ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

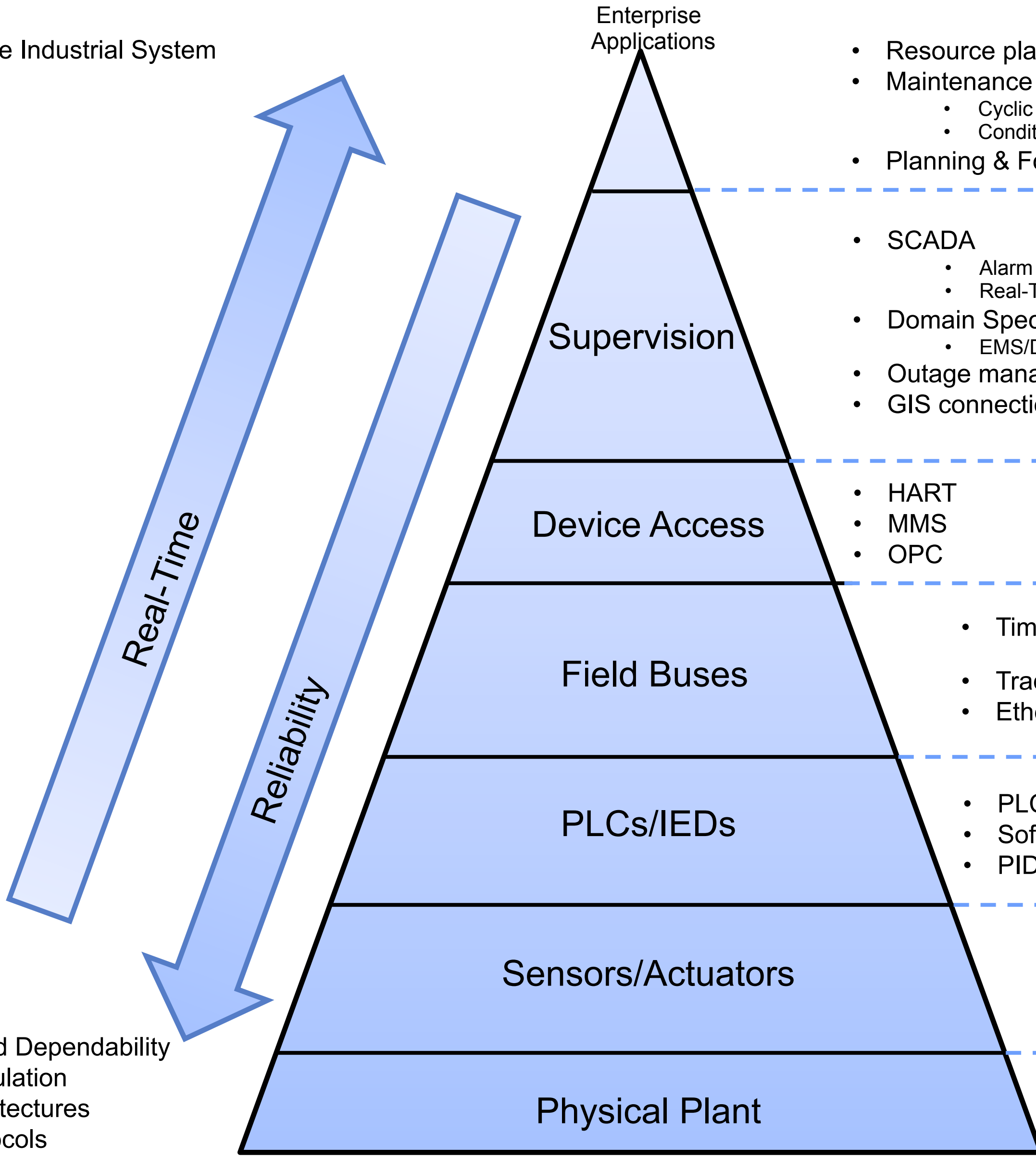
Industrial Automation
Automation Industrielle

SCADA
Operator Interface
Interface Opérateur

Dr. Jean-Charles Tournier

The material of this course has been initially created by Prof. Dr. H. Kirrmann and adapted by Dr. Y-A. Pignolet & J-C. Tournier

- Real Time Industrial System



- Resource planning
- Maintenance
    - Cyclic
    - Condition-based
- Planning & Forecasting

- SCADA
    - Alarm management (EEMU 191)
    - Real-Time Databases
- Domain Specific Applications
    - EMS/DMS
- Outage management
- GIS connections

- HART
- MMS
- OPC

- Time Synchronization
    - PPS, GPS, SNTP, PTP, etc.
- Traditional - Modbus, CAN, etc.
- Ethernet-based - HSR, WhiteRabbit, etc.

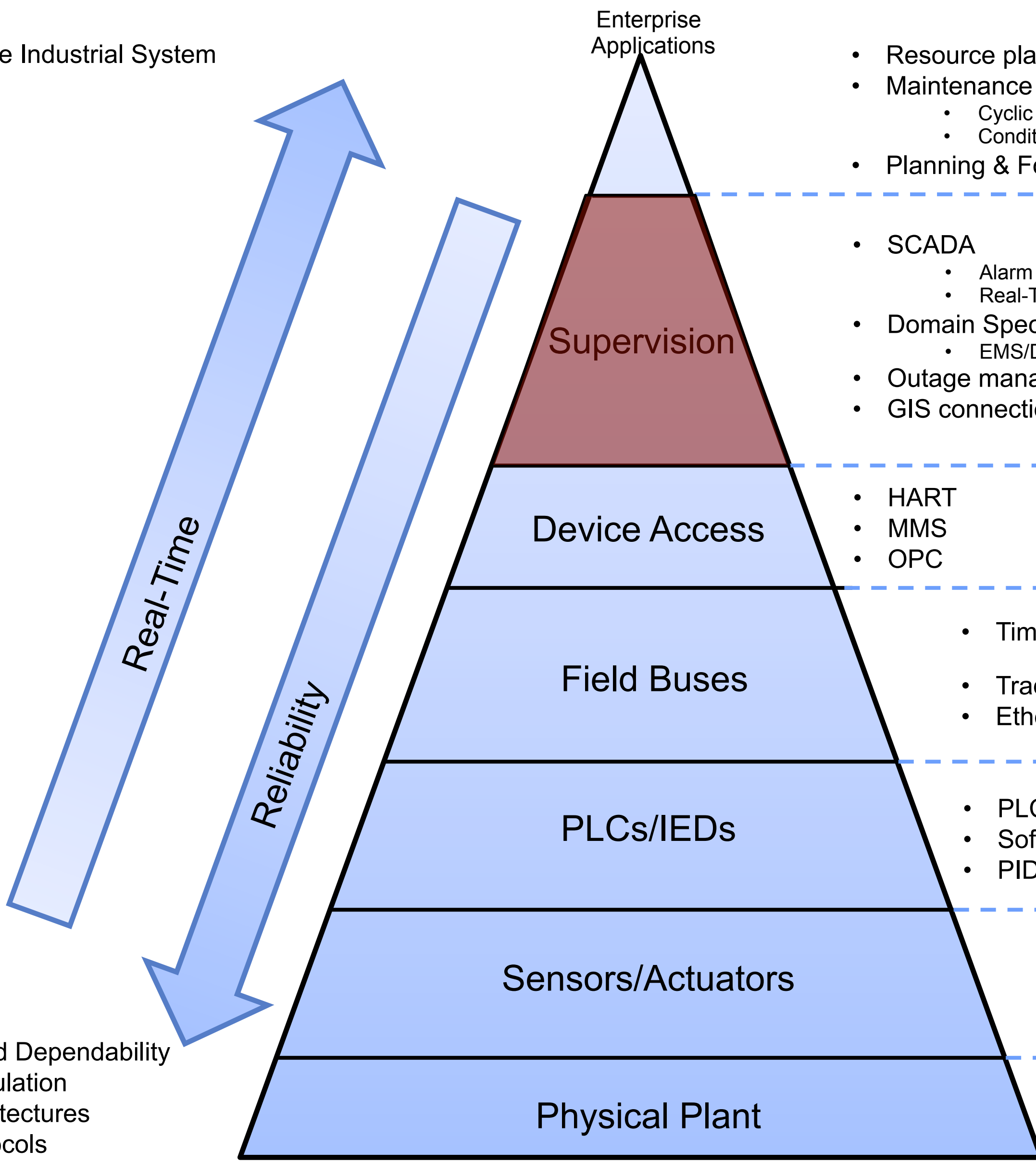
- PLC
- SoftPLC
- PID

- Instrumentation
- 4-20 mA loop
- Sensors accuracy
- Examples (CT/VT, water, gaz, etc.)

- Plant examples
- Why supervision/control?

- Reliability and Dependability
    - Calculation
    - Architectures
    - Protocols

- Real Time Industrial System



- Resource planning
- Maintenance
  - Cyclic
  - Condition-based
- Planning & Forecasting

- SCADA
  - Alarm management (EEMU 191)
  - Real-Time Databases
- Domain Specific Applications
  - EMS/DMS
- Outage management
- GIS connections

- HART
- MMS
- OPC

- Time Synchronization
  - PPS, GPS, SNTP, PTP, etc.
- Traditional - Modbus, CAN, etc.
- Ethernet-based - HSR, WhiteRabbit, etc.

- PLC
- SoftPLC
- PID

- Instrumentation
- 4-20 mA loop
- Sensors accuracy
- Examples (CT/VT, water, gaz, etc.)

- Plant examples
- Why supervision/control?

- Reliability and Dependability
  - Calculation
  - Architectures
  - Protocols

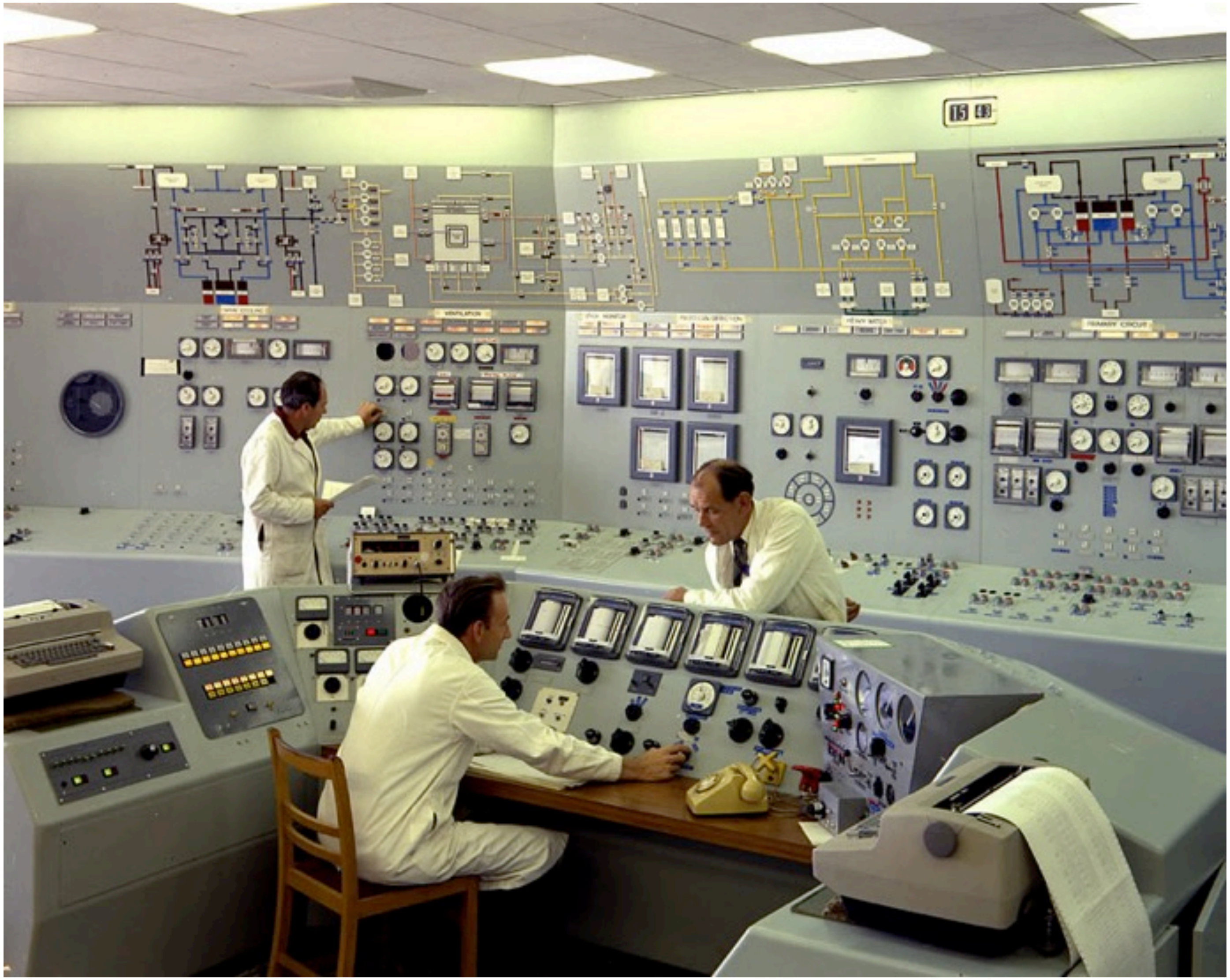
Content

- **Definitions**
- **SCADA Functionalities**
- **Cyber-security and SCADA**
- **Examples of SCADA Systems**

Control Room From the 1950s

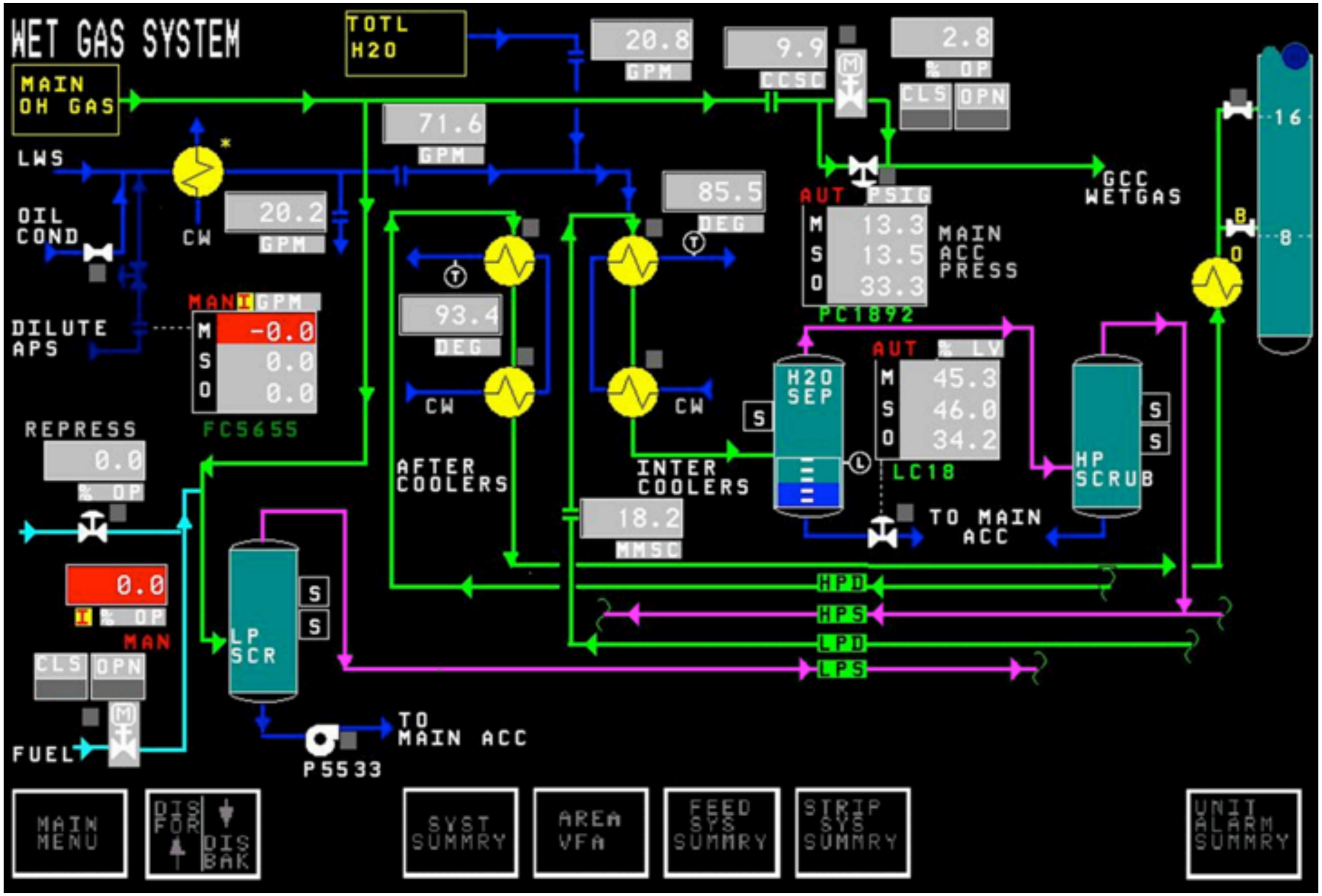
Coal-Fired Battersea Power Station – South London, UK – 1950s
Photo: Fox Photos/Getty Images

Control Room Example From the 1970s



Steam Generating Heavy Water Reactor – (Water Cooled Nuclear Reactor) - Dorset, UK - 1970s

Control Room from the 90s



Control Room From the 2010s

ISO New England Control Room

Next?


12:30 PM
Lunch
JFK
SFO
Virgin Airlines
Flight 23
10:31 AM
On Time
tomorrow
80°
60°
30%
New York
72°

Definitions

- **SCADA**
  - Supervisory Control and Data Acquisition

- **Control Room**
  - Room serving as an operation center from which the operators can monitor and control a system

- **Operator Workstation**
  - Equipment used by the operator in the control room to monitor and control a system

- **Acquisition Device**
  - Field devices bringing data to or from the SCADA and the process devices

SCADA Functionalities 1/2

- Data acquisition
  store binary & analog data into process data base

- Human Machine Interface (HMI):
  graphical object state presentation, lists, reports

- Operator Command handling
  change binary commands, set points
  prepare and run recipes, batches, scripts (command procedures)

- Alarm & Events
  Alert the operators of a specific event
  record specified changes and operator actions

SCADA Functionalities 2/2

- History data base
  keep a record of the process values and filter it

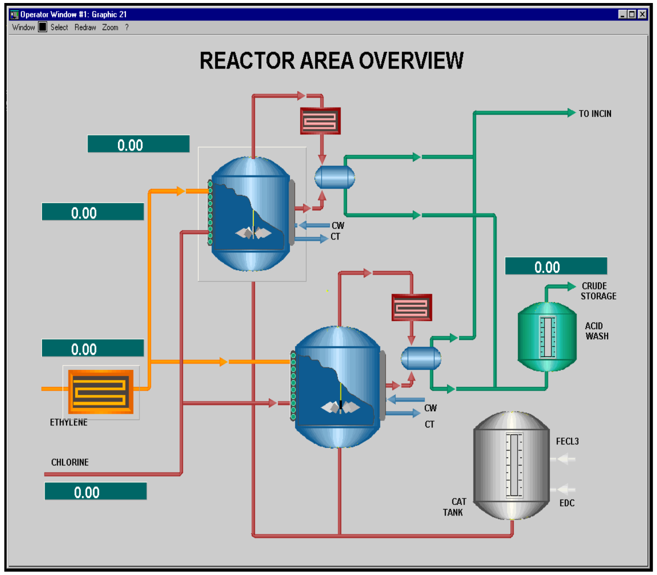
- Measurements processing
  calculate derived values (limit supervision, trending)

- Logging
  keep logs on the operation of the automation system

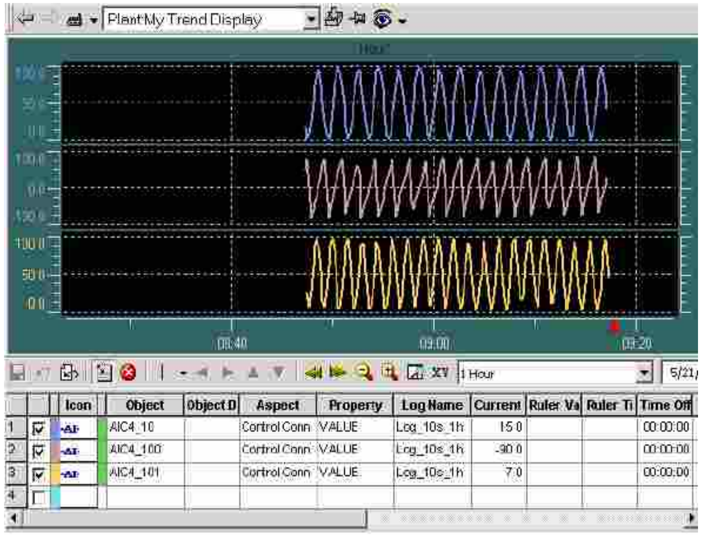
- Reporting
  generate incident reports

- Interfacing to planning & analysis functions:
  Forecasting, Simulation, historian, etc.

