Securing TANGO Control System: A brain storming

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 a Programmable Logic Controllers

Figure: Labview as SCADA example

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

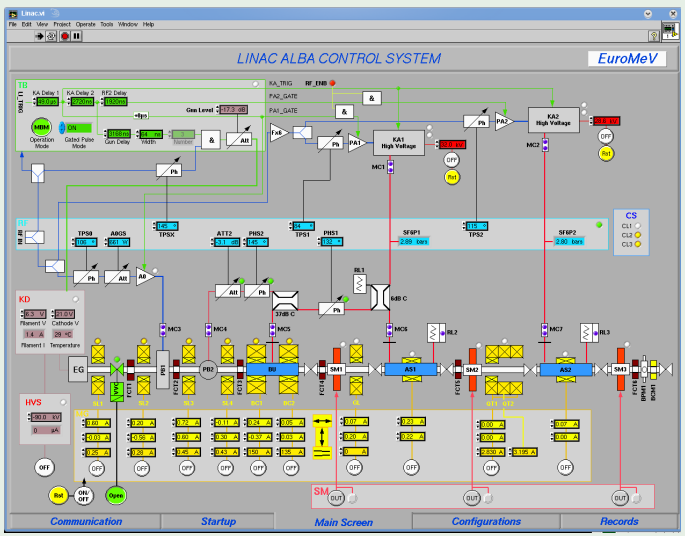


Figure: Labview as SCADA example

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)

Figure: Logos of the Tango Consortium Members

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? (iIII)

TANGO parts

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

Device servers, device classes, and devices

TODO: "*Draw a nice picture about what those three things are...*"

What has an Agent (a device)

TODO: "*commands,attributes and properties*"

