Hall, 2002.
International Edition.


R. J. Anderson, *Security engineering - a guide to building dependable distributed systems (2. ed.)*.
Wiley, 2008.


N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering: Design, principles and practical applications*.
Wiley, 2010.


N. Ferguson and B. Schneier, *Practical Cryptography*.
New York, NY, USA: John Wiley & Sons, Inc., 2003.


"Exchange of eu classified information," 2003.

References II


S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)." RFC 4492 (Informational), May 2006.
Updated by RFC 5246.


A. Jivsov, "Elliptic Curve Cryptography (ECC) in OpenPGP." RFC 6637 (Proposed Standard), June 2012.


"Sec 2. standards for efficient cryptography group: Recommended elliptic curve domain parameters."


"Ansi x9.62, public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ecdsa)."

References III


S. Martínez, *Protocolos de seguridad para sistemas de indentificación por radiofrecuencia*.
PhD thesis, Universitat de Lleida, march 2011.
Directed by: Concepció Roig and Magda Valls.


"Bsi tr-03110: Advanced security mechanisms for machine readable travel documents."


R. Tomàs, *Volcans d'isogenies de corbes el·lítiques: Aplicacions criptogràfiques en targetes intel·ligents*.
PhD thesis, Universitat de Lleida, march 2011.
Directed by: Josep M. Miret and Daniel Sadornil.


"Bsi tr-03111: Elliptic curve cryptography, version 2.0."

References IV

J. Valera, "Volcales de ℓ-isogenias de curvas elípticas," *Sistemas Informáticos. Escola Politècnica Superior. Universidad de Lleida*, Sept 2011.
Directed by: Josep M. Miret.

A. Rostovtsev, E. Rostovtsev, and A. Stolbunov, "Public-key cryptosystem based on isogenies," 2006.

R. Moreno, *Subgrupos de Sylow de las curva ellíipticas definidas sobre cuerpos finitos*.
PhD thesis, Universitat Politècnica de Catalunya, 2005.
Directed by: Anna Rio and Josep M. Miret.

S. Blanch-Torné, R. Moreno, and F. Sebé, "Security risk associated with multiple users sharing the same elliptic curve." Draft.

References V


"Specification for the advanced encryption standard (aes)." Federal Information Processin Standards Publication 197, 2001.


J. Daemen and V. Rijmen, *The Design of Rijndael*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2002.


J. Schaad and R. Housley, "Advanced Encryption Standard (AES) Key Wrap Algorithm." RFC 3394 (Informational), Sept. 2002.


S. Blanch-Torné, R. Moreno, F. Sebé, and M. Valls, "Generalised rijndael." Draft.

Alba's duties

- Diagnostics
  - CCDs
  - Instrumentation
  - Tune excitation
  - Filling Pattern FCT
- Linac
- Power Supplies
  - Magnet cycling
  - StateCode interpreter
  - Fast orbit feedback
- Radio Frequency
  - Digital Low Level RF
  - Fast Data Logger
  - Facade
- Optics lab
  - Autocollimator
- Sardana controllers
  - IBACtrl
  - ElComatCtrl
  - AttenIOR (group)
  - MirrorPM & MonoPM
- Tango naming convention (and DNS)
- "Interfaces to the Alba Control System"
- "Controls coding standard and packaging convention"