Operator workplace: three main functions

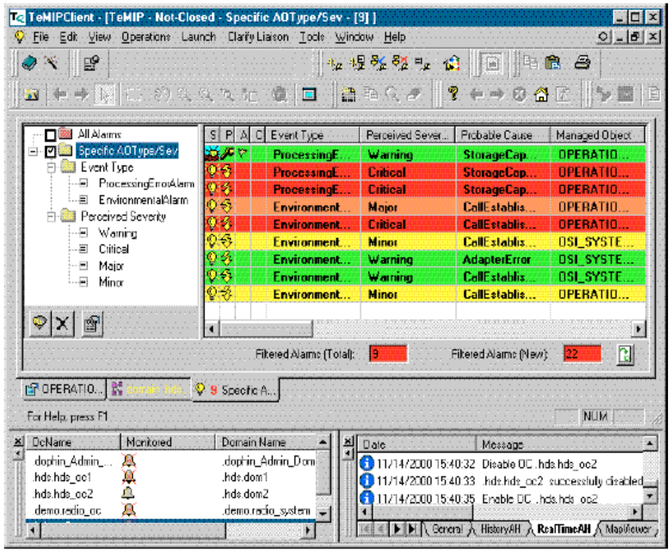


current state

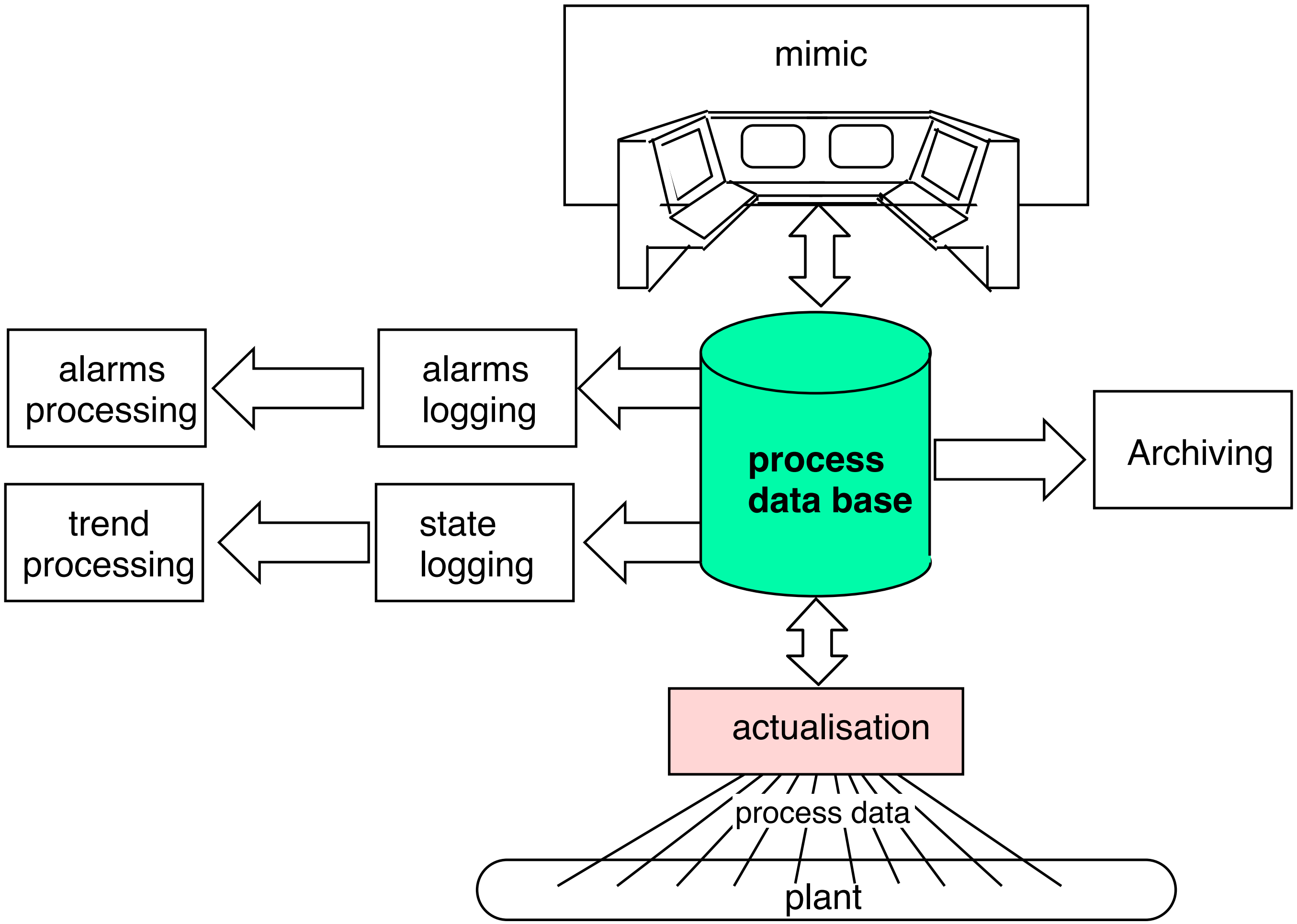


trends and history

alarms and events



Elements of the operator workstation



Data Acquisition

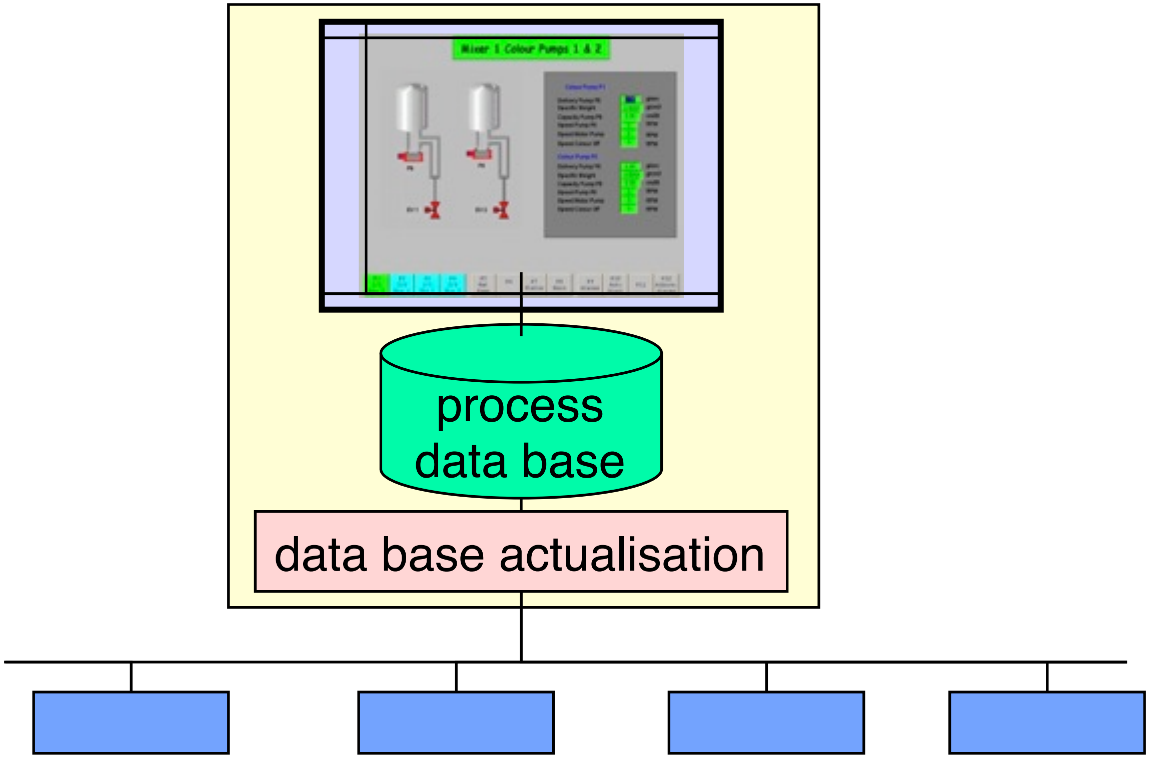
- Acquisition protocols depend on the system/domain
  - c.f. lecture on communication network
  - E.g. Power System Applications
    - DNP, IEC 60870-5-104, IEC 61850
  - E.g. Industrial Plants
    - OPC, S7, MODBUS, etc.
  - Many proprietary protocols that bring a specific characteristics
    - E.g. robustness, real-time, security, etc.

- Acquisition can be
  - Direct
    - Usually when all equipment are on the same networks or local (e.g. for serial communications).
  - Indirect
    - Through data concentrators (e.g. Remote Terminal Unit in Power Substation)
    - Usually the case when different networks are involved

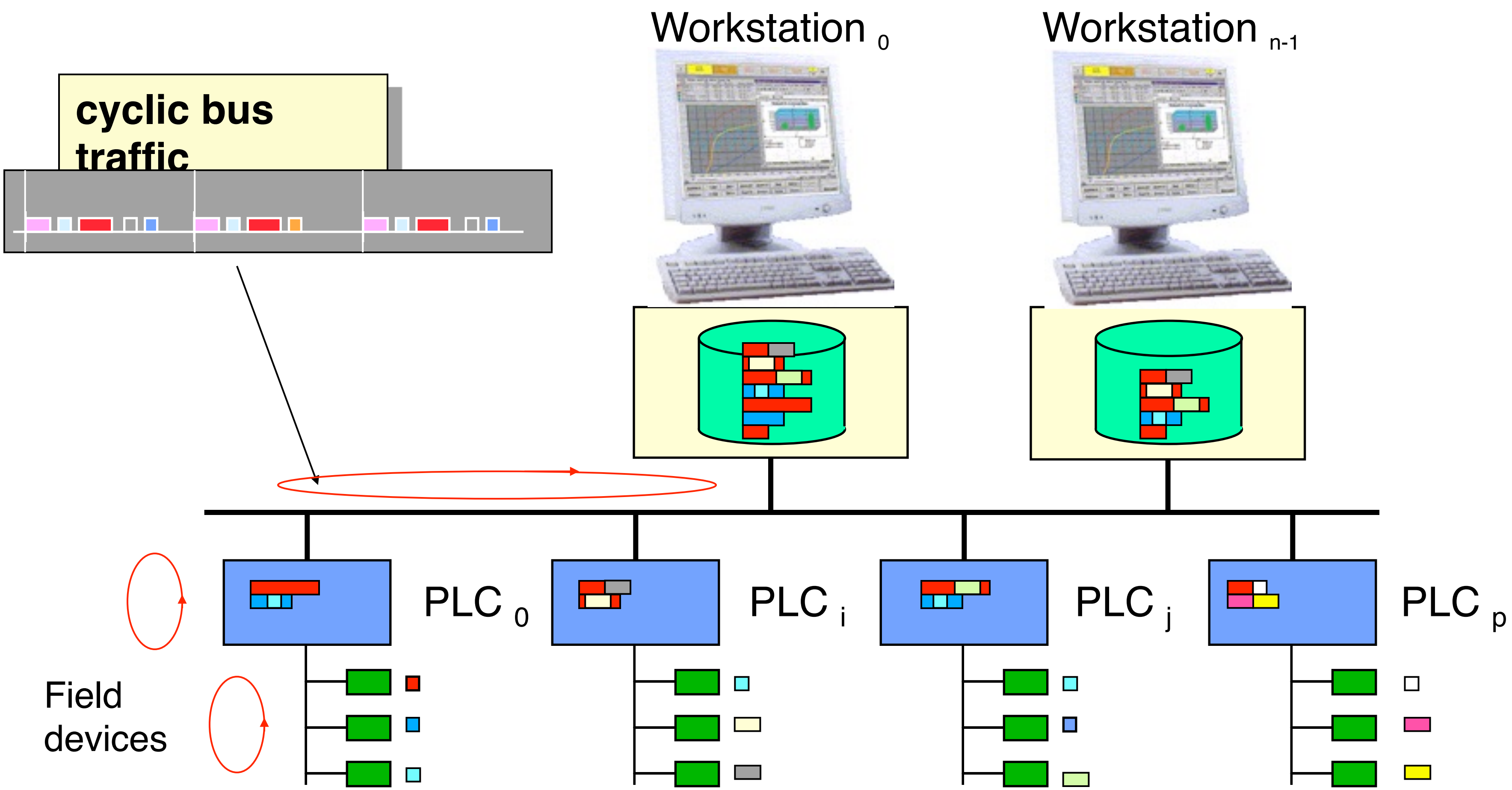
Populating the Process Data Base

Process data represent the current <u>state</u> of the plant.
Older values are irrelevant and are overwritten by new ones ("écrasées", überschrieben)

Process data are actualized either by
- polling (the screen fetches data regularly from the database (or from the devices)
- events (the devices send data that changed to the database, which triggers the screen)



Cyclic operation

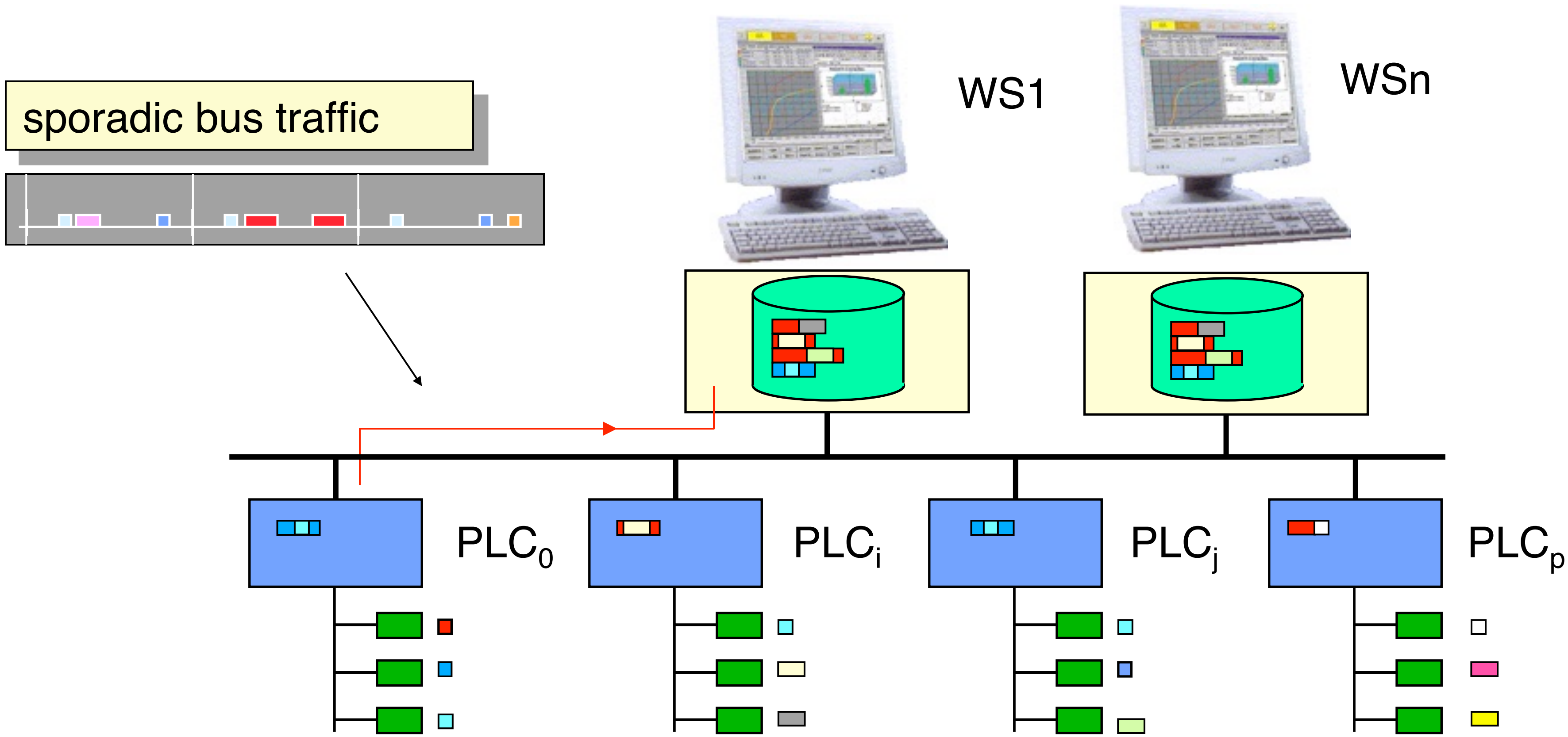


Each station broadcasts cyclically all its variables: the control bus acts as an online database
Datasets are replicated by broadcast to any number of destinations

Advantage: real-time response guaranteed

Drawback: bus bandwidth may become insufficient with large number of urgent data

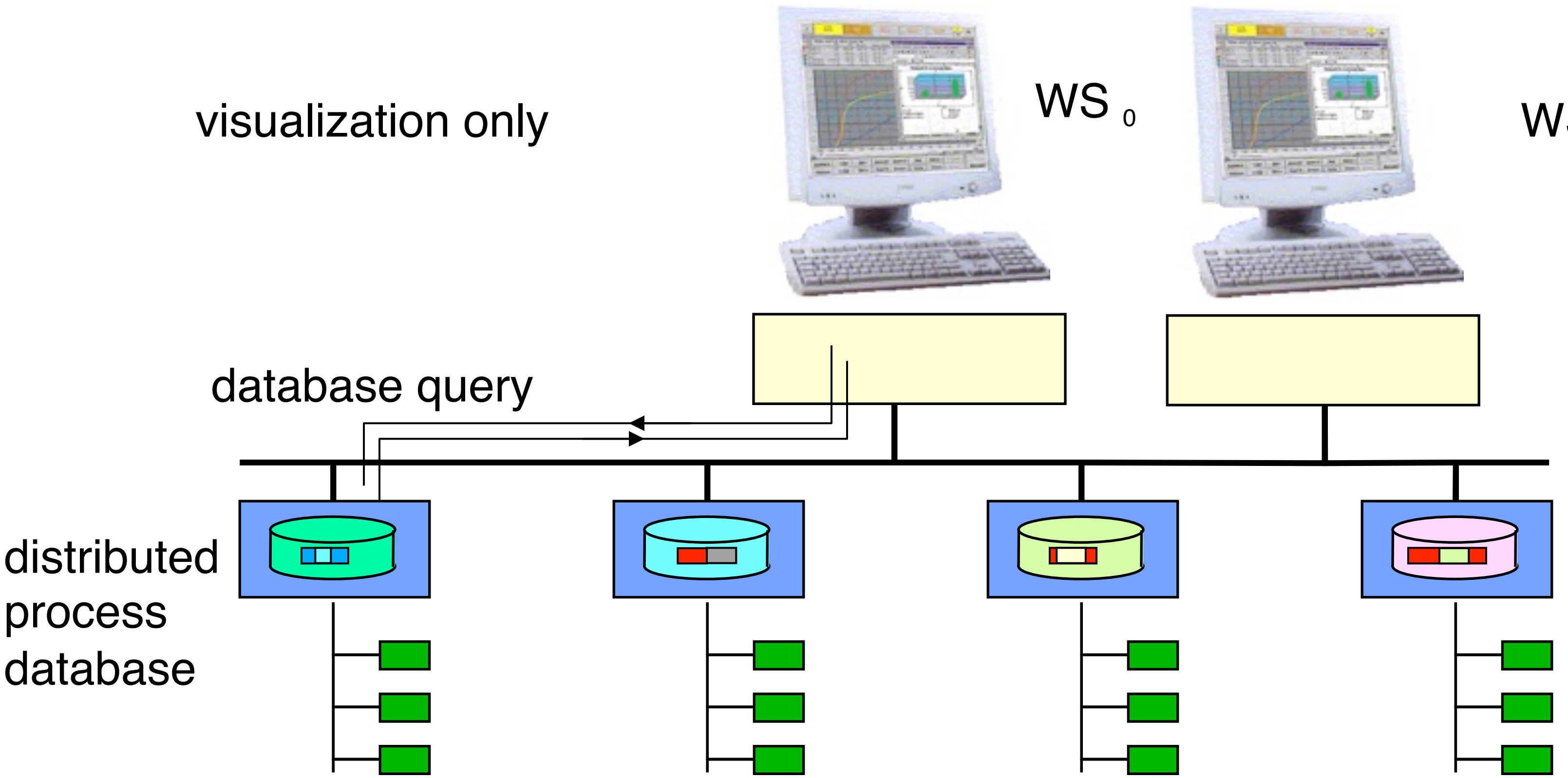
Event-driven operation



Every PLC detects changes of state (events) and sends the new value over the bus
Each operator station receives and inserts data into its local database
Data are readily available for visualization
Multiple operator workstations could be addressed in multicast (acknowledged) or broadcast