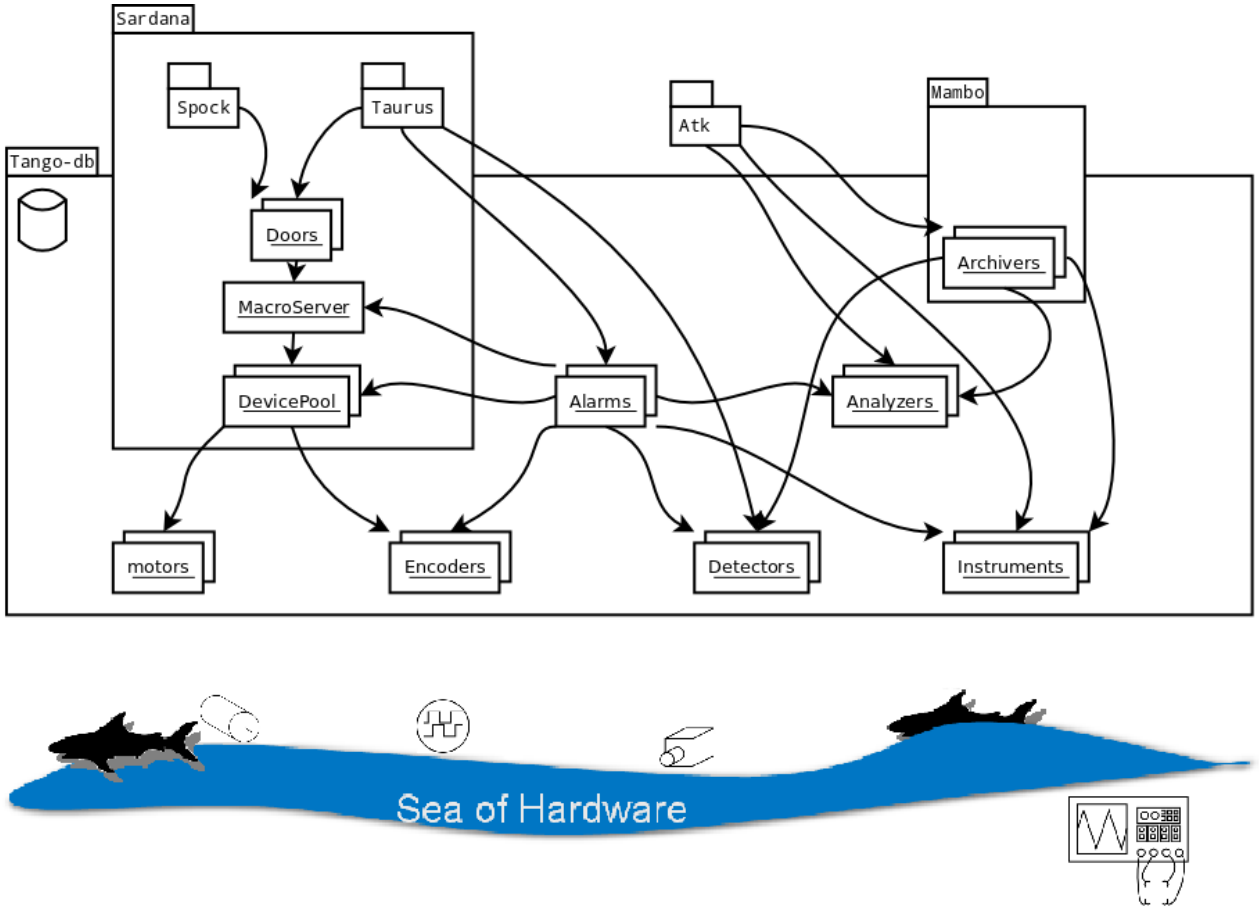
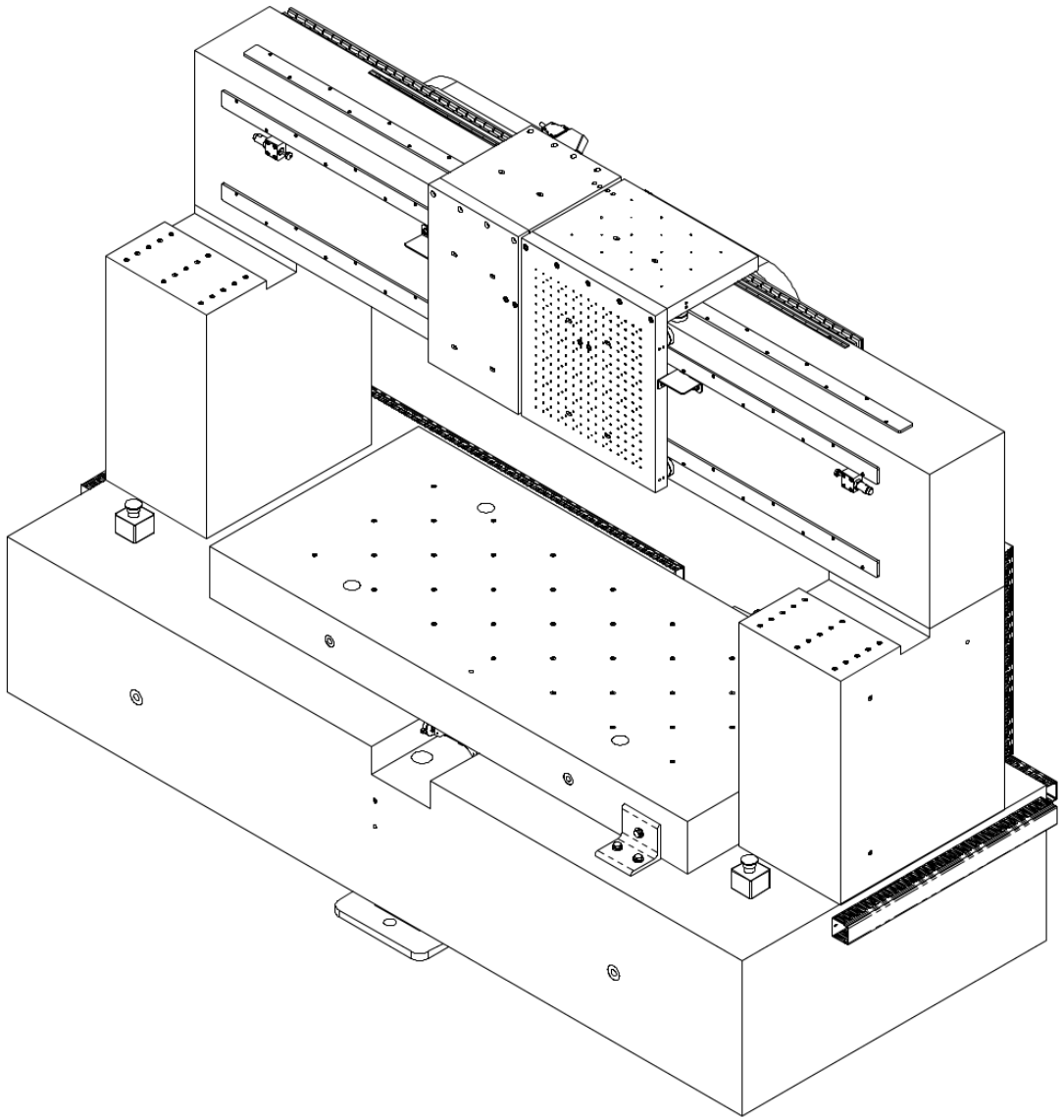
