EPFL

SCADA & Supervision

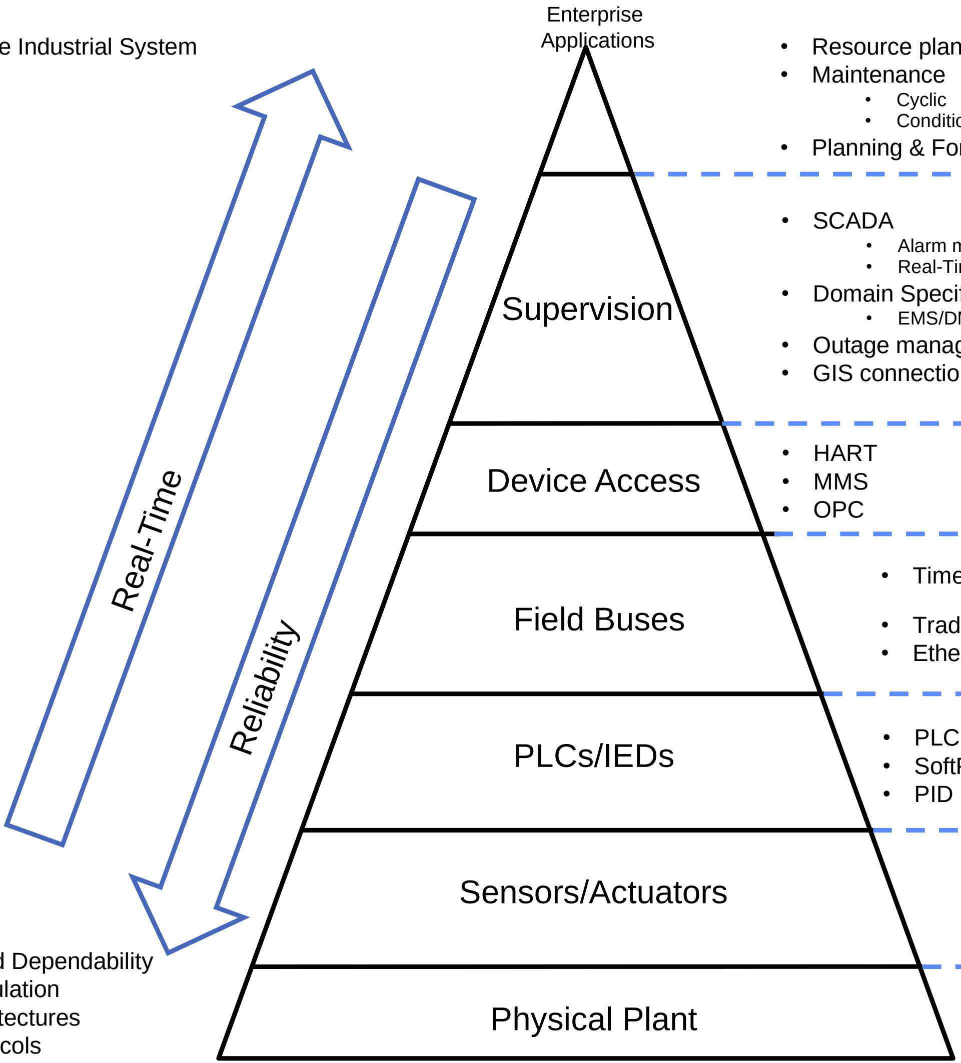
Industrial Automation

Dr. Jean-Charles TOURNIER

Spring 2025

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

- Real Time Industrial System



Enterprise Applications

Supervision

Device Access

Field Buses

PLCs/IEDs

Sensors/Actuators

Physical Plant

- 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.