Drawback: consistency between databases, bus traffic peaks, delays

Subscription principle



To reduce bus traffic, the operator stations indicate to the controllers which data they need.
The controllers only send the required data.
The database is therefore moved to the controllers
The subscription can be replaced by a query (SQL) - this is ABB's MasterNet solution

Human-Machine Interface for Process Operation

Representation of process state	• Lamps, instruments, mimic boards • Screen, zoom, pan, standard presentation • Actualization of values in the windows • Display trends and alarms • Display maintenance messages
Protocol of the plant state	Recording process variables and events with time-stamp
Dialog with the operator	Text entry, Confirmation and Acknowledgments
Forwarding commands	Push-buttons, touch-screen or keyboard
Record all manipulations	Record all commands and especially critical operation (closing switches)
Mark objects	Lock objects and commands
Administration	Access rights, security levels
On-line help	Expert system, display of maintenance data and construction drawings, internet access

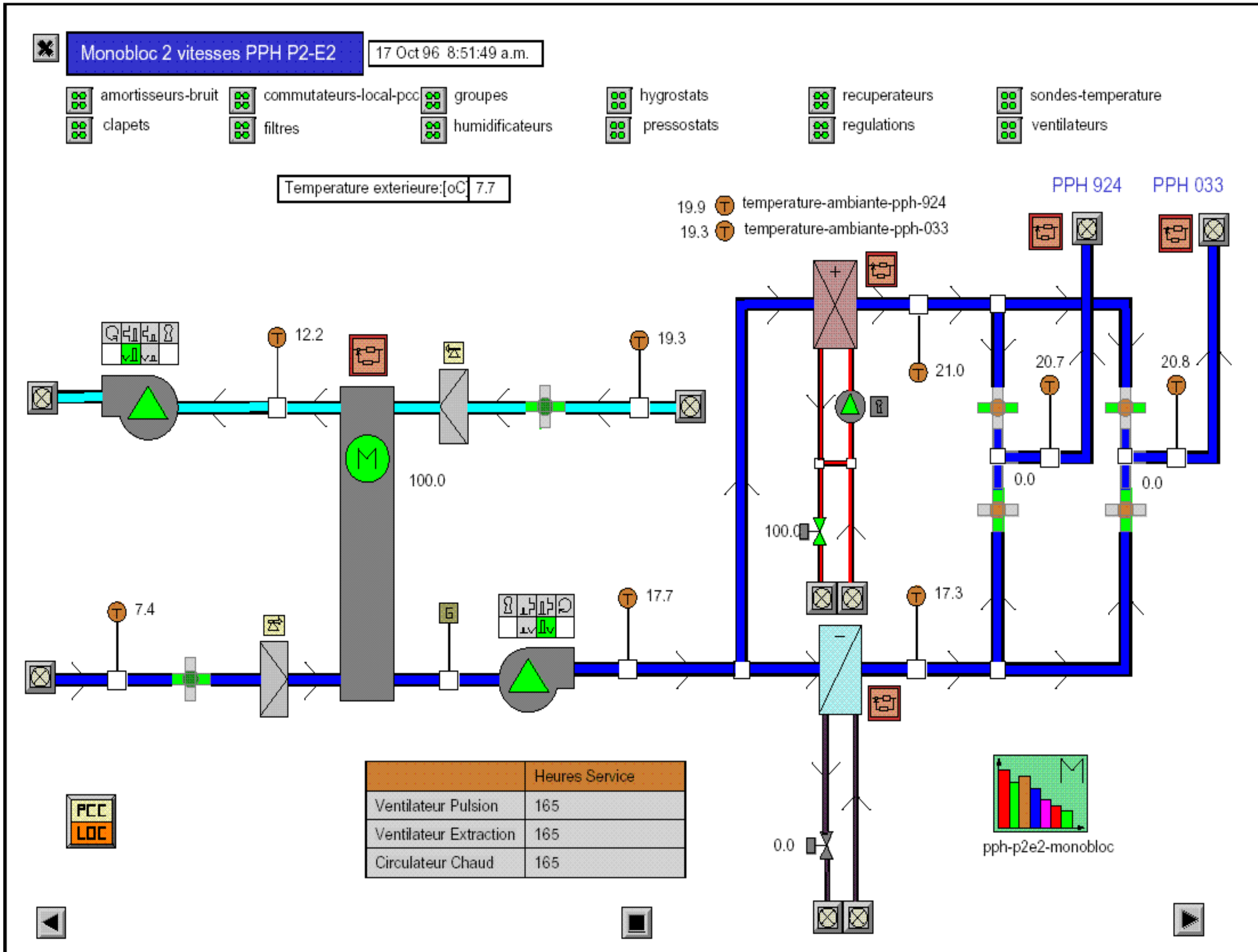
Human-Machine Interface for Engineering

Configuration of the plant	• Bind new devices • Assign names and addresses to devices • Program, download and debug devices
Screen and Keyboard layout	Picture elements, Picture variables, assignment of Variables to Functions
Defining command sequences	Command language
Protocol definition	What is an event and how should it be registered ?
Parameterize front-end devices	Set points, limits, coefficients
Diagnostic help	Recording of faulty situations, fault location, redundancy handling

Mainly used during engineering and commissioning phase,
afterwards only for maintenance and modifications of the plant.

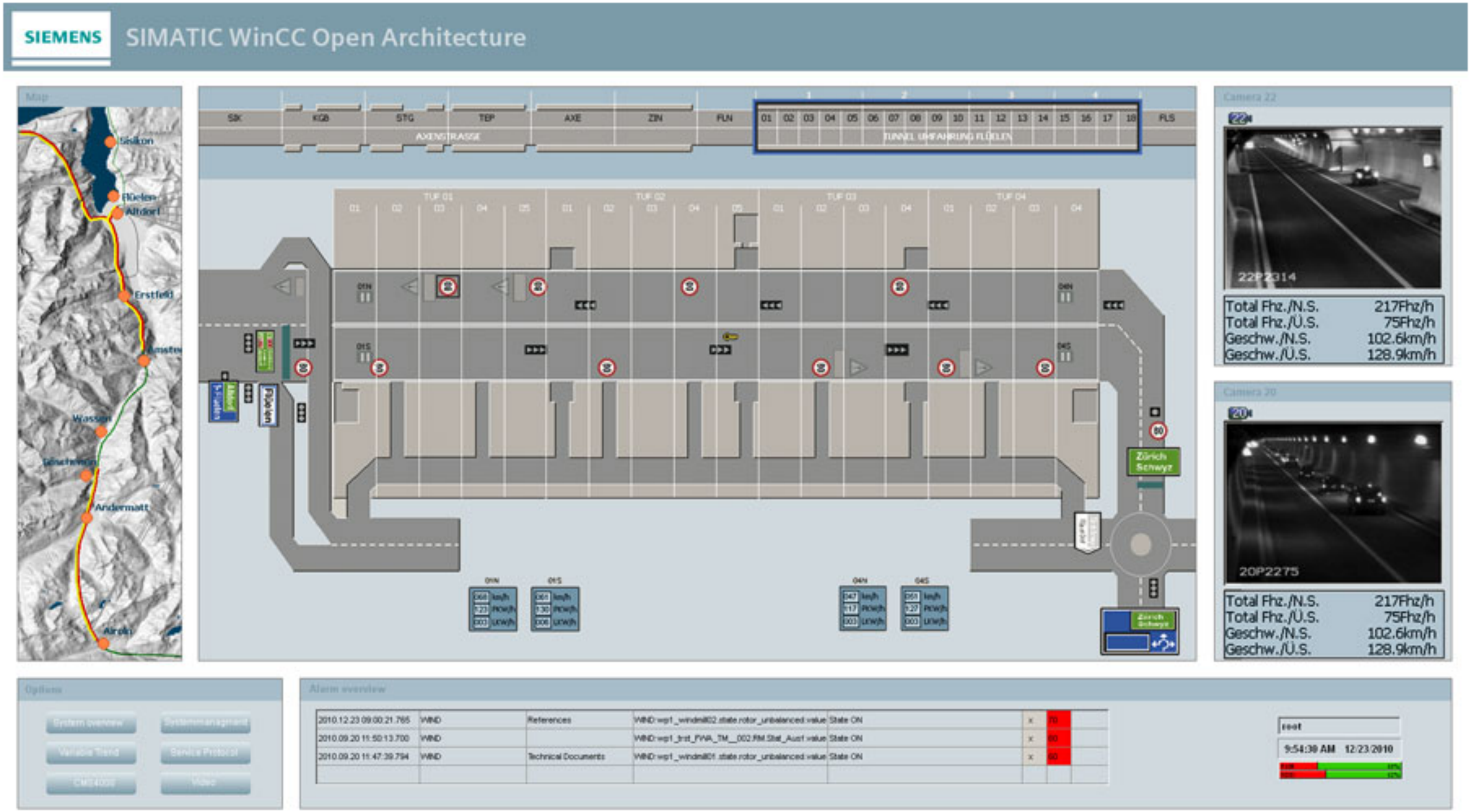
Used more often in flexible manufacturing and factory automation.

HMI Example - EPFL air condition

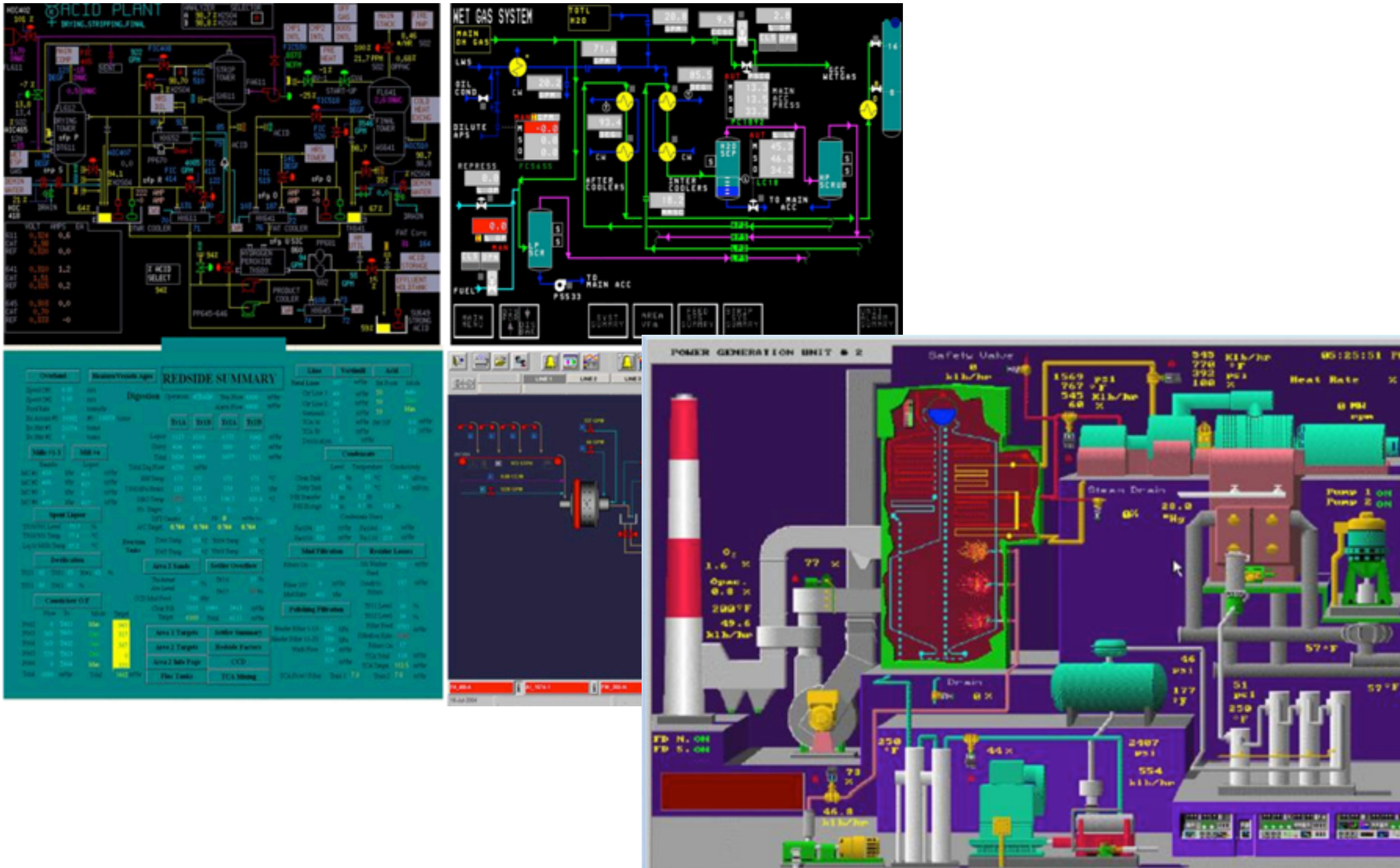


	Heures Service
Ventilateur Pulsion	165
Ventilateur Extraction	165
Circulateur Chaud	165

HMI Example – Tunnel Traffic Supervision



More Common HMI Examples



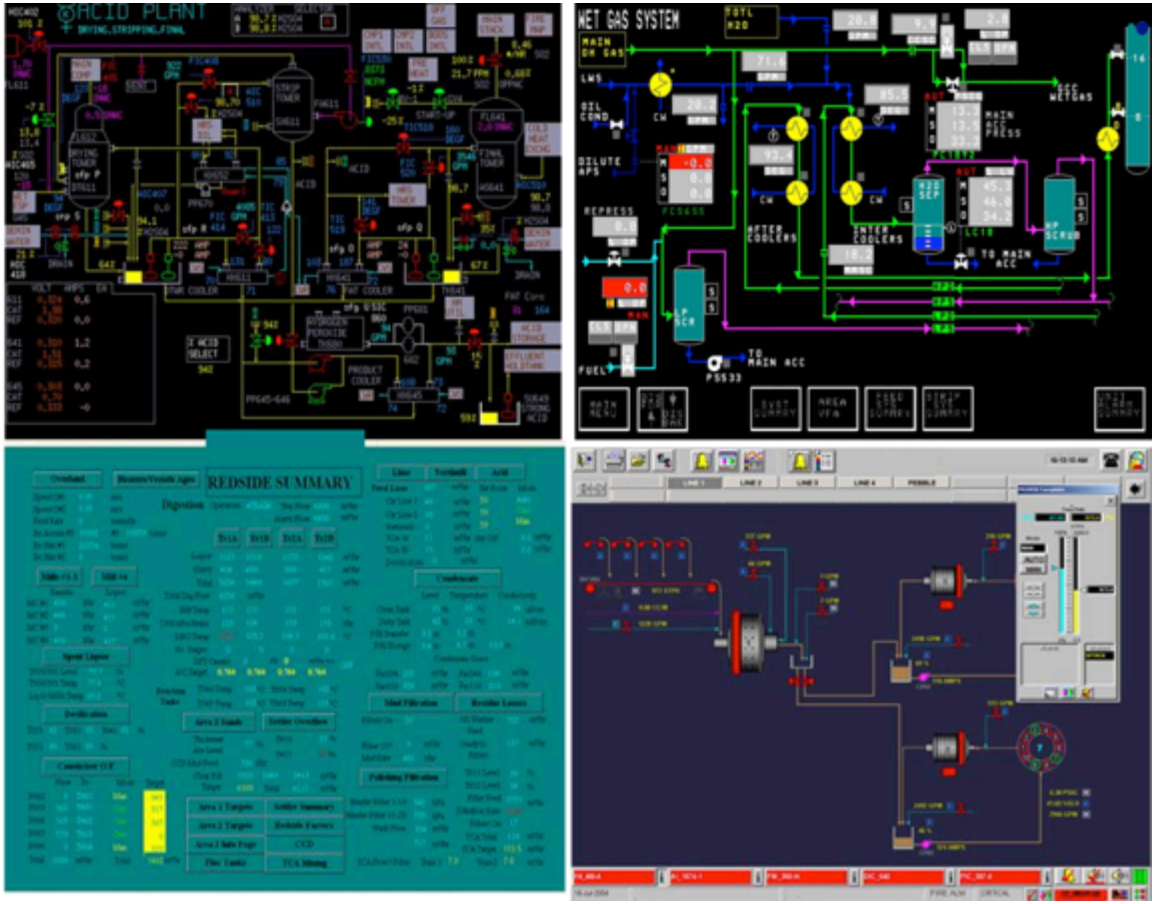
Importance of a well designed HMI

Study by Nova Chemicals and ASM® Consortium

Task	With "Traditional" HMI	With High Performance HMI	Improvement
Detecting Abnormal Situations Before Alarms Occur	10% of the time	48% of the time	A 5X increase
Success Rate in Handling Abnormal Situation	70%	96%	37% over base case
Time to Complete Abnormal Situation Tasks	18.1 min	10.6 min	41% reduction

Common HMI Design Mistakes

- **Numbers sprinkled on the screen**
- **Inconsistent, improper use of colors**
- **Too many color coding**
- **No trend**
- **No condition information**
- **No global overview**
- **Inefficient use of space**
  E.g. previous screenshot only 10% of the space is used for values. 90% is just pretty pictures…



Data Is Not Information - Example

Blood Test Results	
Test	Results
HCT	31.7%
HGB	10.2 g/dl
MCHC	32.2 g/dl
WBC	9.2x10^9 /L
GRANS	6.5x10^9 /L
L/M	2.7x10^9 /L
PLT	310x10^9 /L

How good/bad are the results?

Data Is Not Information - Example

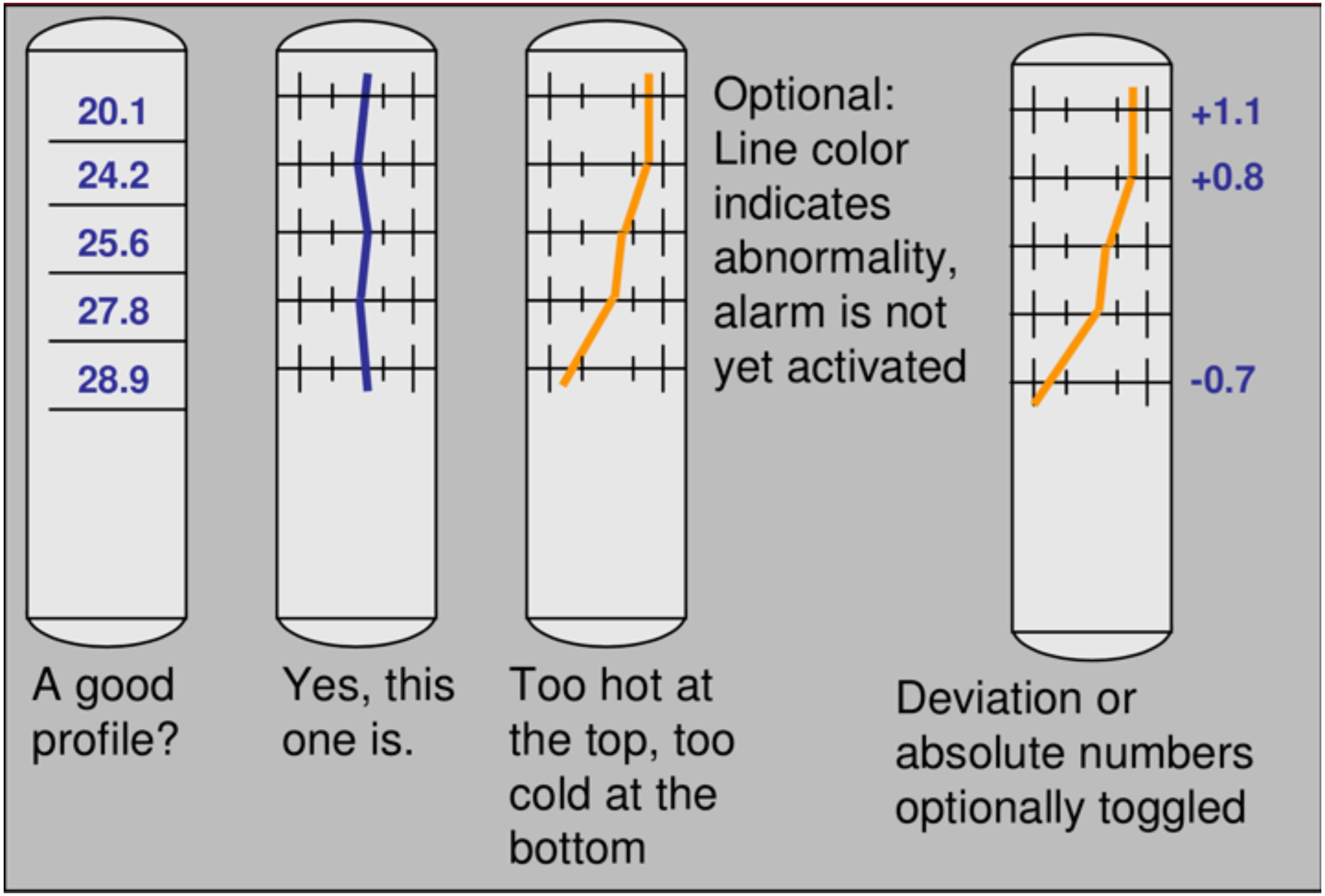
Blood Test Results		
Test	Results	Range
HCT	31.7%	24.0 – 45.0
HGB	10.2 g/dl	8.0 – 15.0
MCHC	32.2 g/dl	30.0 – 36.9
WBC	9.2x10^9 /L	5.0 – 18.9
GRANS	6.5x10^9 /L	2.5 – 12.5
L/M	2.7x10^9 /L	1.5 – 7.8
PLT	310x10^9 /L	175 – 500

Possibility to assess the results, but it still takes some time..

