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 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: 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

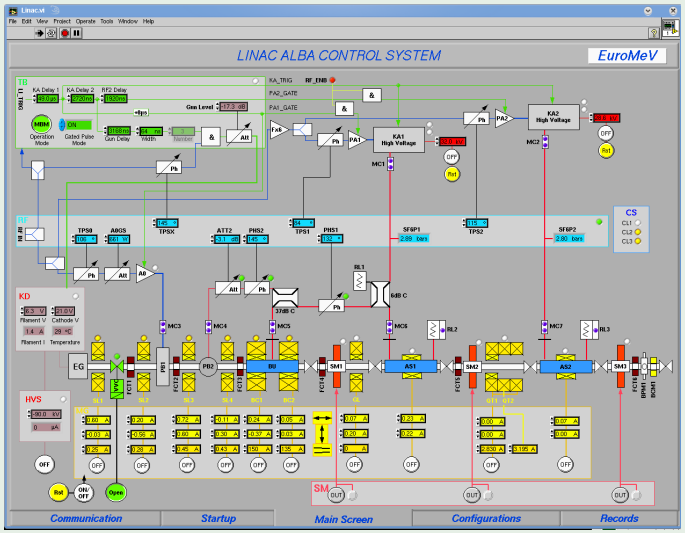


Figure: Labview as SCADA example

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*"