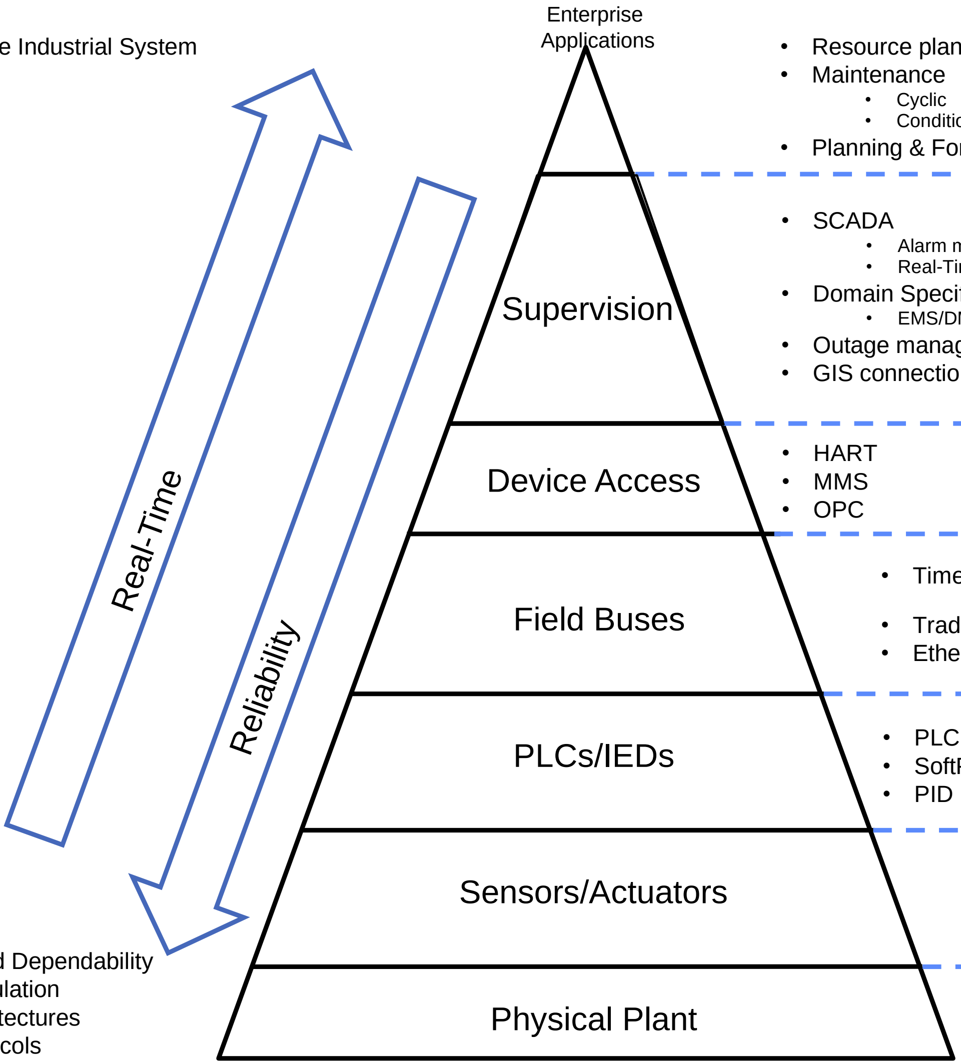
- PLC
- SoftPLC
- PID

- 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.)