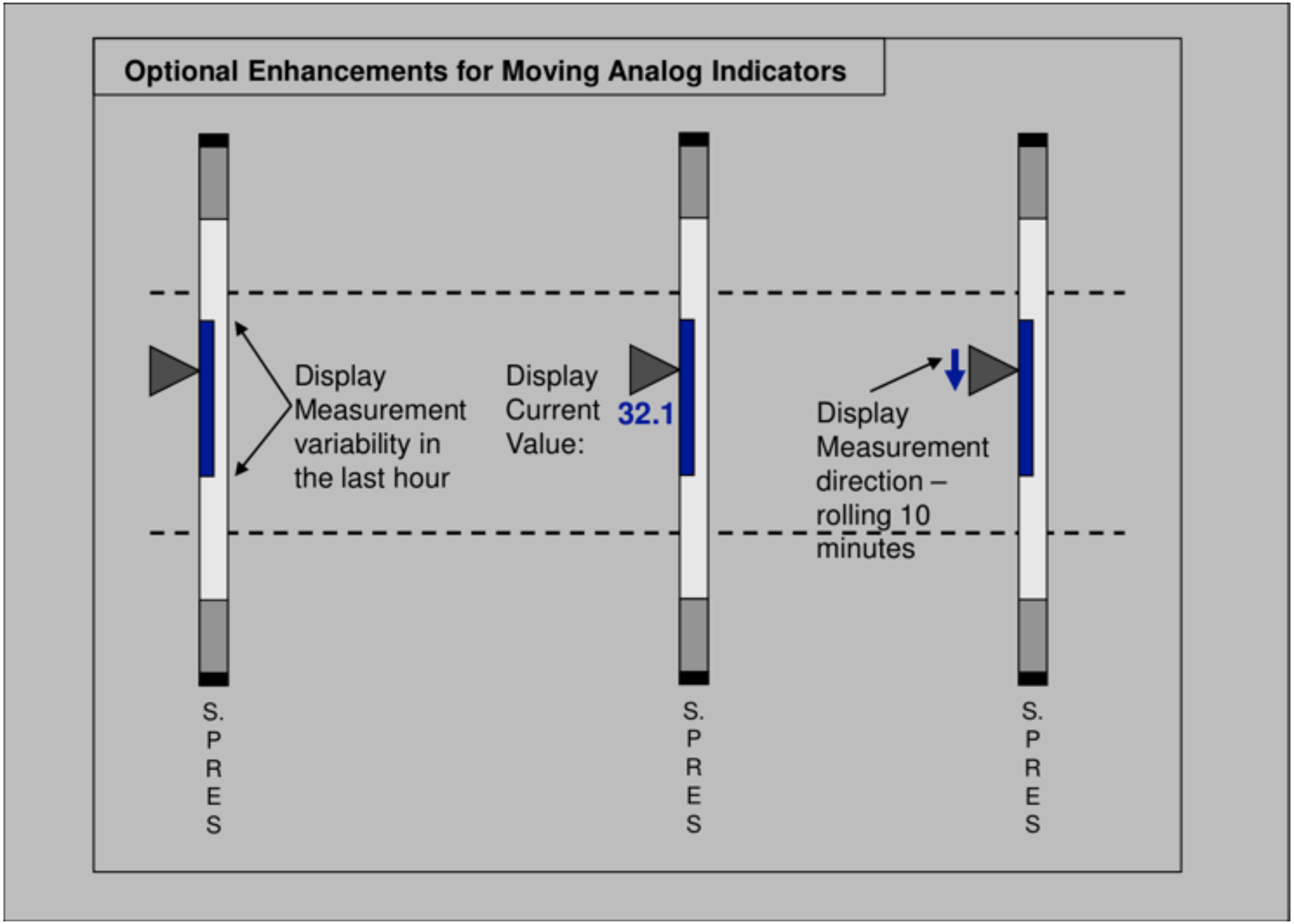
Data Is Not Information - Example

Blood Test Results			
Test	Results	Range	Indicator Low – Normal - High
HCT	31.7%	24.0 – 45.0	
HGB	10.2 g/dl	8.0 – 15.0	
MCHC	32.2 g/dl	30.0 – 36.9	
WBC	40.1x10^9 /L	5.0 – 18.9	
GRANS	6.5x10^9 /L	2.5 – 12.5	
L/M	2.7x10^9 /L	1.5 – 7.8	
PLT	150x10^9 /L	175 – 500	

Application to Industrial Examples

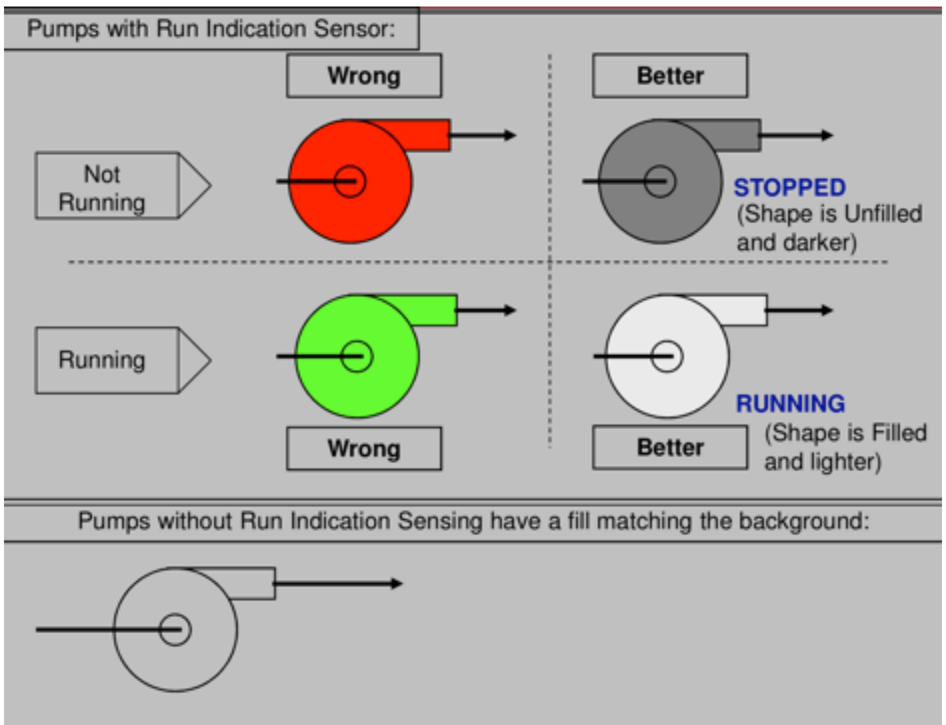


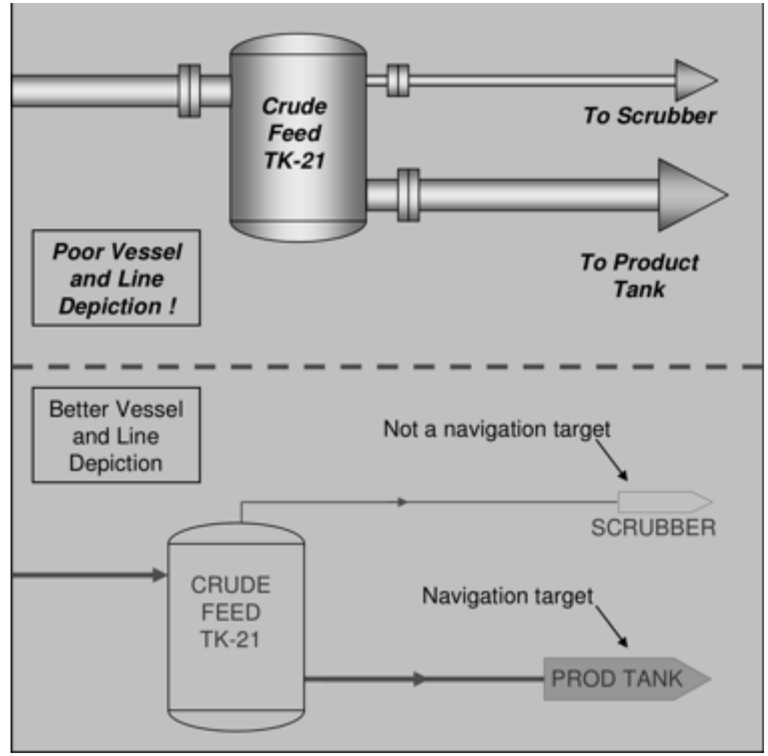
Application to Industrial Examples



Other HMI Recommendations

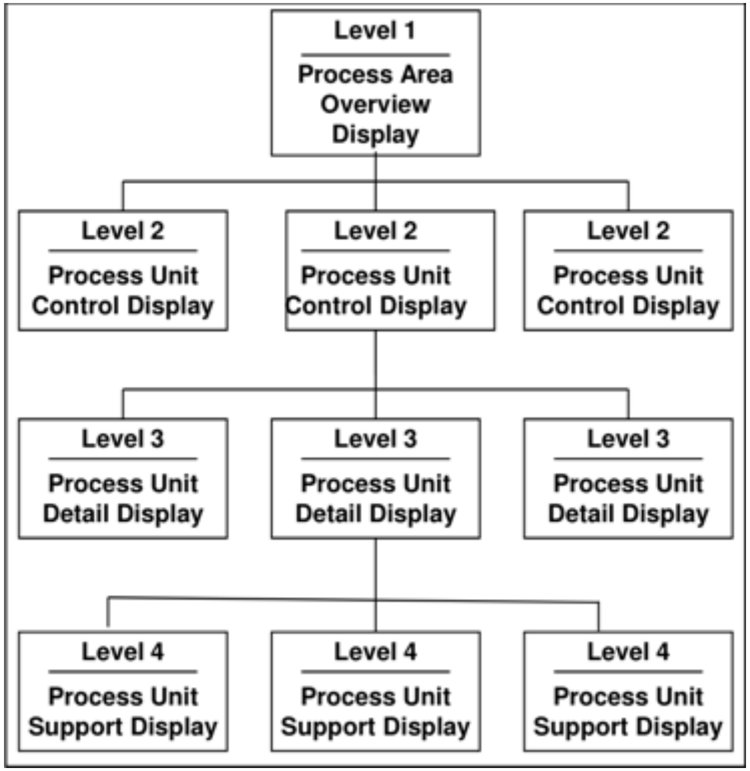
- Don't get fancy (avoid 3D objects)
- Bright/Saturated colors are for abnormal conditions only
- CAPITAL LETTERS TAKE LONGER TO READ





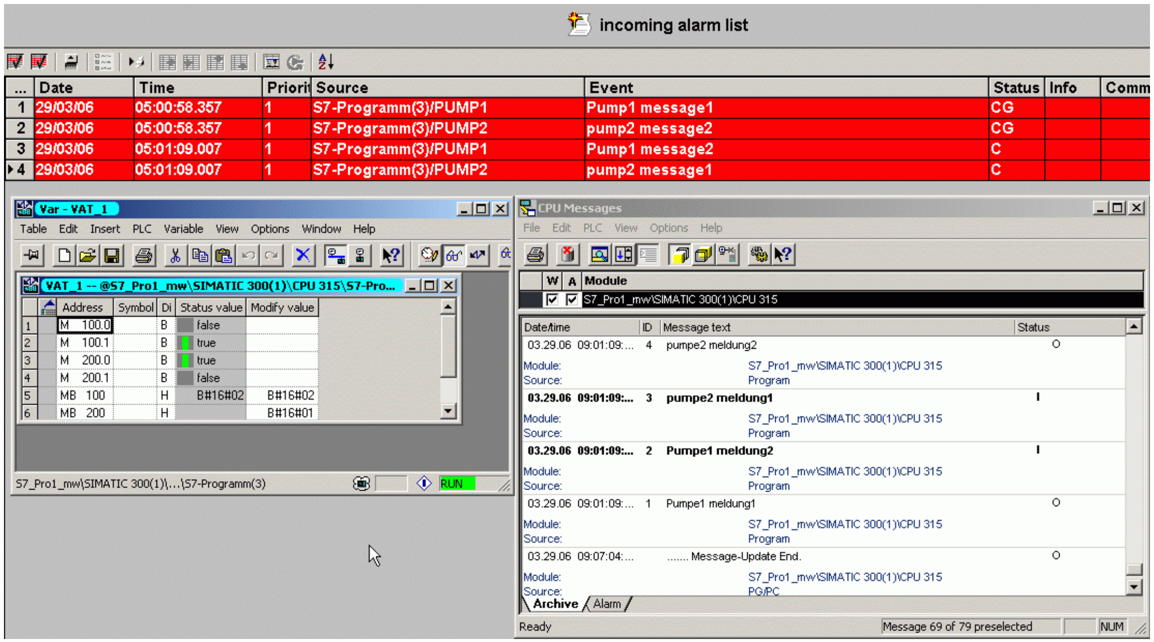
Basic Principles of HMI Design

- **Level 1 – Process Area Overview**
  - Entire operator span of control
- **Level 2 – Process Unit Control**
  - Sub-unit controlled by operator
- **Level 3 – Process Unit Detail**
  - Equipment or controller
- **Level 4 – Process Unit Support and Diagnosis Displays**
  - Interlock, single line diagram



- Proper hierarchy minimizes the number of physical screens and makes for proper navigation
- Graphics designed from P&ID will not accomplish a proper hierarchy

Alarm and Event Management



time stamps exact time of arrival (or occurrence)

categorize by priorities

log for further use

acknowledge alarms

prevent multiple, same alarms

sound alarm (different levels)

remove alarms from screen once reason disappeared (but keeps them in the log)

suppress alarms that are not meaningful (false alarms, section in maintenance)

link to clear text explanation and procedures

What is an alarm, an event ? (1/3)

A&E consider changes occurring in the plant (process) or in the control system (operator actions, configuration changes,…) that merit to be recorded.

Recorded changes can be of three kinds:

- informative: no action required

  (e.g. "*production terminated at 11:09")*

- warning: plant could stop or be damaged if no corrective action is taken "soon"

  (e.g. "*toner low*")

- blocking: the controller took action to protect the plant and further operation is prevented until the reason is cleared (e.g. "*paper jam*")

What is an alarm, an event ? (2/3)

In general, warnings and blocking alarms should be acknowledged by the operator
(”acquitter", "quittieren").

An alarm is not necessarily urgent, several levels of severity may be defined but requires an action

An event is a change related to:

- operator actions ("*grid synchronisation performed at 14:35*"),
- configuration changes ("*new software loaded in controller 21*"), and
- system errors ("*no life sign from controller B3*")

What is an alarm, an event ? (3/3)

- Alarm definition according to per ISA-18.2

An alarm is an audible and/or visible means of indicating - There must be an indication of the alarm. An alarm limit can be configured to generate control actions or log data without it being an alarm.

- To the operator

The indication must be targeted to the operator to be an alarm, not to provide information to an engineer, maintenance technician, or manager.

- an equipment malfunction, process deviation, or abnormal condition

The alarm must indicate a problem, not a normal process condition. (e.g., pump stopped ,valve closed)..

- requiring a response

There must be a defined operator response to correct the condition and bring the process back to a desired (safe and/or productive) state. If the operator does not need to respond, then the condition should not be an alarm but rather an event.

What triggers an alarm ?

- binary changes of process variables (individual bits), some variables being dedicated to alarms

- reception of an analog variable that exceeds some threshold (upper limit, lower limit), the limits being defined in the operator workstation

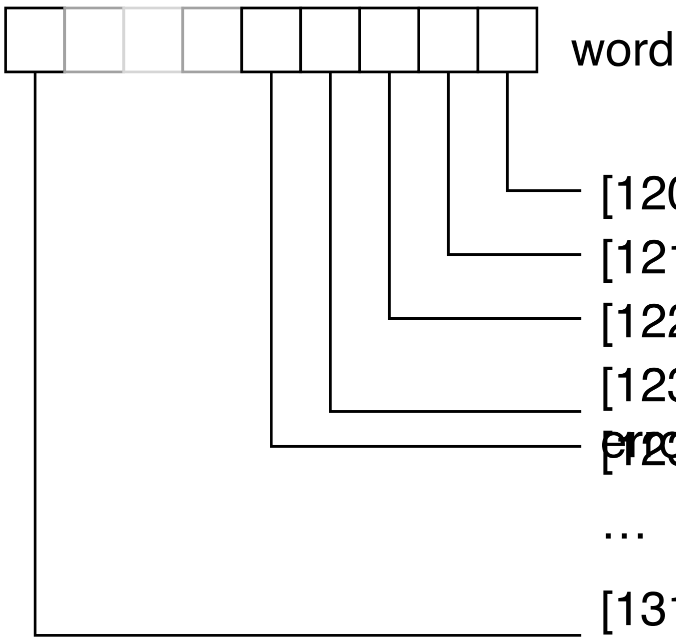
- reception of an alarm message (from a PLC that can generate such messages)

- computations in the operator workstation (e.g. possible quality losses if current trend continues)

- calendar actions (e.g. unit 233 did not get preventive maintenance for the last three months)

Implementing alarms by variables

An alarm was often encoded as a simple 16-bit word sent by an object (thru PLC) in the plant.
Each bit has a different meaning, the error condition is reset when the word is 0.



[120] low oil pressure	[120] pression huile bas
[121] low water level	[121] niveau eau bas
[122] trajectory error	[122] erreur trajectoire
[123] synchronisation error	[122] erreur synchronisation
[123] tool error	[122] erreur outil
…	…
[131] robot %R1% not ready	[131] robot %R% non prêt

This coding allows to display the error message in several national languages.
A database contains the translations.

Problem: keep devices and alarm tables in the operator workstation synchronized

Alarm Management - Examples

- Alarm is a basic and easily understood concept. However, its implementation can be ineffective and defeat its purpose.