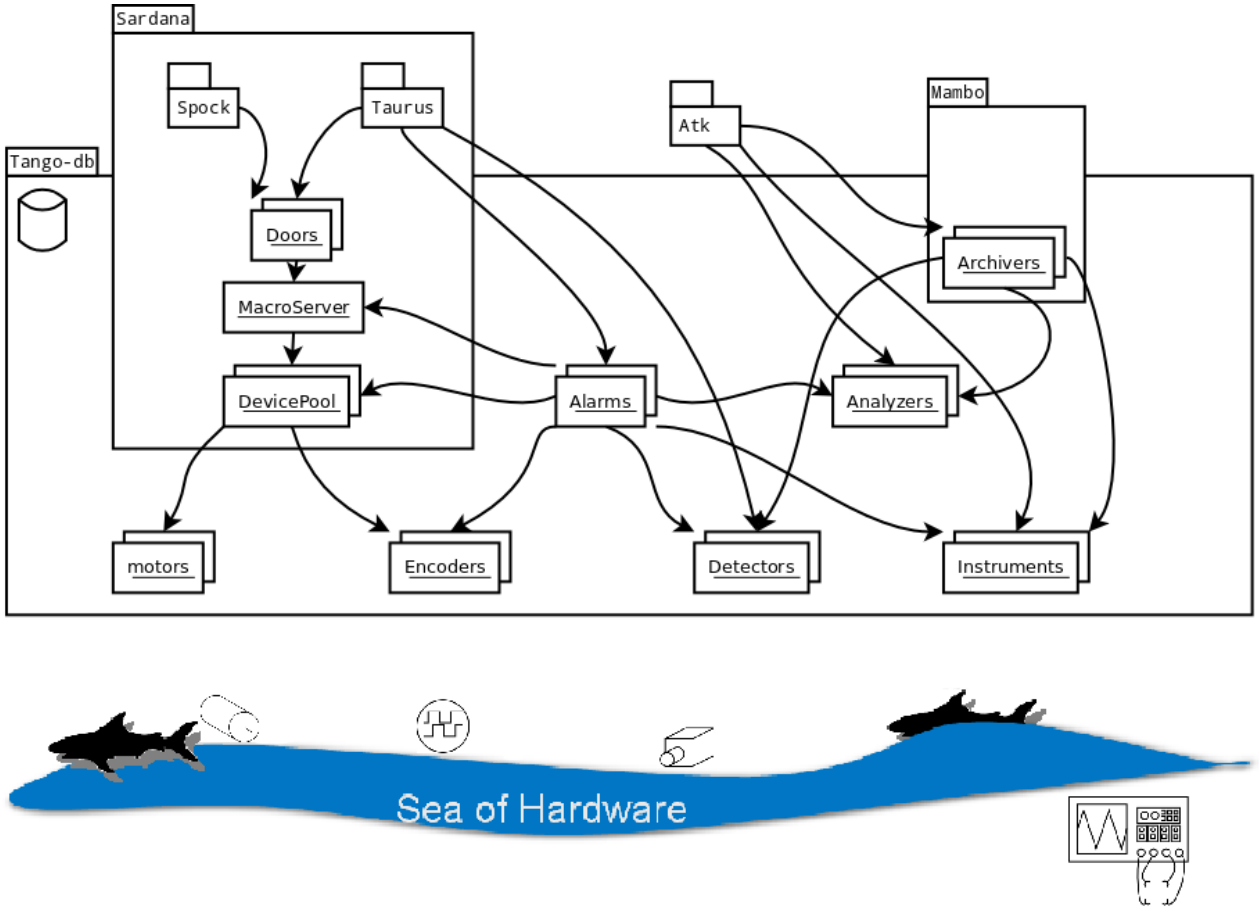
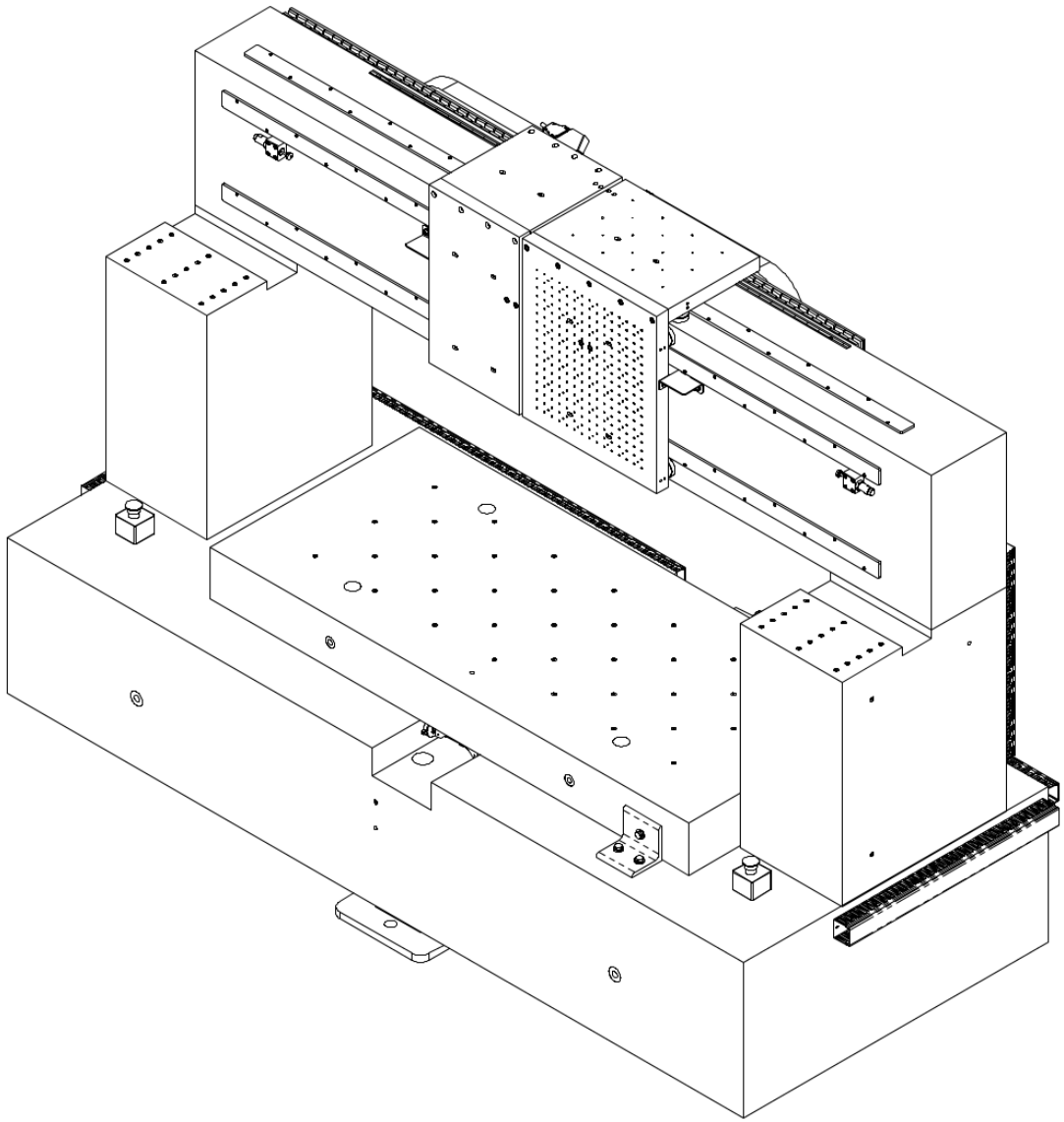