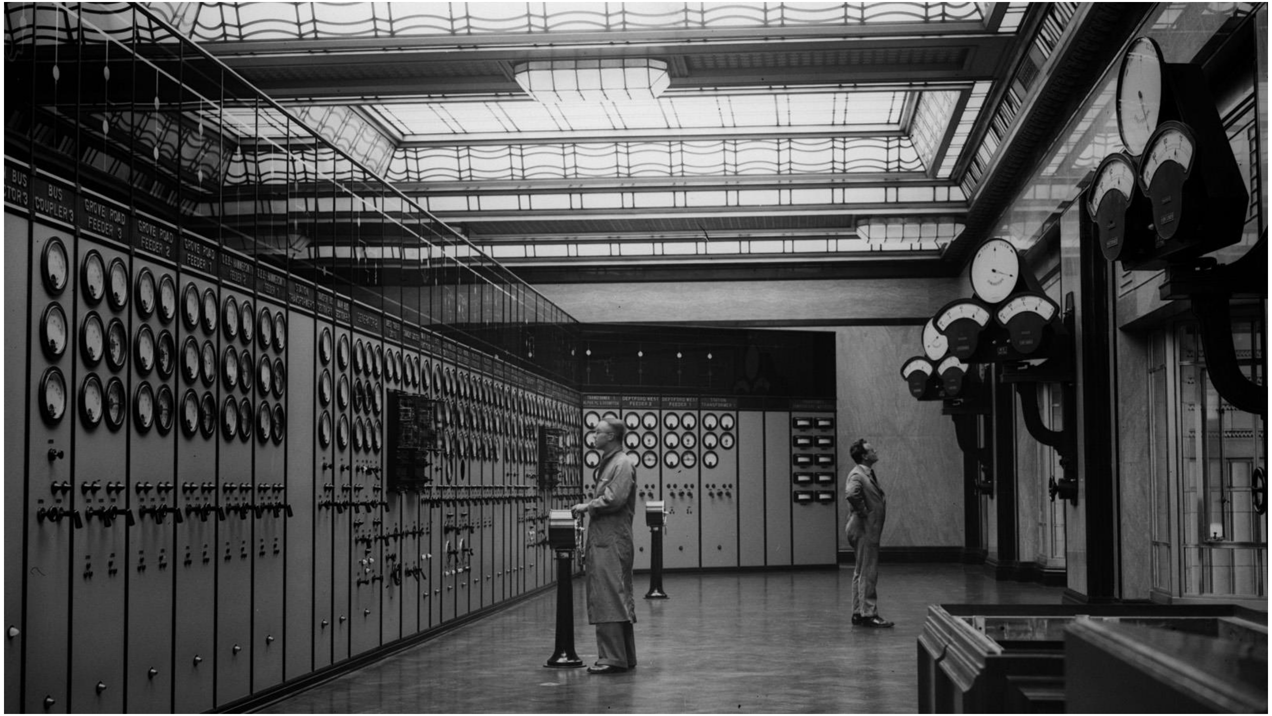
- Plant examples
- Why supervision/control?