- **Texaco Refinery Incident, Milford Haven, 1994:**
  - Alarm floods; too many standing alarms
  - Control displays and alarms did not aid operators:
    - » No process overview to help diagnosis (& see EEMUA Publication 201)
    - » Alarms presented faster than they could be responded to
    - » 87% of the 2040 alarms displayed as "high" priority, despite many being informative only
    - » Safety critical alarms not distinguished

- **Esso Longford:**
  - 300-400 alarms daily
  - Up to 8500 in upset situation
  - Alarm numbers accepted as ‘normal’
  - No engineering support on site
  - Operators did their best to meet perceived company priorities

Best practice for Alarm Management

- **Alarm reduction**
- **Correct Characterization of alarm**
  - Priority, description
  - Identification of issues
  - Remedial actions
- **Performance/Functionality of the alarm management system**
  - Responsive system
  - Filtering capabilities
  - Link to other parts of the system
    - » alarm archives
    - » Synoptic views
    - » GIS
    - » remedial actions DB

Some Standards for Alarm Management

- **ISA-18.2**
  - International Society of Automation (US)
  - Management of Alarm Systems for the Process Industries (2009)
  - Applicable to most industrial systems

- **EEMUA 191:**
  - non profit, European based, industry association
  - Consensus, good and best practice of alarm systems
  - Wide applicability to any industrial systems

- **US Nuclear Regulatory Commission**
  - NUREG/CR-6684
  - Advanced Control Room Alarm System: Requirements and Implementation Guidance
  - Addresses nuclear control system

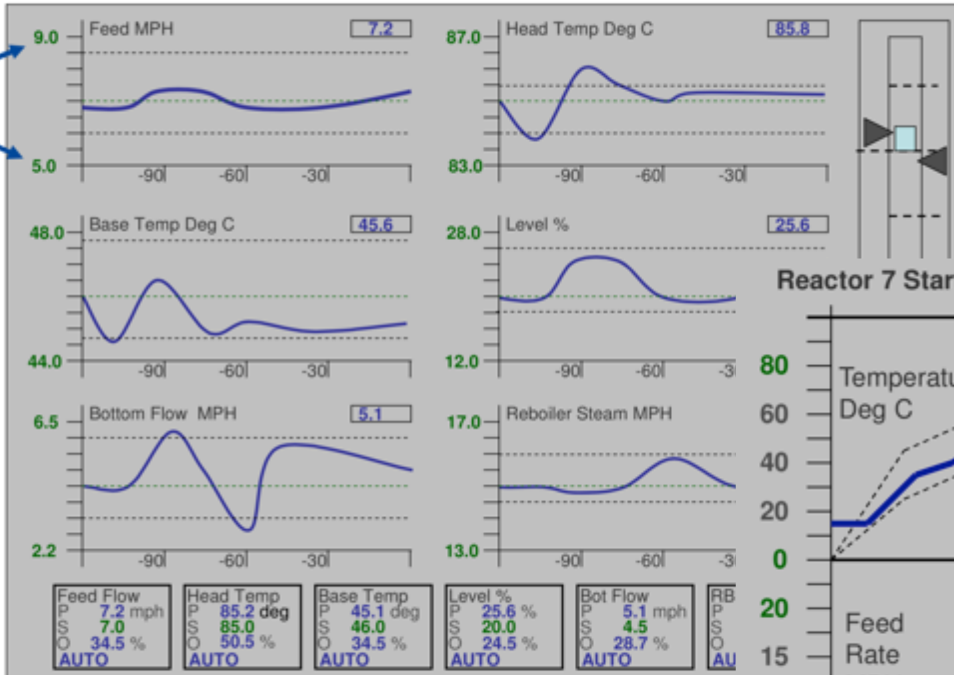
-

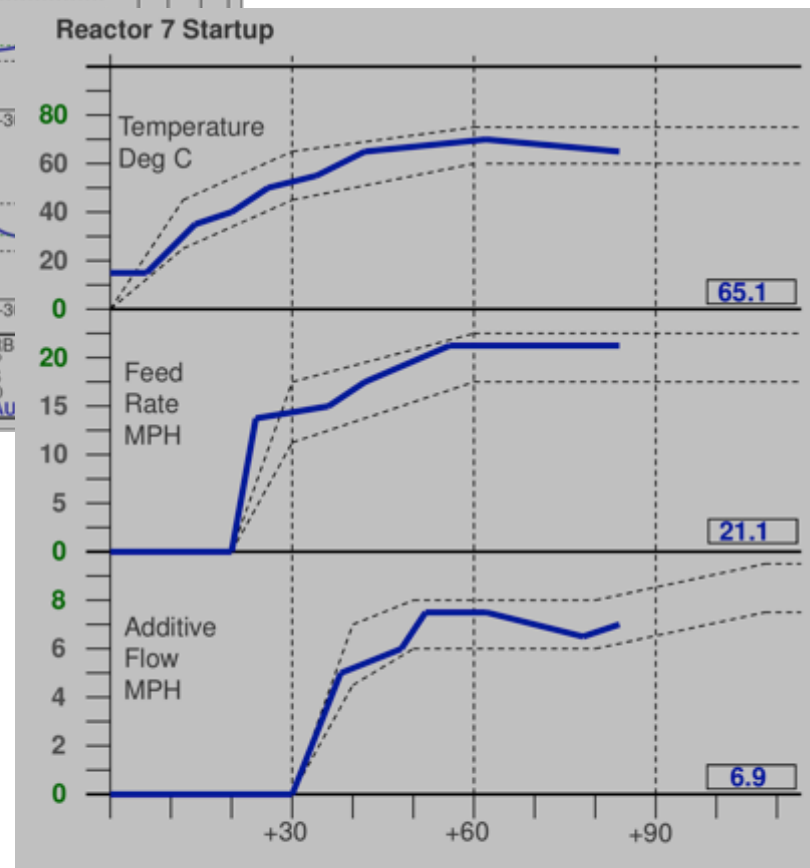
Trends

Trends allow to follow the behaviour of the plant and to monitor possible excursions.
Monitored process data (sampled or event-driven) are stored in the historical database.
Data can be aggregated for a faster display (e.g. display monthly/daily/hourly average)
Problem: size of the database (GB / month)

Trend more than values

- **Proper Auto-ranges**
- **Show boundaries of "What is good"**





- Always allow the operator to identify:
  - Where am I?
  - How far am I from the boundaries

Historian

The historian keeps process relevant data at a lower granularity than the trend recorder, but with a larger quantity.

Data from different sources is aggregated in one data base, normally using data compression to keep storage costs low.

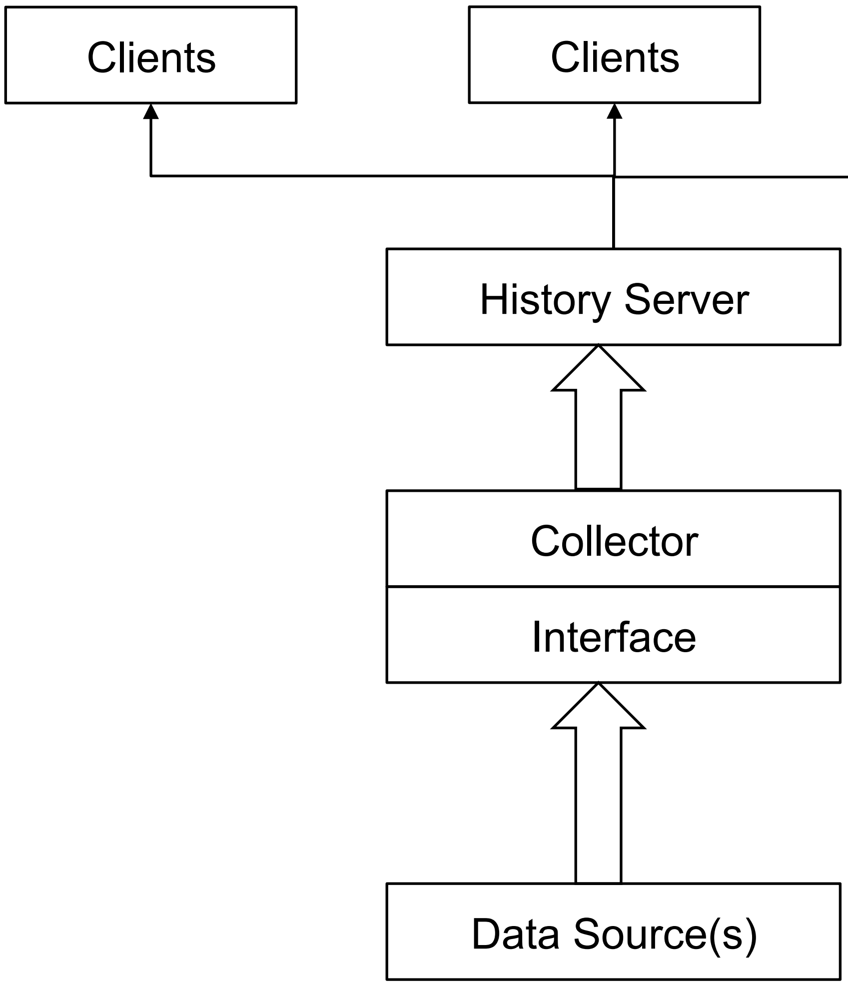
Data are analysed according to "calculation engines" to retrieve "metrics":
- performance indicators
- quality monitoring
- analysis of situations (why did batch A worked better than batch B)

Build the audit trail: "who did what, where and when"
especially in accordance with regulations (e.g. Food and Drugs Administration 's CFR 11)

Examples:

ABB's Information Manager
GE's Proficy Historian
Siemens's WinCC-Historian
OSIsoft's PI Historian

Historian – General Architecture



- Desktop analysis tools
- Other business DB

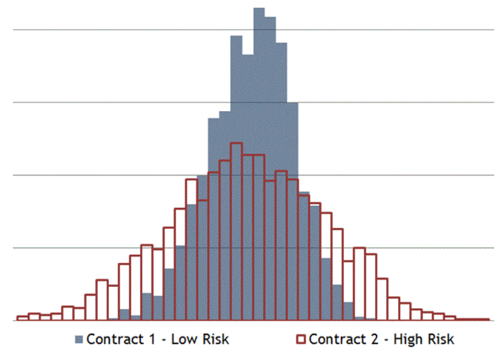
- Real-Time process history DB
- Relational process and/or tag DB
- History Engine and query server

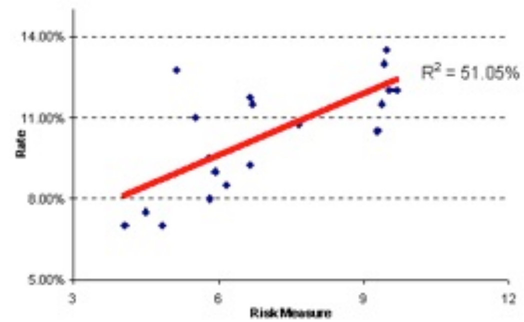
- Tag Scan Tables
- Data Buffering
- I/O Driver/Interface

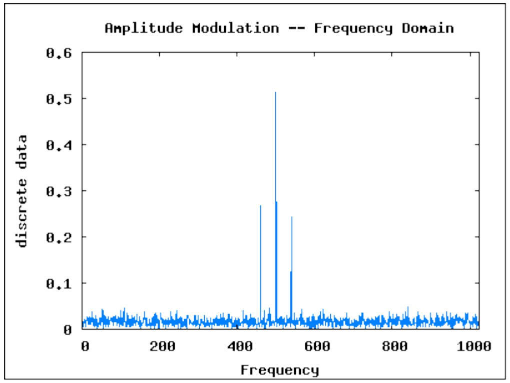
- Remote Terminal Unit - RTU
- PLC
- Distributed Control System (DCS)
- Data Acquisition Systems
- Other Databases

Historian – Examples of Analysis

- Time series plot
- Statistical plot
  - Average, Min, Max, etc. over a period
- Histogram of distribution values
- Regression and correlation
- Frequency domain analysis
- Performance indexes calculation (e.g. SAIFI, SAIDI)







Additional functions

printing logs and alarms (hard-copy)

reporting

display documentation and on-line help

email and SMS, voice, video (webcams)

access to databases (e.g. weather forecast)

optimisation functions

communication with other control centres

personal and production planning (can be on other workstations)

web-access

Engineering tools

draw the synoptic

define alarm threshold

define address to access data

bind controllers to variables

define the reports and logs

define recipes (=macros)

distribute the SCADA application (on several computers,…)

support fault-tolerance and back-ups

define interfaces to external software (SQL, SAP, etc.)

Generic visualization packages

Company	Product
ABB	Process Portal, Operator^{IT}
CTC Parker Automation	interact
Citect	CitectSCADA (AUS, ex CI technologies, www.citect.com)
Intellution (GE Fanuc)	Intellution (iFix3.0) 65000 installs, M$38 turnover
Iconics	Genesis
National Instruments	LabView, Lookout
Rockwell Software	RSView
Siemens	WinCC, ProTool/Pro
Taylor	Process Windows
TCP	SmartScreen
USDATA	Factorylink, 25000 installs, M$28 turnover
Wonderware (Invensys)	InTouch, 48000 installs, M$55 turnover

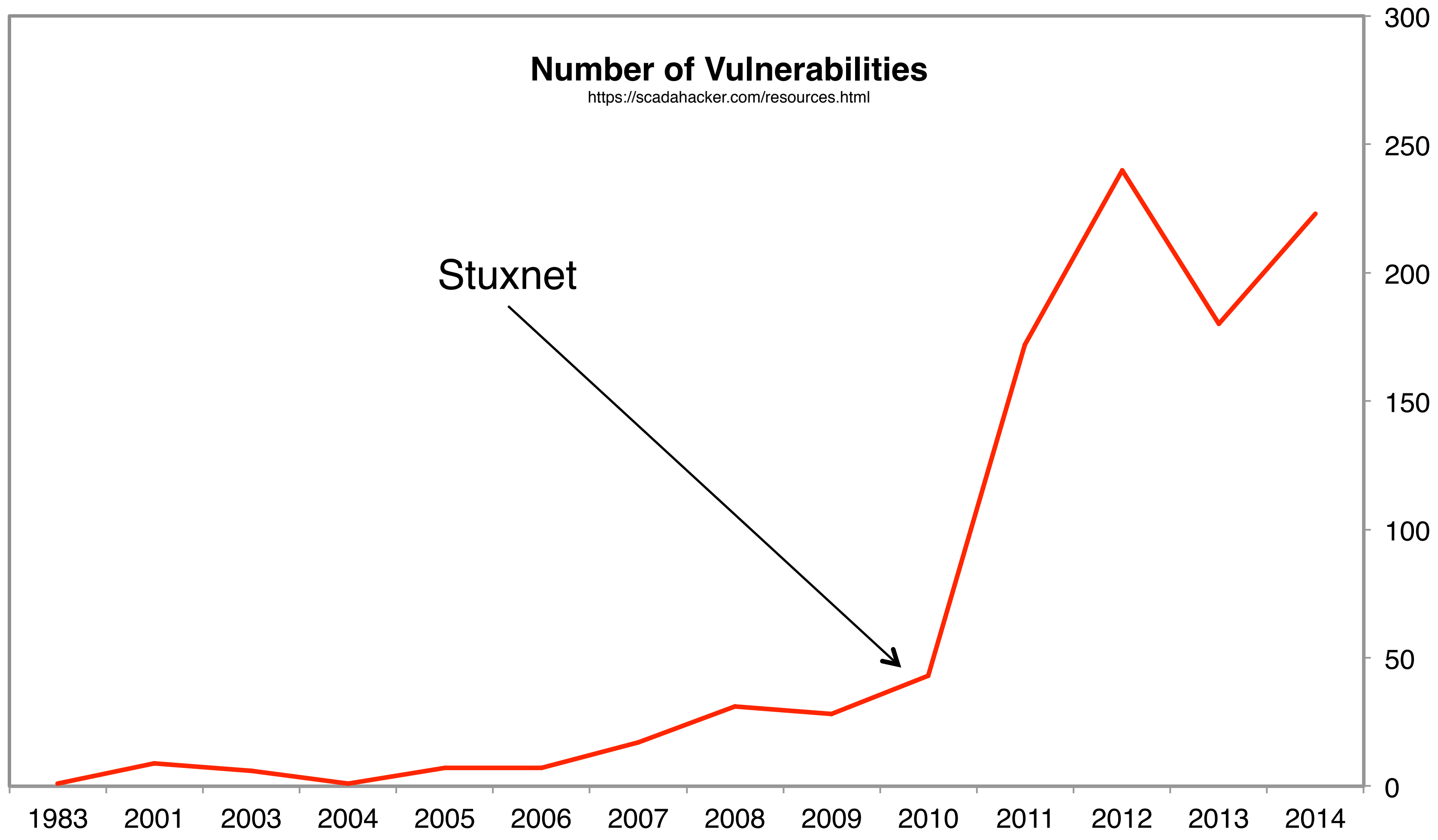
…XYCOM, Nematron, Modicon PanelMate, OIL System PI Data Historian.
Ann Arbor Technology, Axeda, Eaton Cutler-Hammer, ei3, InduSoft, Opto22, ….

Trends in SCADA

- Systems based on open-standard and COTS products
  - Used to be custom products
- Visualization of process data on mobile devices (tablets, smartphones) and webaccess
- Many protocols are now based on TCP/IP and Ethernet for acquisition
  - Used to be proprietary (serial) protocols
- Systems are getting connected to each other
  - Used to be standalone, isolated systems
- Historical database are accessible from/to the corporate network
- False sense of security because the system is “isolated”, but
  - Some acquisition devices can be far away from the SCADA
    - » Need for third party communication infrastructure, e.g. satellite, phone lines, etc.
  - Maintenance operations are still needed
    - » A single maintenance laptop connected to the acquisition network can have access to all devices
- Since Stuxnet, cyber-security in SCADA starts to be a real concern

Cyber-Security and SCADA

Trends in SCADA



Attacks Against SCADA

- Denial of Service
  - Attack to overload the SCADA server or any of the acquisition devices
  - Lost of supervision/control
- Delete System File
  - Lost of certain functionalities
  - May not be noticeable immediately
- Plant a trojan
  - Take control of a plant
- Log keystroke
  - Get operator login and password
- Log any company sensitive operation
  - Loss of competitive advantage
- Change data point value to force a plant shutdown
- Use SCADA as a launching point to attack other systems in the corporate network
- Etc.

SCADA Security Strategies 1/2

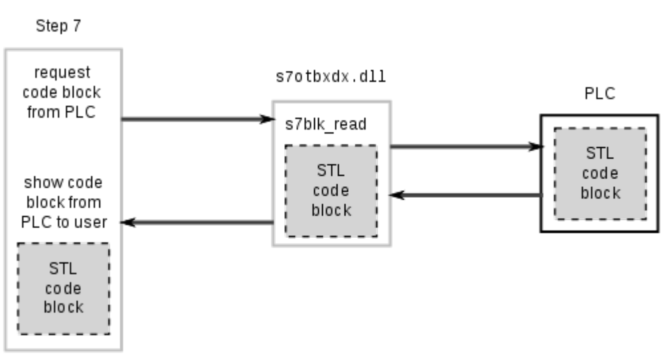
- Laptop and removable drive
  - No personal computer on the process/technical network
  - No remove drive
- Default login/passwords
  - Change/disable them
- Ring of defense
  - Subdivise subnetwork to limit the consequence of a compromise
- Authentication
- Encryption
- Security Assessment as part of the periodic maintenance process

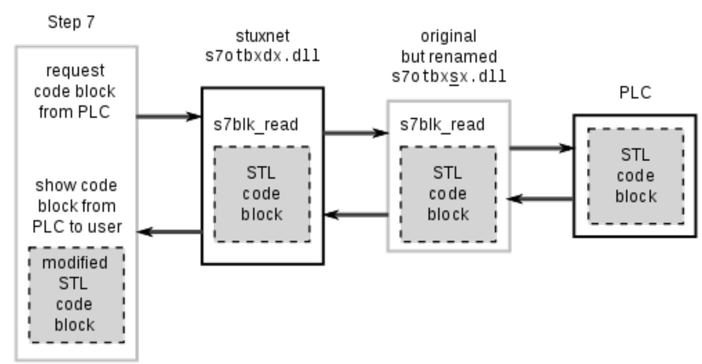
SCADA Security Strategies 2/2

- Defense in depth
  - Identification, Classification and Categorization
  - Electronic Security Controls and Measures
  - Physical Security Controls and Measures
  - Security Review/Audits
  - Incident Response Training
- Be aware of new vulnerabilities and apply patches
  - Vulnerability Databases
    - » ICS-CERT, NVD, CVE, Bugtraq, OSVDB, Mitre Oval Repositories, exploit-db, Siemens Product CERT
- Know the security standard applicable to the industry
  - E.g. IEC 62351 for most protocols used in power system industry
  - E.g. Transportation Security Administration (TSA), Pipeline Security Guidelines, April 2011
  - NERC (power industry), NIST, NRC (nuclear plant)

Case Study

- Stuxnet
  - Worm discovered in June 2010
  - Targeted nuclear facilities
  - Initially spread through USB keys
  - Spreads via Windows using 4 0-day vulnerabilities, but targets PLC
  - Man in the middle attack:
    - » sends fakes sensor values so the system does not shutdown when abnormal situation is encountered





