# Securing TANGO Control System: A brain storming

Sergi Blanch i Torné

Cryptography & Graphs
Math Department
Universitat de Lleida

September 24th, 2013

# Outline

1. Introduction
2. Identify scenarios
3. Cryptography engineering
4. Proposed solutions
5. Reference Papers
6. Journals & Conferences

# 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: Part 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."

## Examples of an SCADAs

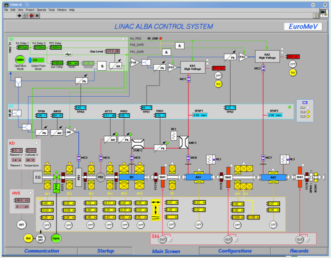


Figure: Labview as SCADA example

# 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)

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

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 ∅MQ 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*"

## Definitions

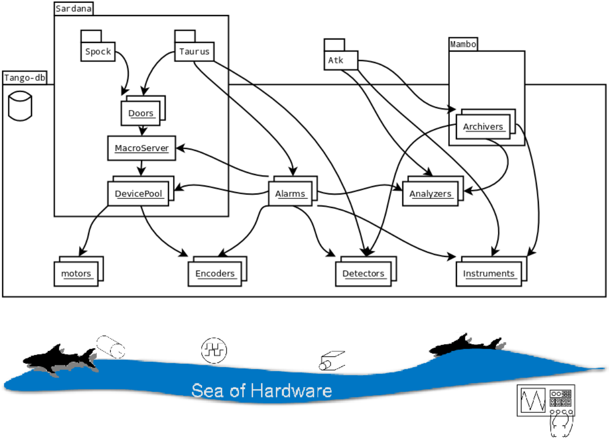
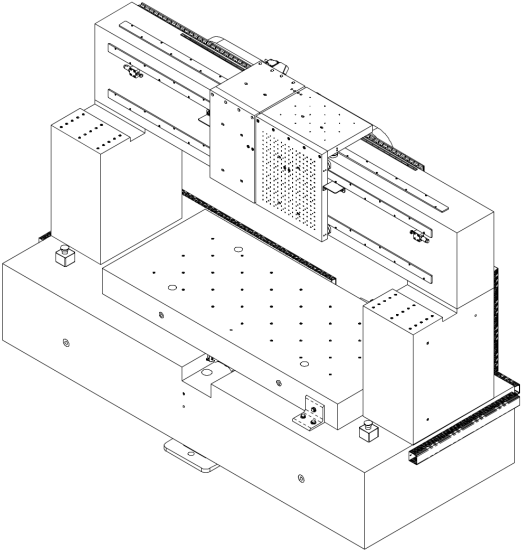
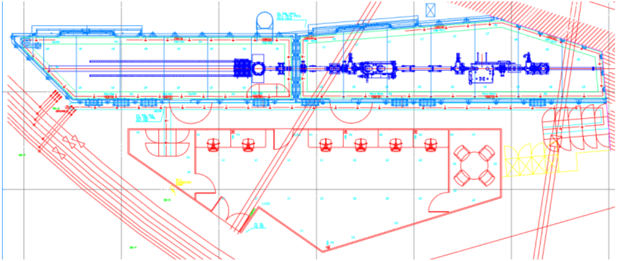