- Reliability and Dependability
  - Calculation
  - Architectures
  - Protocols

Content

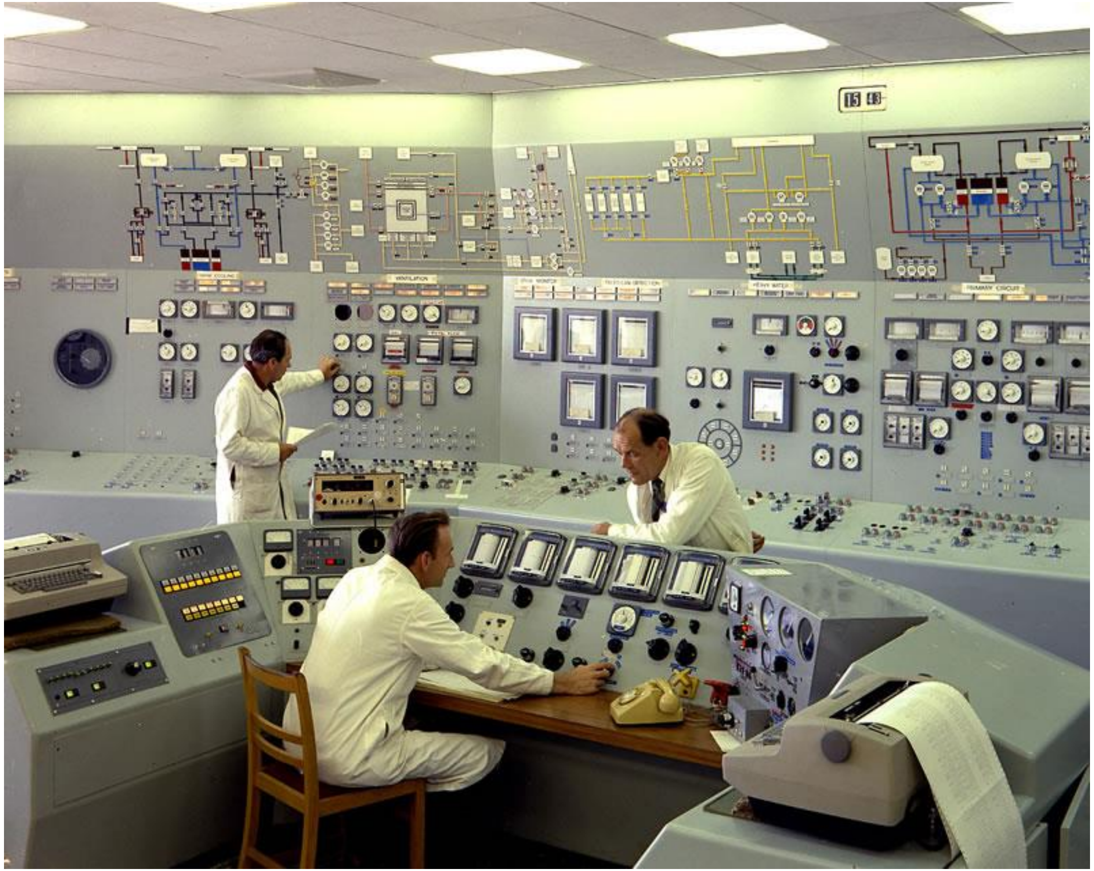
- Definitions
- SCADA Functionalities
- Cyber-Security and SCADA Systems
- Examples of SCADA Systems

Control Room ca. 1950s



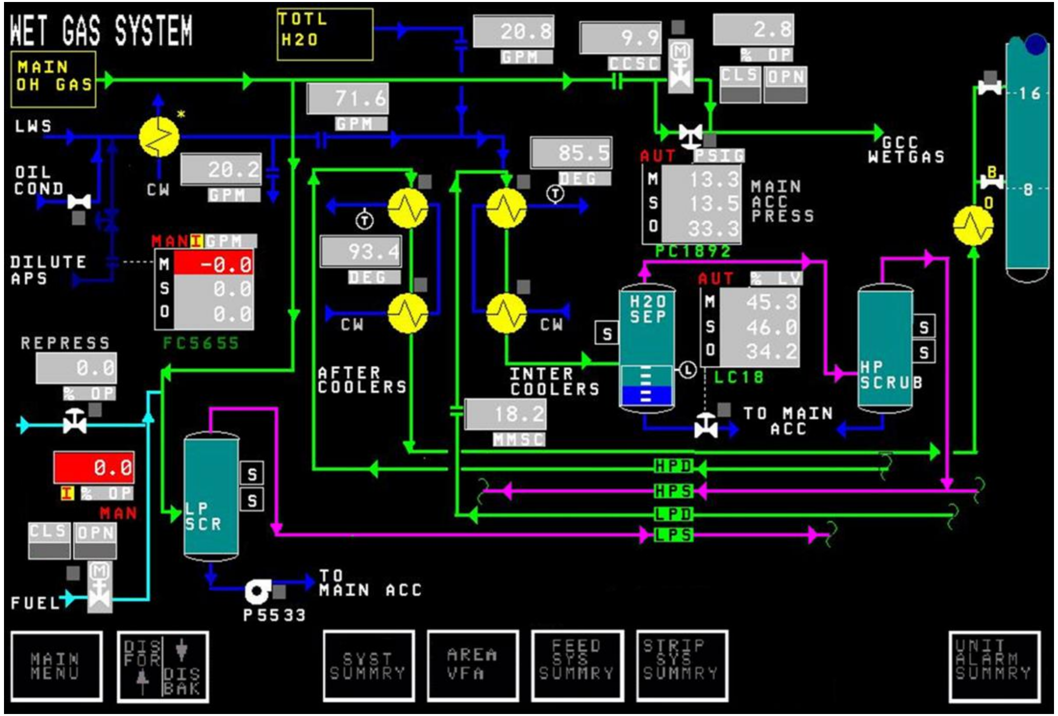
Coal-Fired Battersea Power Station – South London, UK – 1950s
Photo: Fox Photos/Getty Images