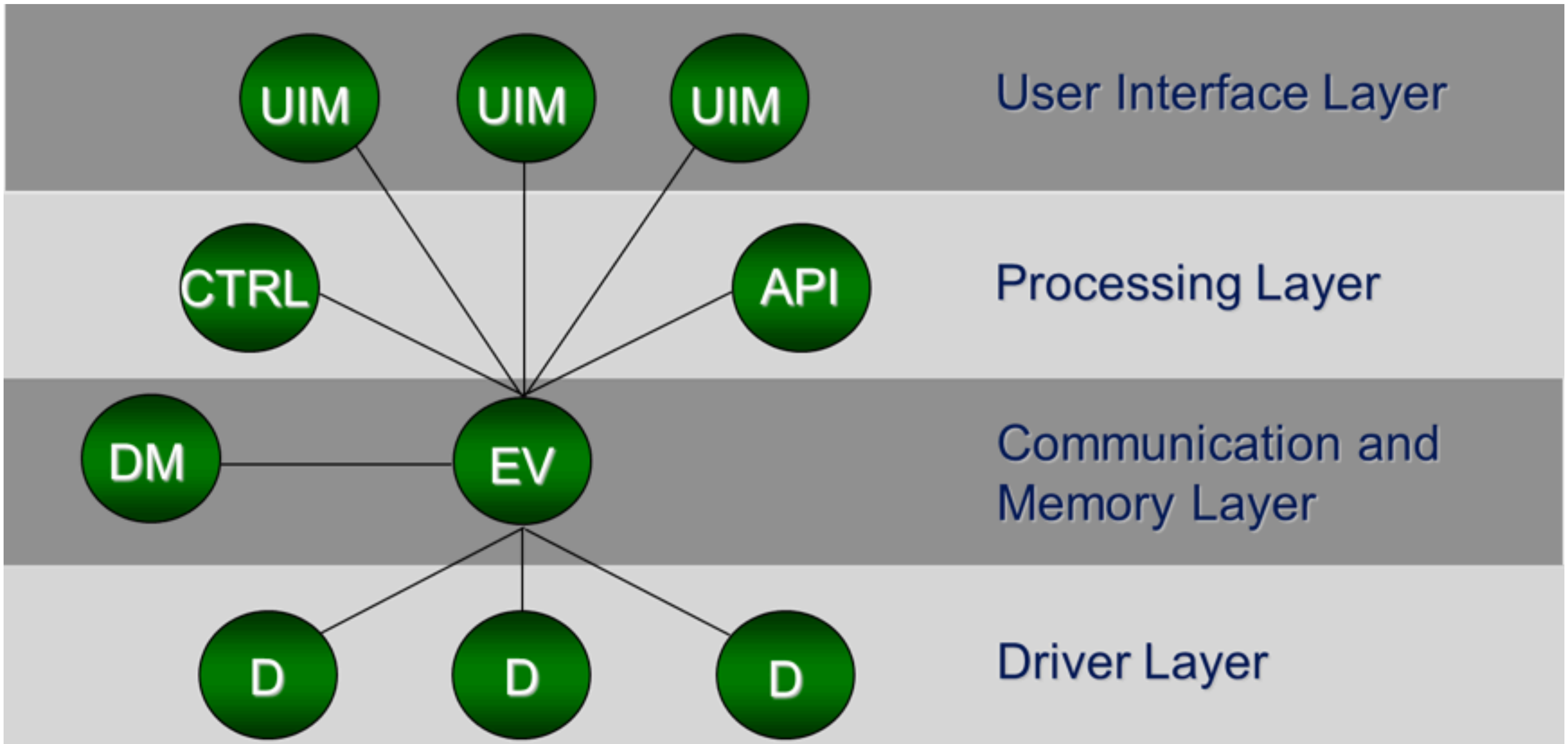
Source: Wikipedia – March 2012 - http://en.wikipedia.org/wiki/Stuxnet

Examples of SCADA Systems

WinCC OA - Introduction

- **SIMATIC WinCC Open Architecture** is a Siemens product
- Basis of most supervision systems at CERN
- Framework to build a SCADA system
  - Not bound to any domain
  - Include main traditional SCADA functionalities:
    - Engineering (device creation, device settings, etc.)
    - Acquisition (OPC, IEC 104, etc.)
    - Alarm handling, display, filtering
    - Archiving, trending, logging
    - User Interface
    - Access Control
  - Does not include domain specific applications
    - E.g. State estimation of power system network, load forecasting, etc.
- Based on the notion of managers
  - Event manager, archive, driver, control, etc.

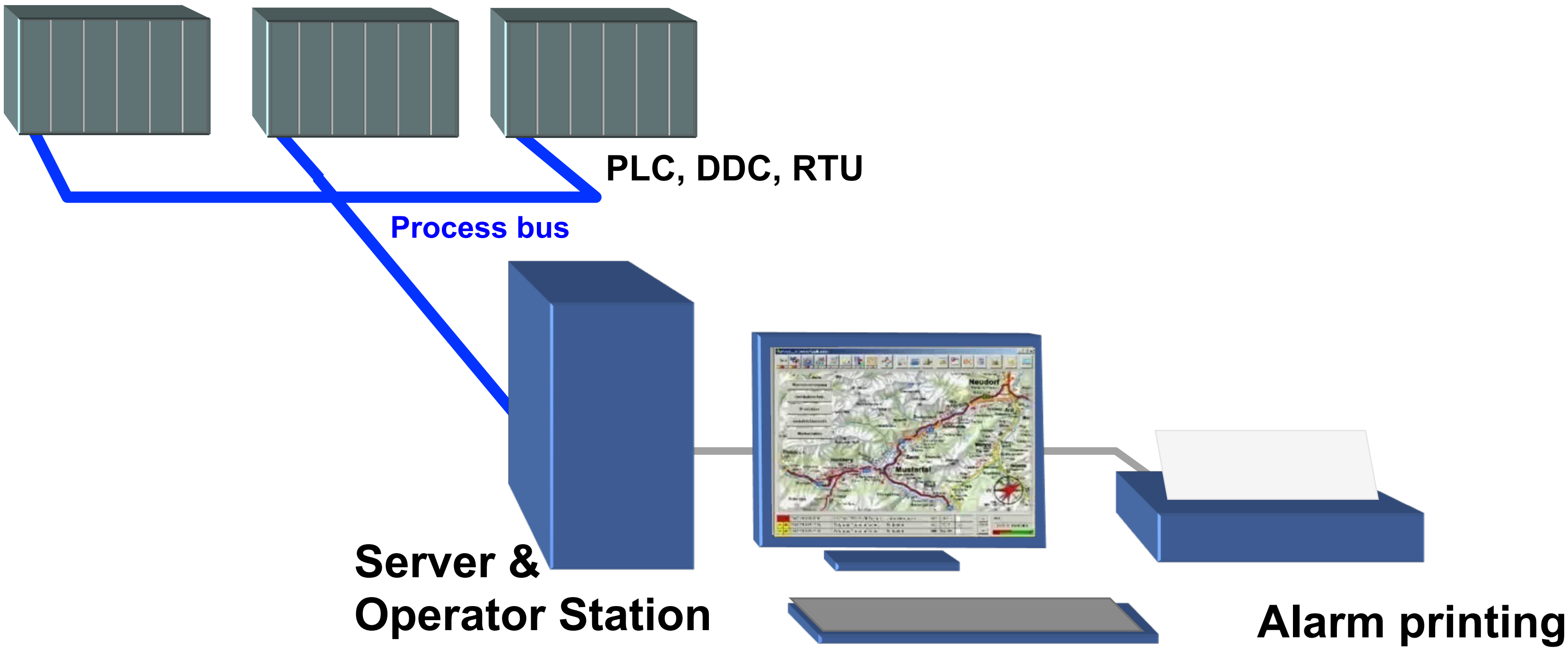
WinCC OA - Managers



Copyright – WinCC OA ETM Siemens

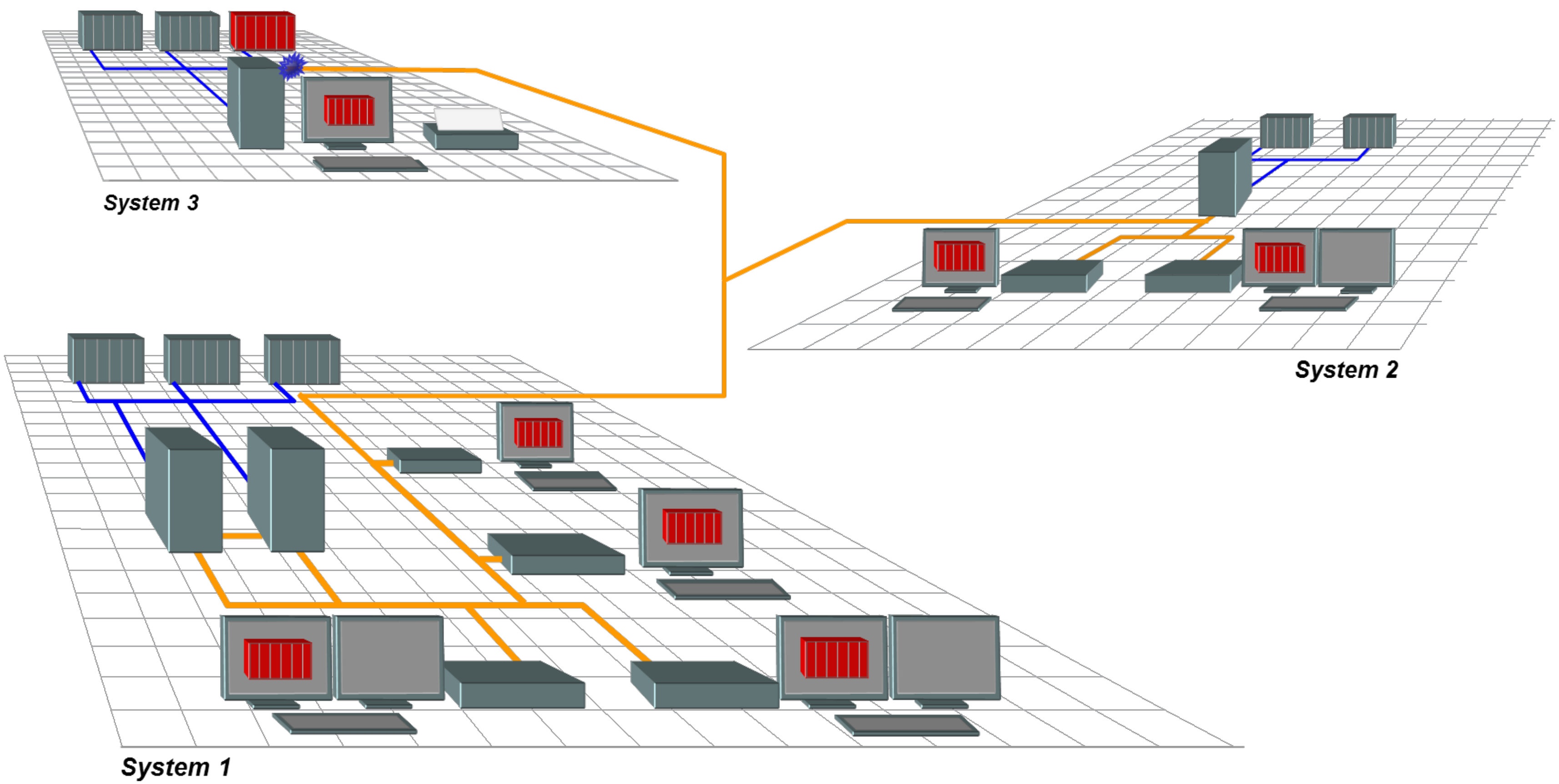
WinCC OA - Architectures

- **Single Machine System**
  - All managers run on the same machine
  - Server is also the operator workstation
  - Pros: simple, fit for small system
  - Cons: does not scale, low availability



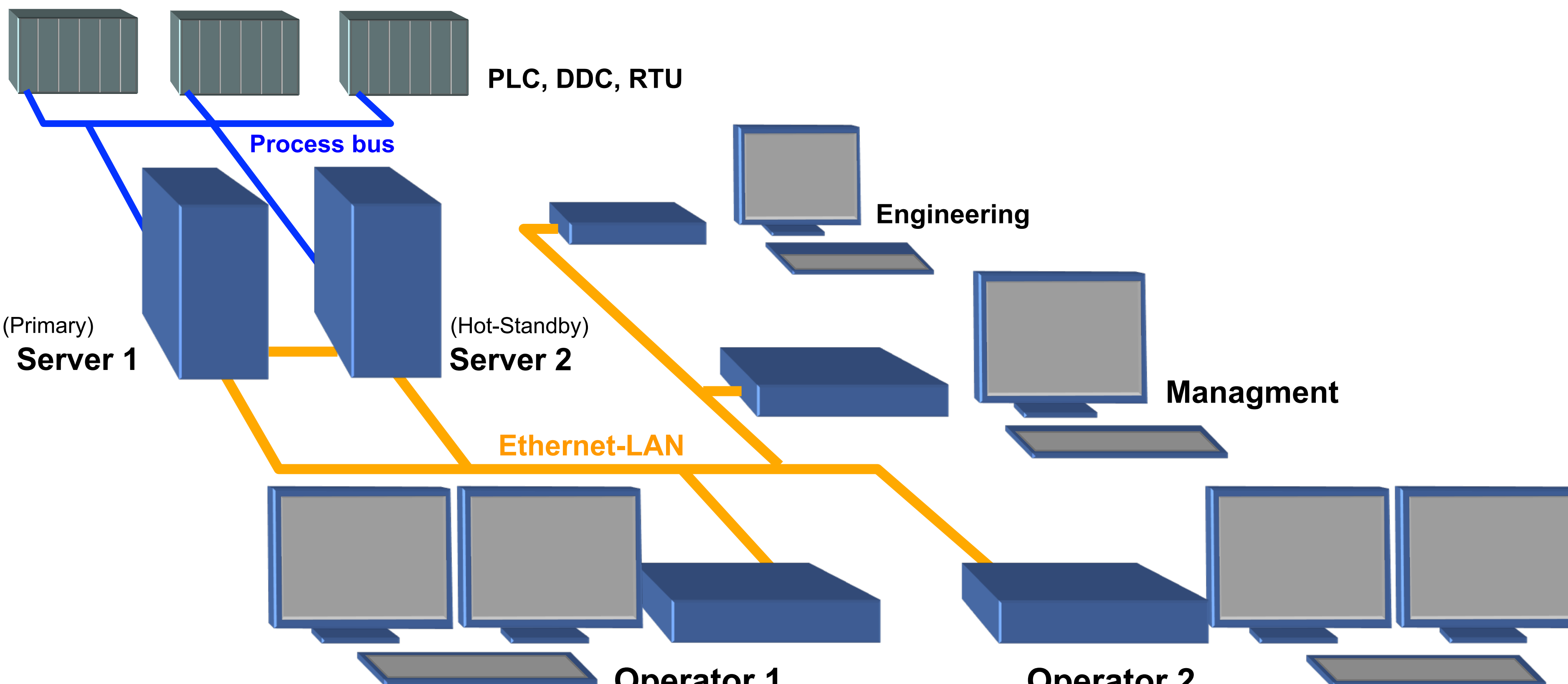
WinCC OA - Architectures

- **Distributed System**
  - Two or more systems are connected via a network
  - Each system can display data from other systems

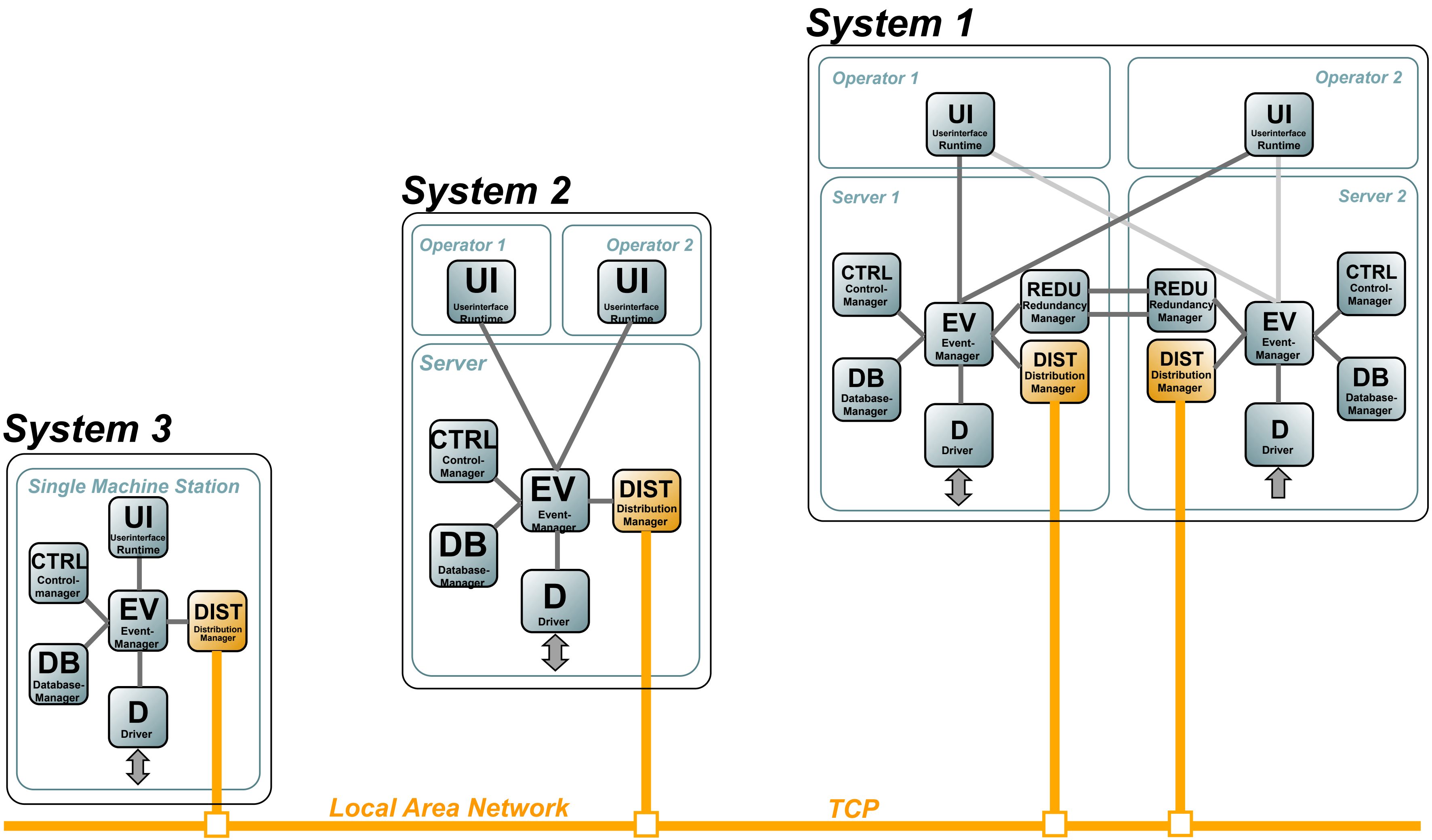


WinCC OA - Architectures

- **Redundant System**
  - Hot/Standby redundancy
  - Automatic switchover of all operator workstations
  - Split mode capability

