

# 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 Security levels
- 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."

## Examples of an Industrial Control System

**TODO:** "Add sample pictures here..."

# 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

**TODO:** *"Add sample pictures here..."*

# What is an DCS?

## 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)

The sea of Hardware

**TODO:** *"Add the nice picture of the shark..."*

# What is a TANGO? (II)

It's an Distributed Control System  
using CORBA as a Middleware

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  $\Rightarrow$  the Middleware
- TANGO Device Servers  $\Rightarrow$  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)

- Data types: Boolean, [U]Short, [U]Long[64], Double, String
- Data dimensions: Scalar, Spectrum, Image

**TODO:** *"commands, attributes and properties"*



# Optics Lab: Long Term Profiler

# A beamline

# Control a synchrotron accelerator

# Against the transparencies

Access	Hide differences in data representation and how a resource
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 v
Replication	Hide that a resource is replicated
Concurrency	Hide that a resource may be shared by several competitiv
Failure	Hide a faulure and recovery of a resource
Persistence	Hide whether a (software) resource is in memory or on di

# Against the layers

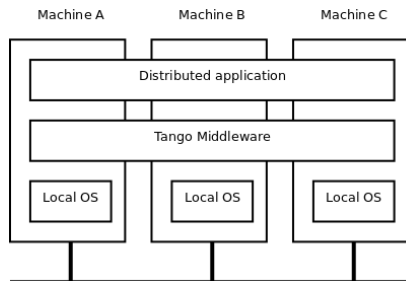


Figure: From [1], A distributed system organized as middleware

# Basics

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

# Security levels

# Security levels

European commission *fiche 17*

“Exchange of EU classified information” [2]

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



# Authentication

# Encryption

Introduction  
oooooooo

Identify Scenarios  
ooo

Security levels  
oo

Proposed solutions  
oo●

Reference Papers  
ooooo

Journals & Conferences  
ooo

Database

# Database access

# Zero-knowledge proof for authentication

# Secret broadcasting

# Symmetrics

# 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.