Figure: Tango schematic layout

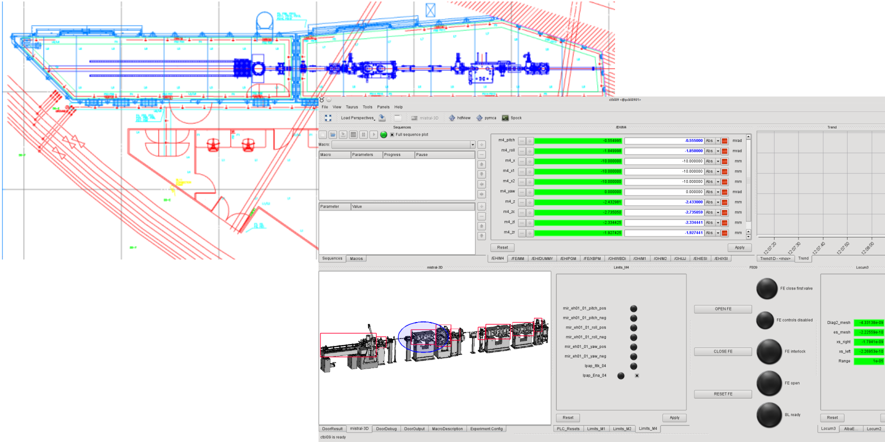
# Optics Lab: Long Term Profiler



# A beamline



# A beamline



| | | | | |
|---|---|---|---|---|
| m4_pitch | -0.554995 | -0.555000 | Abs | mrad |
| m4_roll | -1.849998 | -1.850000 | Abs | mrad |
| m4_x | -10.000000 | -10.000000 | Abs | mm |
| m4_x1 | -10.000000 | -10.000000 | Abs | mm |
| m4_x2 | -10.000000 | -10.000000 | Abs | mm |
| m4_yaw | 0.000000 | 0.000000 | Abs | mrad |
| m4_z | -2.432981 | -2.433000 | Abs | mm |
| m4_zc | -2.735050 | -2.735059 | Abs | mm |
| m4_zl | -2.334425 | -2.334441 | Abs | mm |
| m4_zr | -1.927425 | -1.927441 | Abs | mm |

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 ●
Ipap_Itlk_04 ●
Ipap_Ena_04 ● ☒

| | |
|---|---|
| Diag2_mesh | -4.33138e-09 |
| es_mesh | -2.22559e-10 |
| xs_right | -1.7941e-09 |
| xs_left | -2.26953e-10 |
| Range | 1e-05 |

## Control a synchrotron accelerator

- TODO: "*Draws of the synchrotron layout and data from the ccdb about the service area numbers*"
- TODO: "*List subsystems in the accelerator*"
  - Timming (132 agents)
  - Vaccum (1085 agents)
  - Power supplies (491 agents)
  - Radio frequency (124 agents)
  - Diagnostics (744 agents)
  - +2500 agents
- TODO: "*Astor*"

# 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).

### Passive

- Eavesdropping

### Active

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

### counter-measures

- Intrusion detection and recovery

# Security threads, policies and mechanisms

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

# Security threads, policies and mechanisms

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

# Security threads, policies and mechanisms

- 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

- 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

- 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

- Agent authentication
- User authentication (PAM in Unix)

# Authentication

- Agent authentication
- User authentication (PAM in Unix)

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

# Authentication

- 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

- 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, unlike RFC6637 [7]

# Encryption

- Encrypt what has send to an agent
- Encrypt what has been answered by an agent
- Encrypt events emitted

# Encryption

- Encrypt what has send to an agent
- Encrypt what has been answered by an agent
- Encrypt events emitted

- There are transmissions of 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
- Encrypt what has been answered by an agent
- Encrypt events emitted

- There are transmissions of 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 and/or Stream cyphers
  for data transmission and event broadcasting

# 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 cyphers
- 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.[8]
- BSI TR-03110:"*Advanced security mechanisms for machine readable travel documents.*".[9]

# 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.[10]
- BSI TR-03111:"*Elliptic curve cryptography, version 2.0*".[11]
- 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]

# Symmetric cyphers

- "*Specification for the advanced encryption standard (aes).*" Federal Information Processing Standards Publication 197, 2001.[12]
- J. Daemen and V. Rijmen, "*The Design of Rijndael*". Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2002. [13]
- Smaller block size requested
- Bigger block size would be better than block cipher modes (CBC, CFB, CTR)
- J. Schaad and R. Housley, "*Advanced Encryption Standard (AES) Key Wrap Algorithm.*" Sept. 2002. RFC3394 [14]

# Stream cyphers

- TODO: “*More information required!*”

# 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
- 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.

- 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."

# References III

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."

"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.