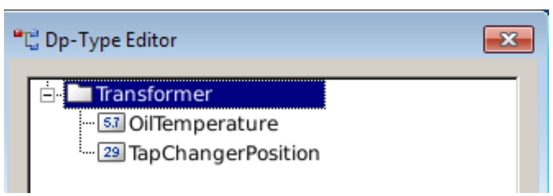


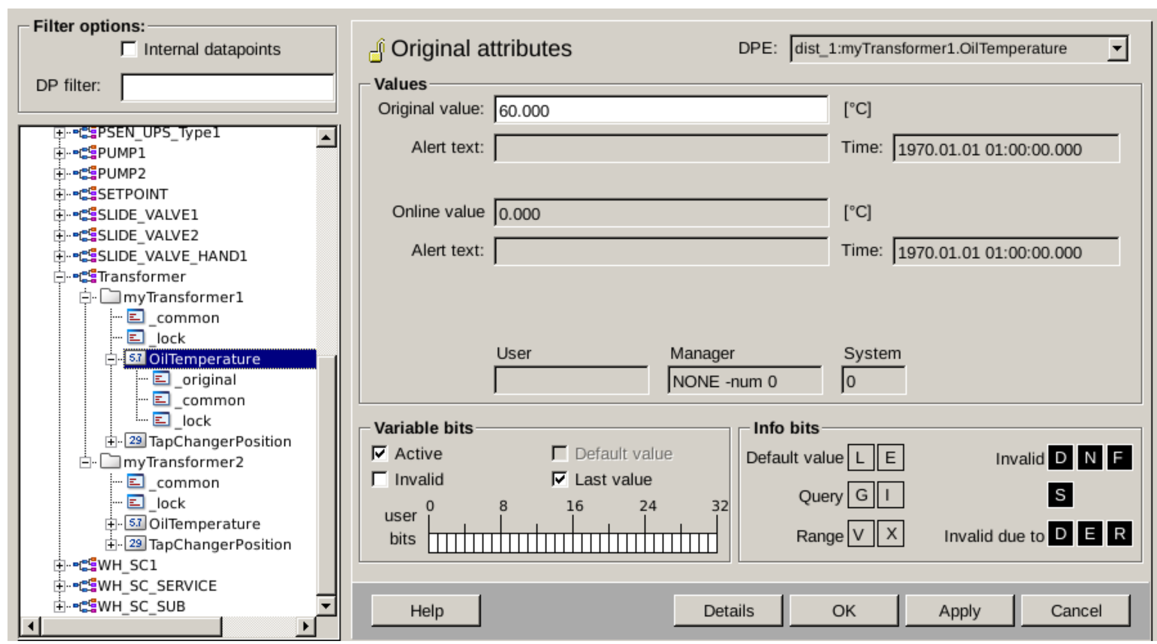
WinCC OA – Architectures Overview



WinCC OA – Process Data Base

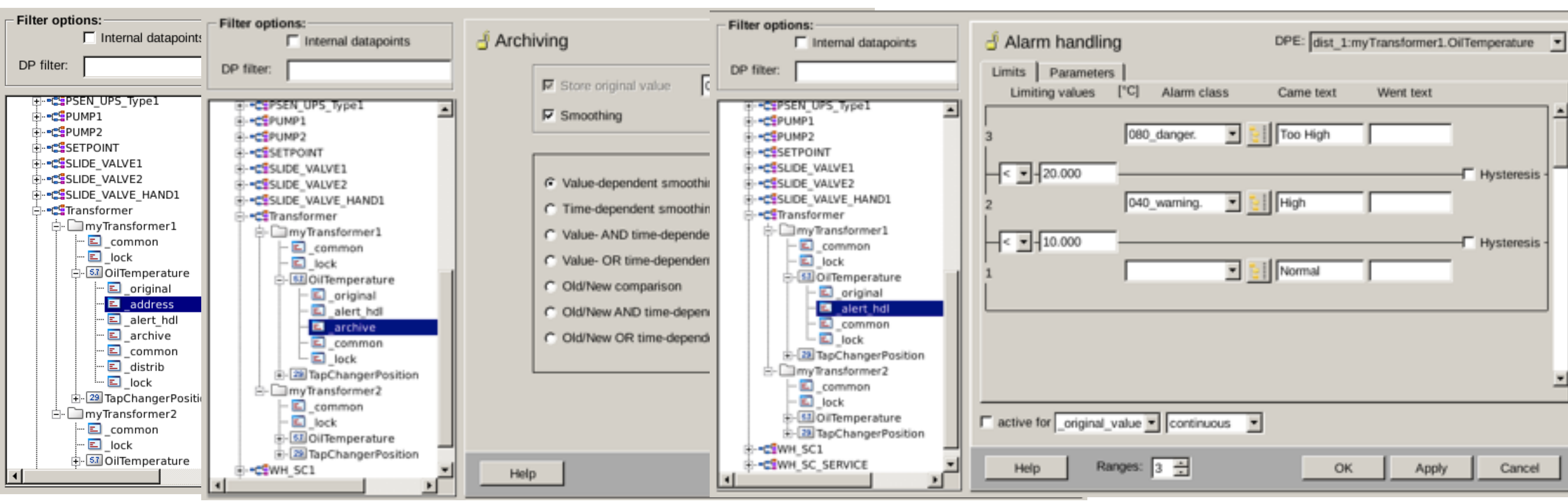
- Process DB is based on the concept of object
  - A field device is represented by DP (data point) which is an instantiation of a DPT (data point type).
  - A DP has attributes called DPE (data point element) which holds the measurements associated to the device
  - Data acquisition can be done by various protocols
  - Depending on the protocols, data acquisition is pulled or pushed





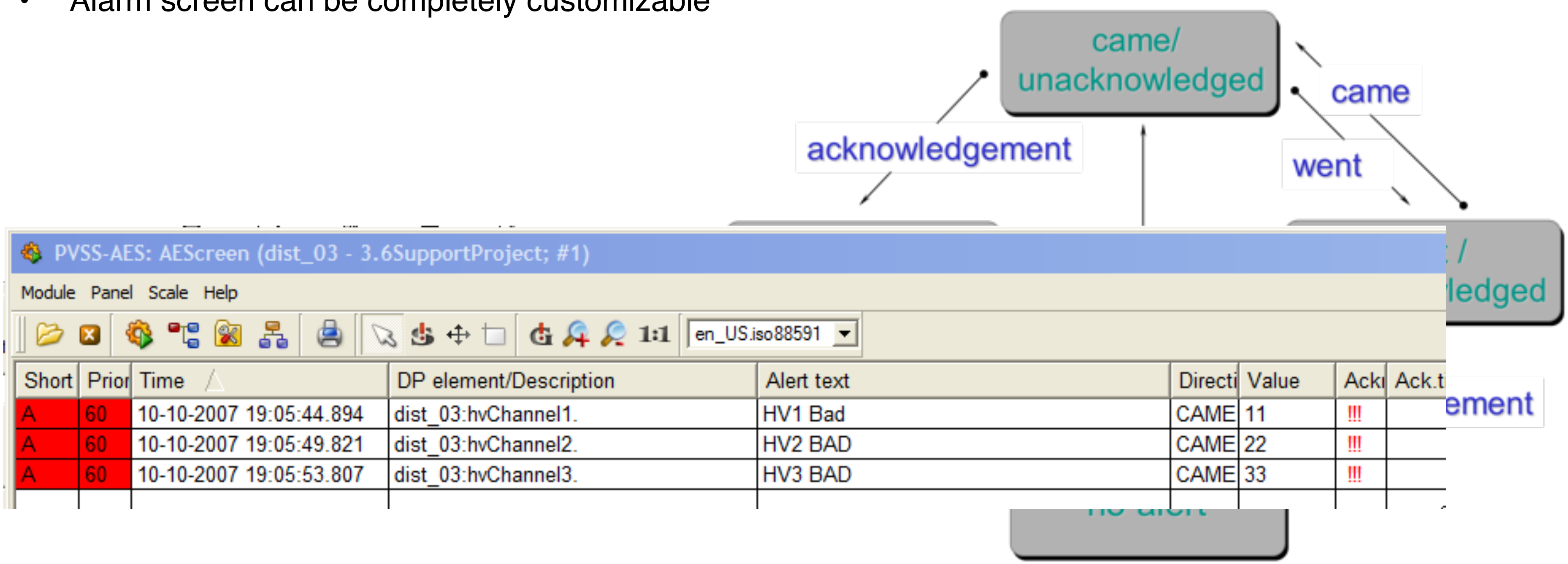
WinCC OA – Engineering

- Panel creation
  - Qt based
  - Drag and drop of widgets (button, text field, process data animated, etc.)
  - Development of custom widgets libraries
- Device configurations
  - Alarm settings, Archive, Smoothing, Acquisition
  - Can be done manually or automatically (through a database or files)

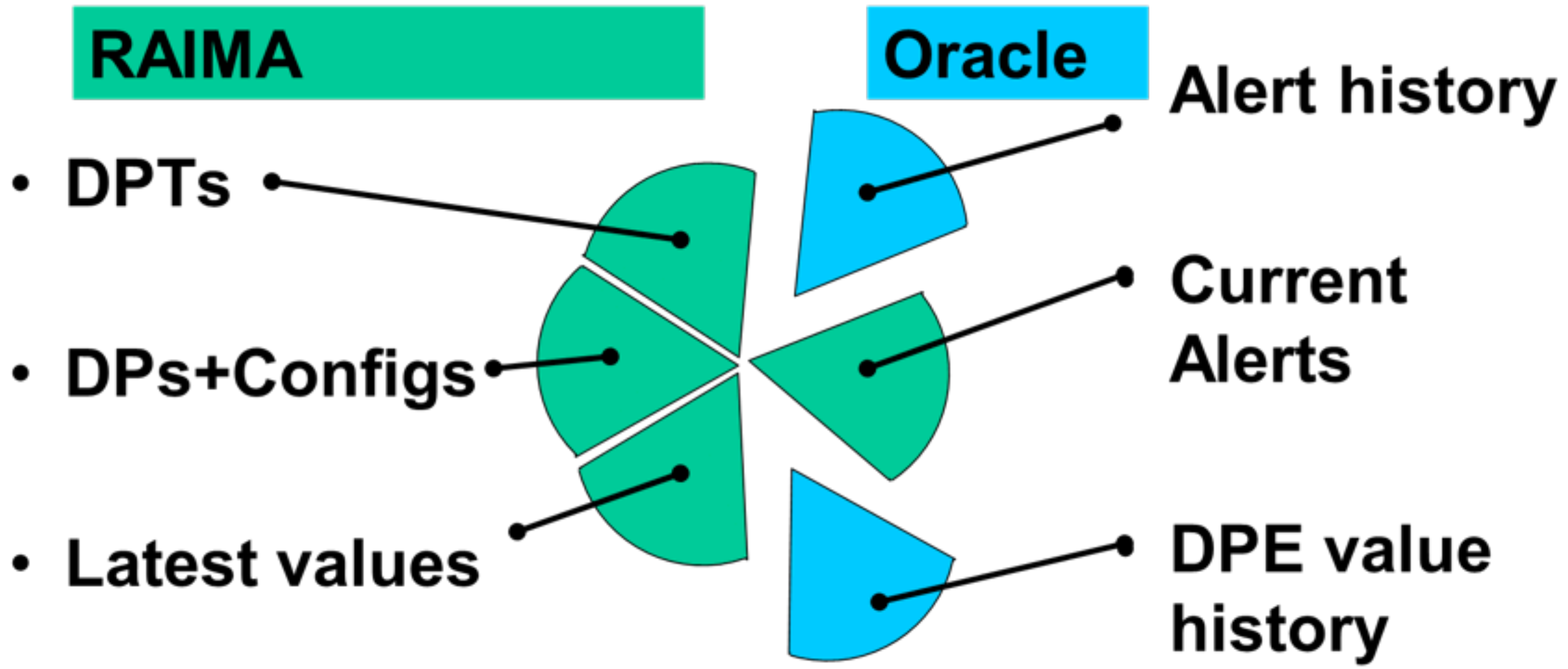


WinCC OA – Alarms

- An alert definition is in 2 parts:
  - The conditions under which the alert should be raised (made active). This is kept in the “alert_hdl” config (c.f. previous slide).
  - Related information in “alert_class” config, attributes which generally apply to more than one alert:
    - » Priority; Colour; Acknowledgement rules; Text formating
    - » Automatic script execution.
- Alarm summary
- Alarm filtering
- Alarm screen can be completely customizable



WinCC OA – Archiving

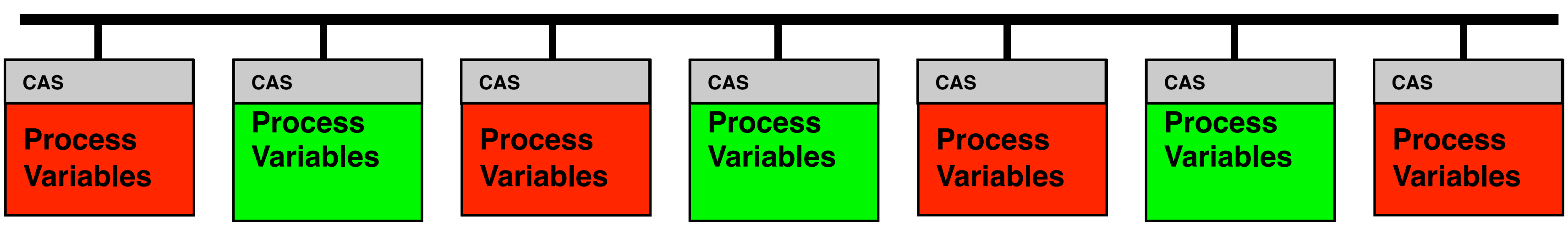


Copyright – WinCC OA ETM Siemens

EPICS

EPICS - Introduction

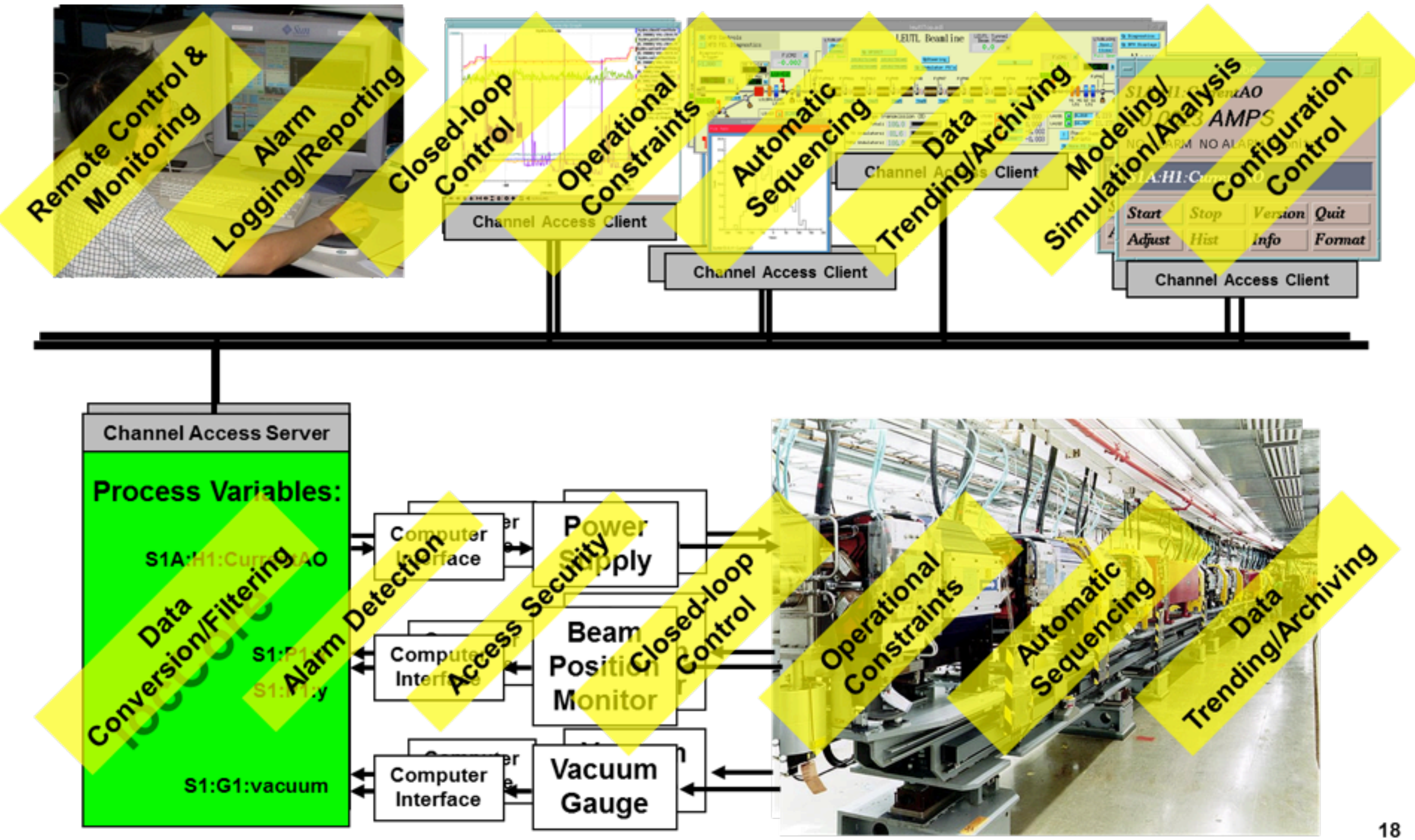
- **Experimental Physics and Industrial Control System** is an open source software lead by Argonne National Laboratory
- Main domains of application are scientific instruments
  - Particle accelerators, telescopes, etc.
- Set of software components and tools to create a control system
- Network based client/server model where the basic element is a Process Variable
  - The Channel Access Protocol defines how Process Variable data is transferred between a server and client
  - The entire set of Process Variables establish a Distributed Real-time Database of machine status, information and control parameters
  - Client broadcast PV names to the find the servers
  - Publish/subscribe protocol



EPICS - Introduction

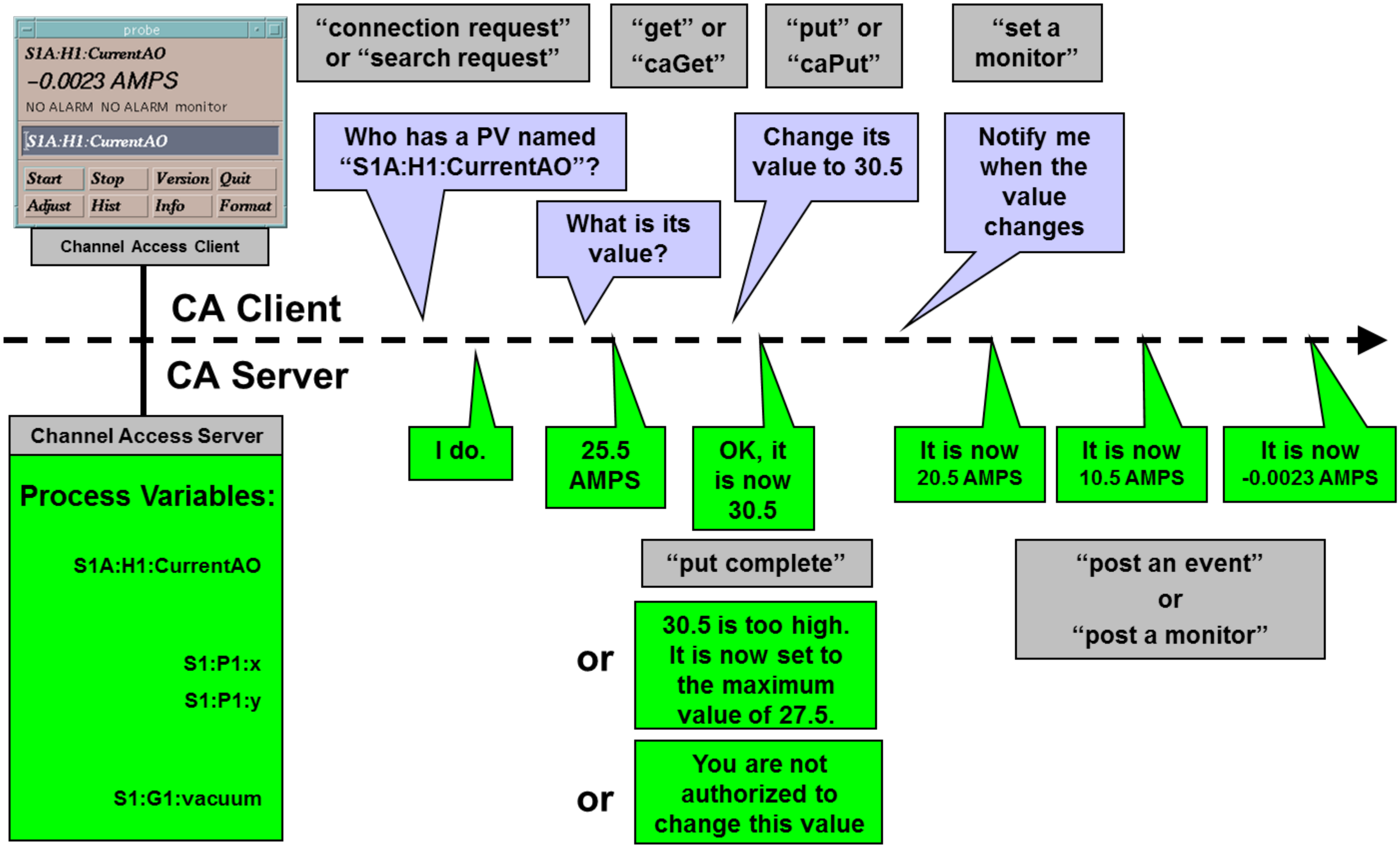
- Basic data element is a Process Variable
  - Process variable is a named piece of data with a set of attributes
- Examples of Attributes:
  - Alarm Severity (e.g. NO_ALARM, MINOR, MAJOR, INVALID)
  - Alarm Status (e.g. LOW, HI, LOLO, HIHI, READ_error)
  - Timestamp
  - Number of elements (array)
  - Normal Operating Range
  - Control Limits
  - Engineering Unit Designation (e.g. degrees, mm, MW)