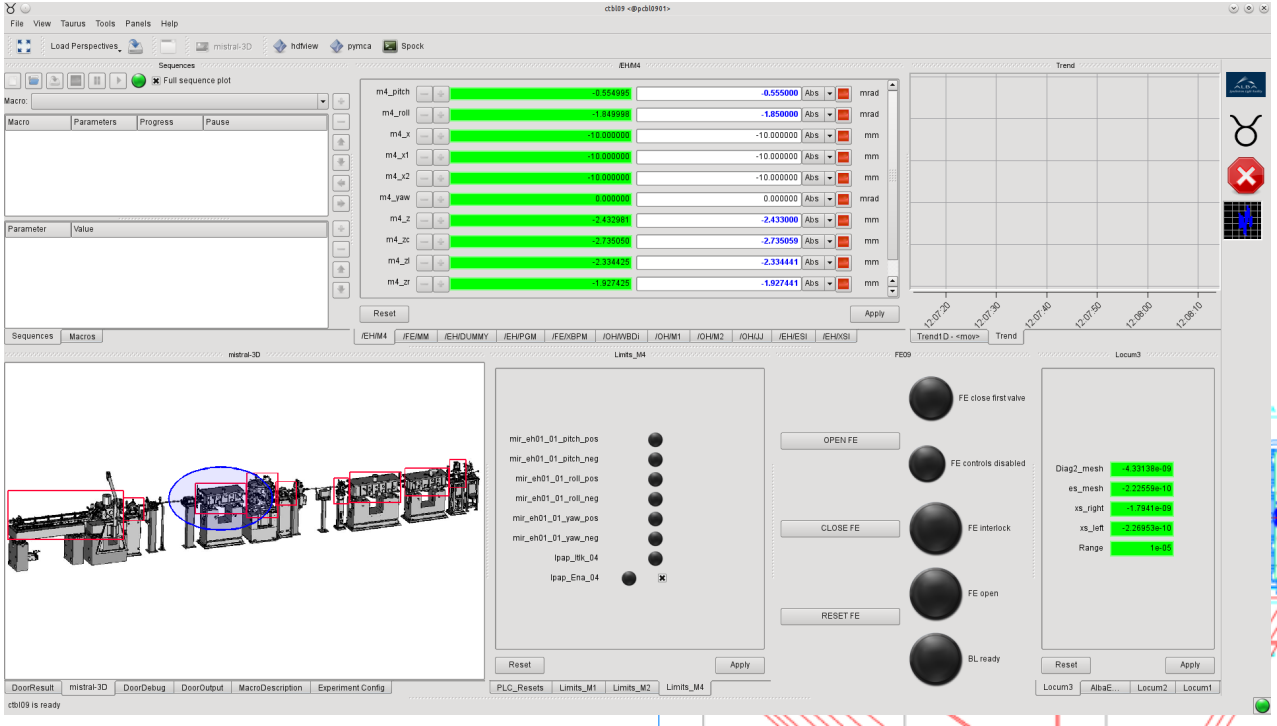