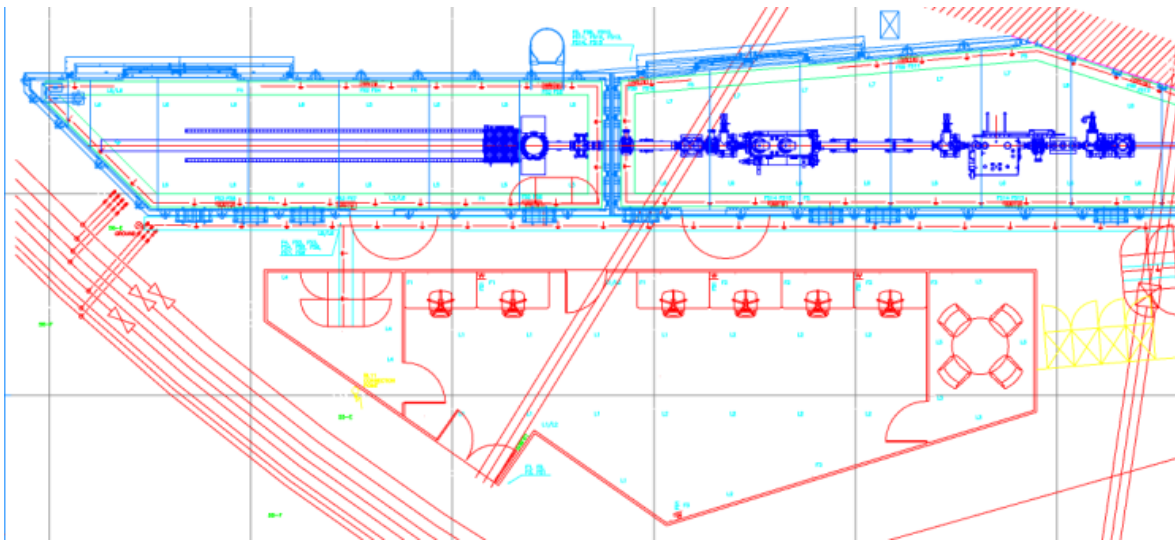