EPICS - Overview

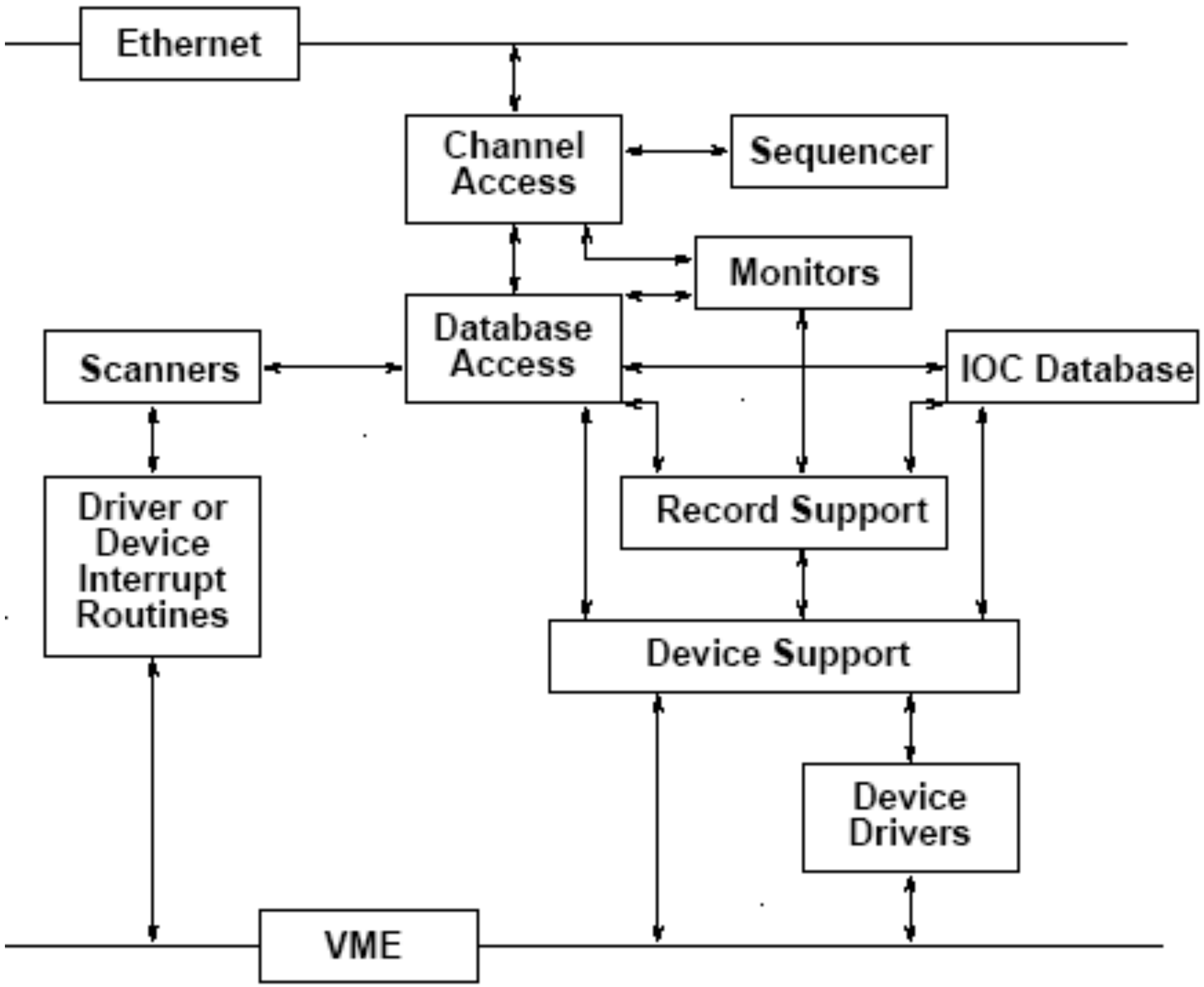


18

Epics – Data Acquisition



CAS Architecture



CAS DataBase

- Collection of records
- Each record represents a system parameter (process variable, PV)
  - Unique name
  - Set of attributes
  - Attributes and value can be modified
- Records must process to do something
  - An input record can read a value every 10 seconds
  - A CA write to an output record causes the record to process
  - Either input or output, not both

EPICS Record

- Input
  - Analog In (AI)
  - Binary In (BI)
  - String In (SI)
- Algorithm/control
  - Calculation (CALC)
  - Subroutine (SUB)
- Output
  - Analog Out (AO)
  - Binary Out (BO)
- Custom – only needed when existing record types or a collection of existing record types are inadequate

Tango

Tango - Introduction

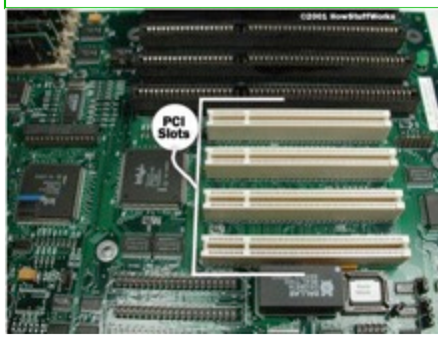
- Open Source control systems mainly used by European institutions
- Similar target as EPICS, high energy physics laboratory, very high customization
- It is an object oriented distributed control system based on
  - Corba, for the synchronous an asynchronous communications
  - ZeroMQ for the even based communication
- Programming supports are C++, Java and Python

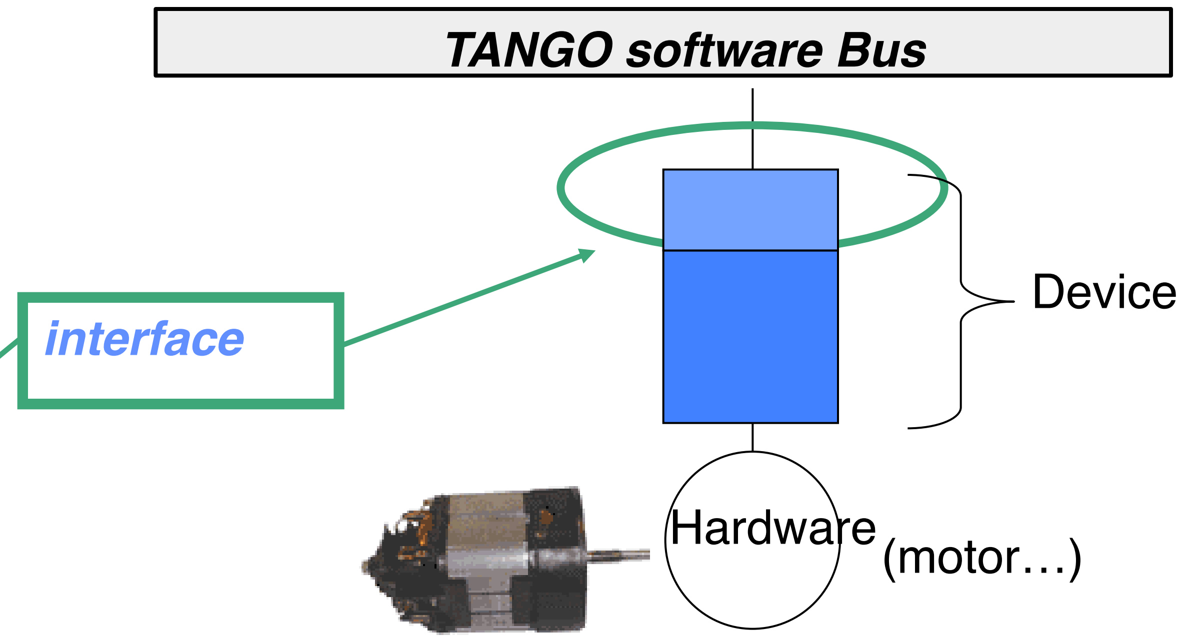
- Concepts
  - Each piece of hardware or software to be controlled (from the simplest to the most sophisticated) is a **device**
  - A device is an instance of a **Tango class** which is hardware/software specific
  - Device supports **commands** (actions) and **attributes** (data)
  - Tango classes are merged in operating system process called **Device Server**
  - **Device configuration parameters** and network address stored in a database

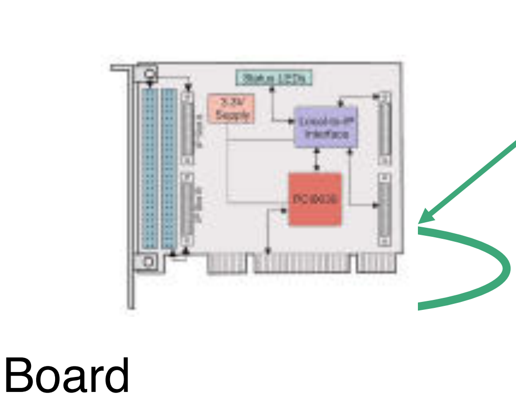
Tango As a Software Bus

- Analogy with an electronical bus because:
  - Each card plugged on the bus has a well-identified function
  - Each card is not or hardly coupled to the others
  - Development of each card can be decoupled

- *But* each card must respect a strict and well-defined *interface* in order to connect to the bus

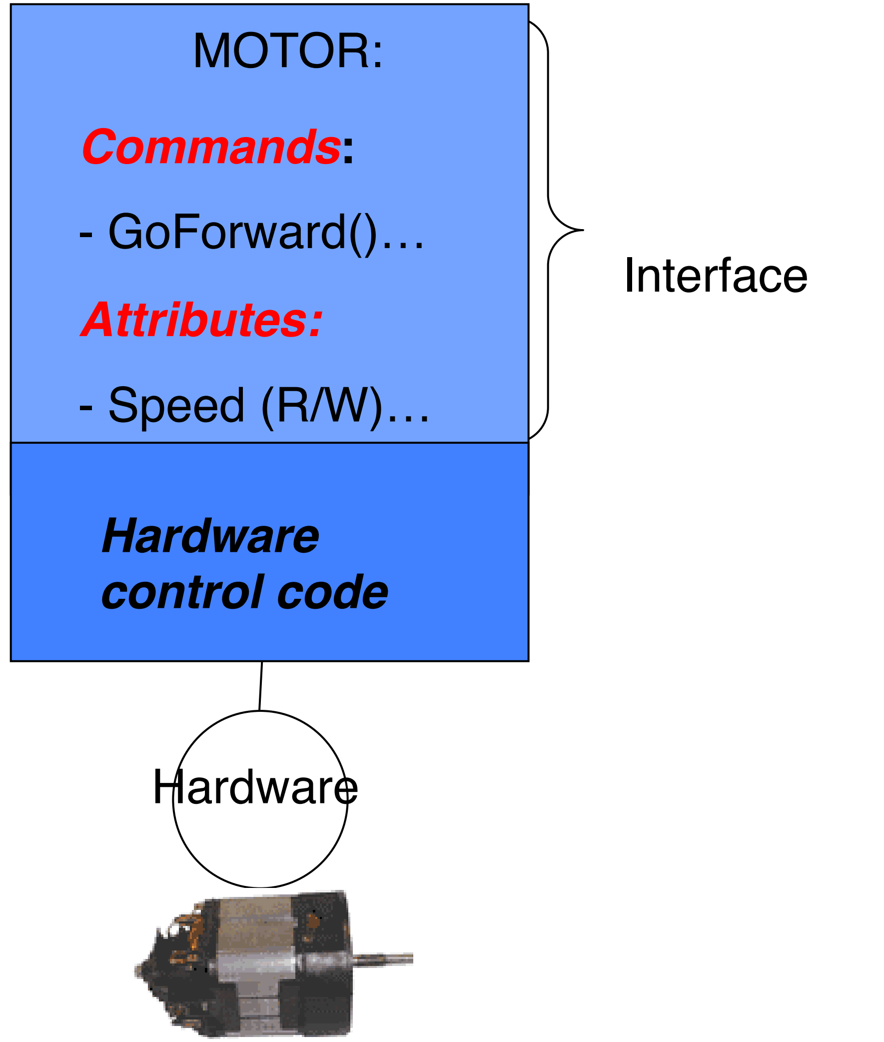




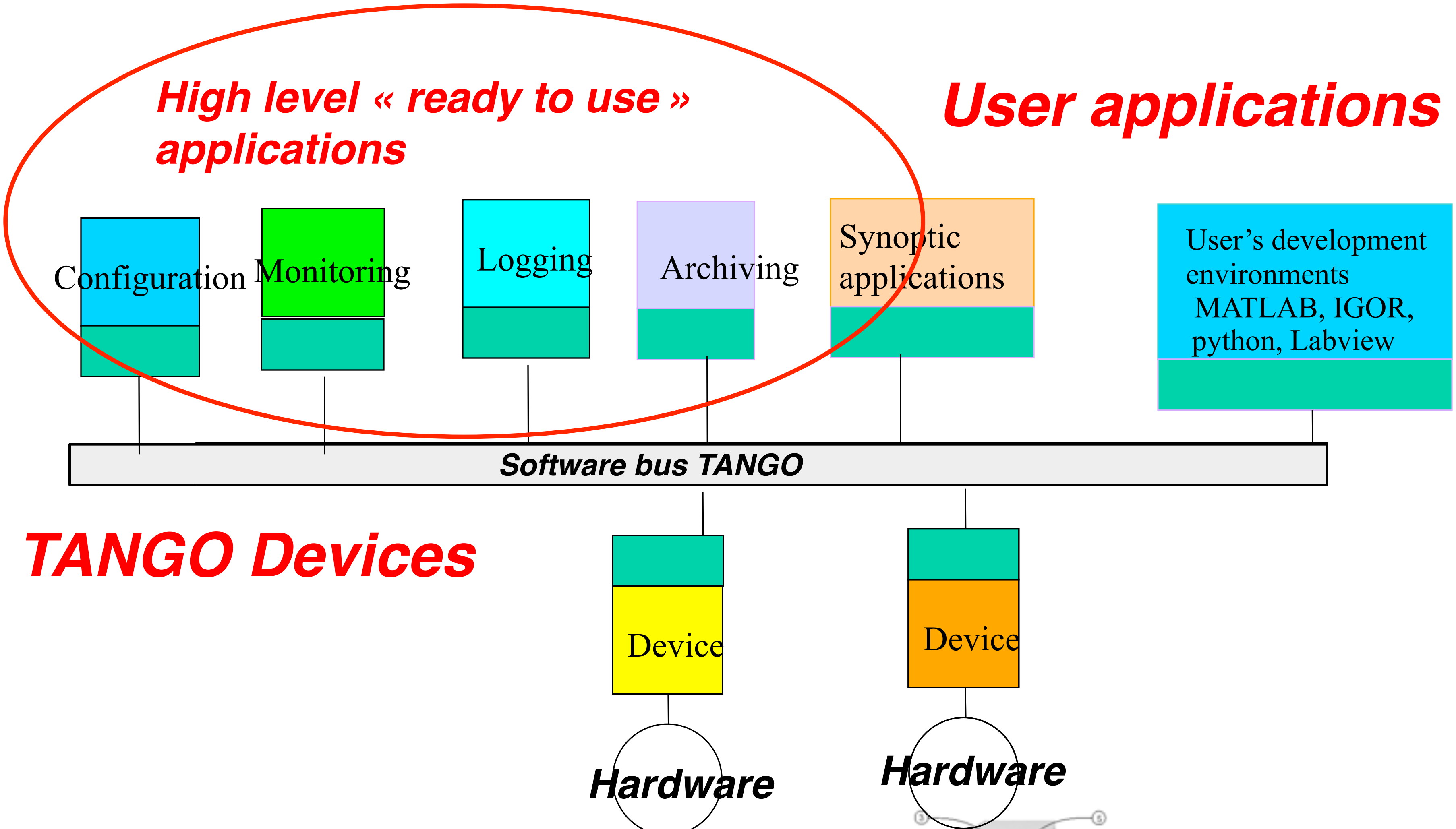


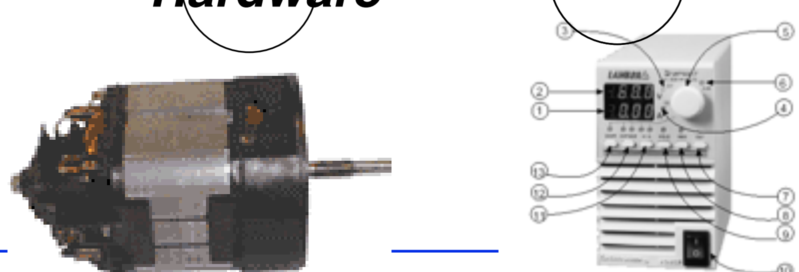
Example of a device

- **The Interface :**
  - **describes what the Device is supposed to do**
  - **It’s only a promise of the services you may expect from the Device**
- **But there isn’t any magic**
  - **Code has to be written to fullfill the promised services**

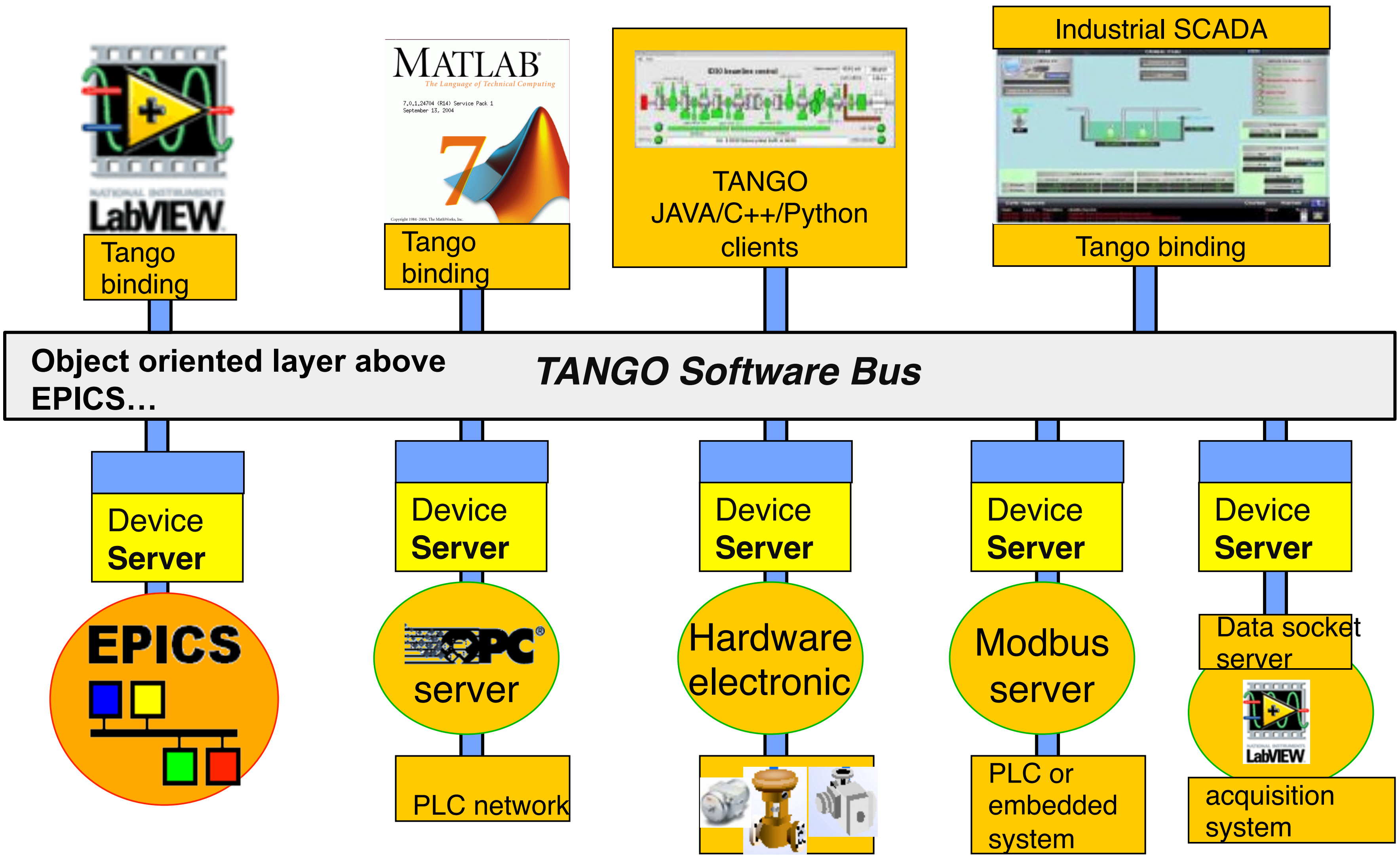


Tango Applications





Tango Interoperability



Main Tango Tools

- **Taurus Designer**
  - **Qt Designer application to develop synoptic view**
- **Pogo**
  - **Develop device server in C++**
- **Jive**
  - **Tango database browser and device testing tool**
- **Astor/Starter**
  - **Control system administration**
  - **Start/stop device server**
- **Sardana**
  - **Set of applications built on top of Tango for an “out-of-the-box” system**

References

- **SCADA HMI:**
  - The High Performance HMI Handbook, Bill Hollifield, Plant Automation Services; 1st edition (September 15, 2008)
  - Effective Console Operator HMI Design Practices (ISBN: 978-1492875635)
- **Alarm Management**
  - Effective Alarm Management Practices (ISBN: 978-1442184251)
- **SCADA Products**
  - WinCC OA
    - » http://w3.siemens.com/mcms/human-machine-interface/en/visualization-software/simatic-wincc-open-architecture/pages/default.aspx
  - EPICS
    - » http://www.aps.anl.gov/epics/
  - TANGO
    - » http://www.tango-controls.org/