Figure: Tango schematic layout

Optics Lab: Long Term Profiler



A beamline


File View Taurus Tools Panels Help
Load Perspectives
Sequences
Full sequence plot
Macro
Parameter
Value
Sequences
Macros
/EH/M4
m4_pitch
m4_roll
m4_x
m4_x1
m4_x2
m4_yaw
m4_z
m4_zc
m4_zl
m4_zr
Reset
Apply
Trend
Trend1D - <mov>
mistral-3D
Limits_M4
mir_eh01_01_pitch_pos
mir_eh01_01_pitch_neg
mir_eh01_01_roll_pos
mir_eh01_01_roll_neg
mir_eh01_01_yaw_pos
mir_eh01_01_yaw_neg
lpap_lltk_04
lpap_Ena_04
FE09
OPEN FE
CLOSE FE
RESET FE
FE close first valve
FE controls disabled
FE interlock
FE open
BL ready
Locum3
Diag2_mesh
es_mesh
xs_right
xs_left
Range
DoorResult
mistral-3D
DoorDebug
DoorOutput
MacroDescription
Experiment Config
PLC_Resets
Limits_M1
Limits_M2
Limits_M4
Locum1
Locum2
ctbl09 is ready

Control a synchrotron accelerator

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 layers

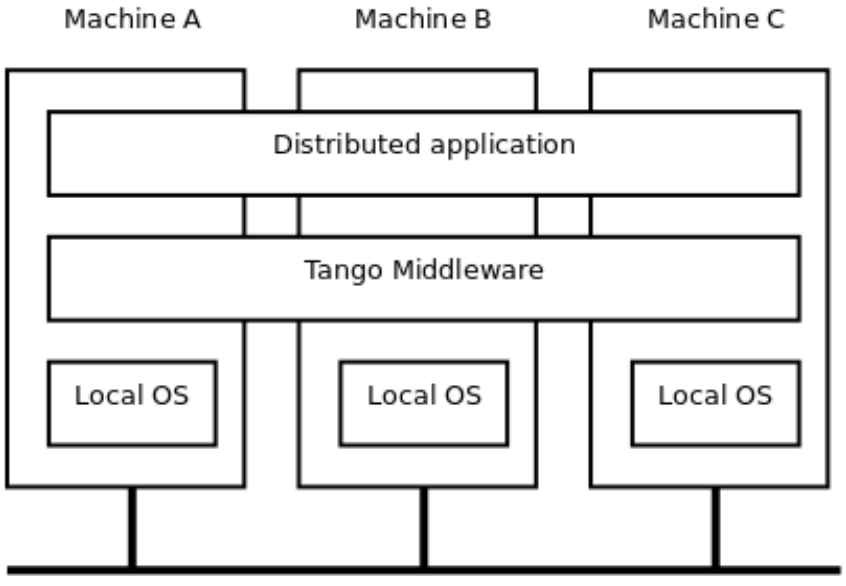


Figure: From [1], A distributed system organized as middleware

Basics

- Confidentiality
- Authenticity
- Integrity
- Availability
- Non-repudiation

Security threads, policies and mechanisms

Security levels

European commission *fiche 17*
"Exchange of EU classified information" [2]

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

Authentication

- Agent authentication
- User authentication

Rights

Who have rights to do any read/write action
Access Control Levels (ACL): would be similar than linux permissions

Encryption

Database access

(free) Paper sources

- iacr
- arxiv
- scholar
- dblp

Zero-knowledge proof for authentication

Secret broadcasting

Symmetric cyphers

Stream cyphers

Private database query system

Reference journals

Reference conferences

References I


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


"Exchange of eu classified information," 2003.