Figure: Tango schematic layout

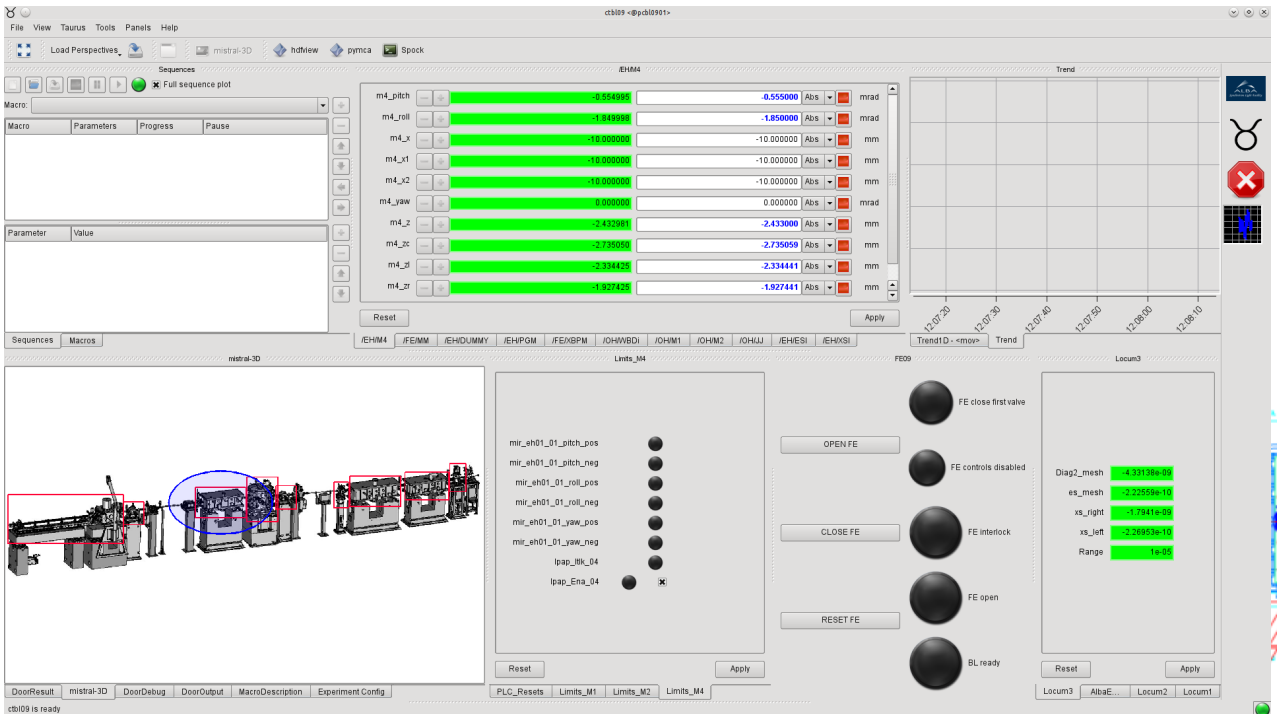
Optics Lab: Long Term Profiler

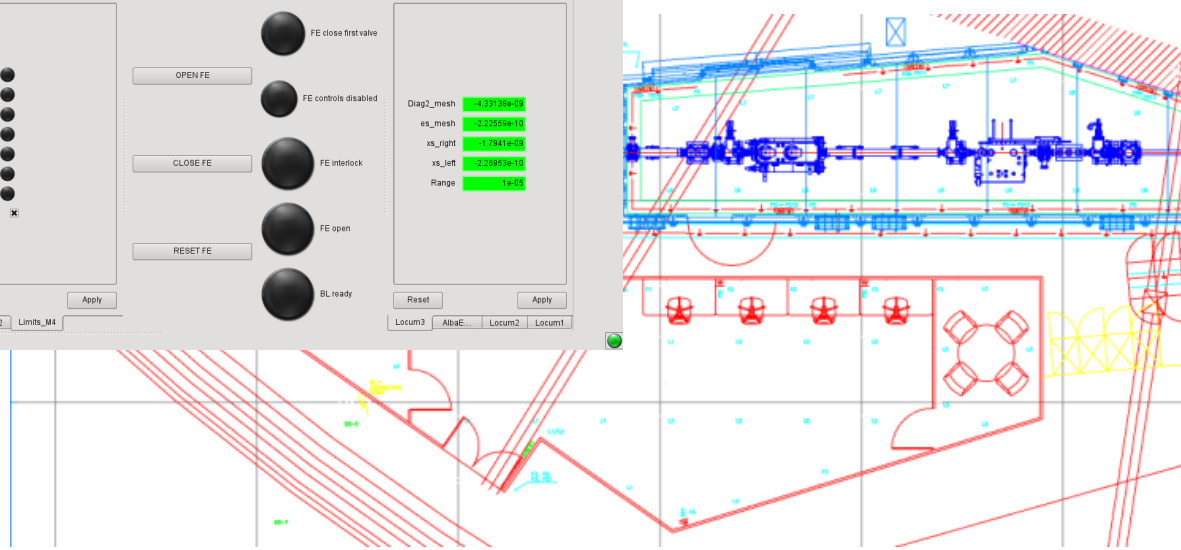


A beamline



A beamline


File View Taurus Tools Panels Help
Load Perspectives
Sequences
Full sequence plot
Macro
Parameter
Value
Reset
Apply
Trend
mistral-3D
Limits_M4
FE09
Locum3
OPEN FE
CLOSE FE
RESET FE
FE close first valve
FE controls disabled
FE interlock
FE open
BL ready
Range
Sequences
Macros
DoorResult
mistral-3D
DoorDebug
DoorOutput
MacroDescription
Experiment Config
PLC_Resets
Limits_M1
Limits_M2
Limits_M4
Locum3
Locum2
Locum1



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).

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 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

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

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

Tools

- Elliptic curve cryptosystem

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

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

(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.


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.