Control Room ca. 1970s

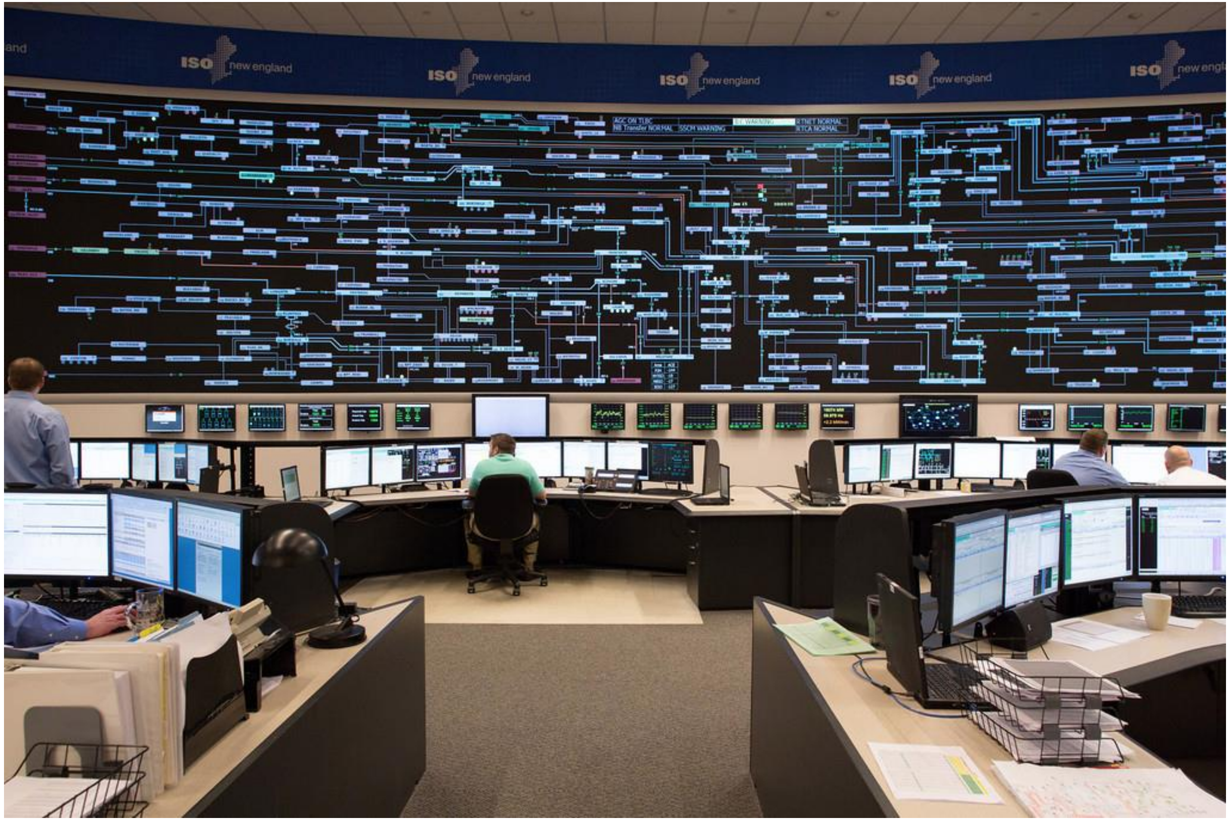


Steam Generating Heavy Water Reactor – (Water Cooled Nuclear Reactor) - Dorset, UK - 1970s

Control Room ca. 1990s



Control Room ca. 2010s

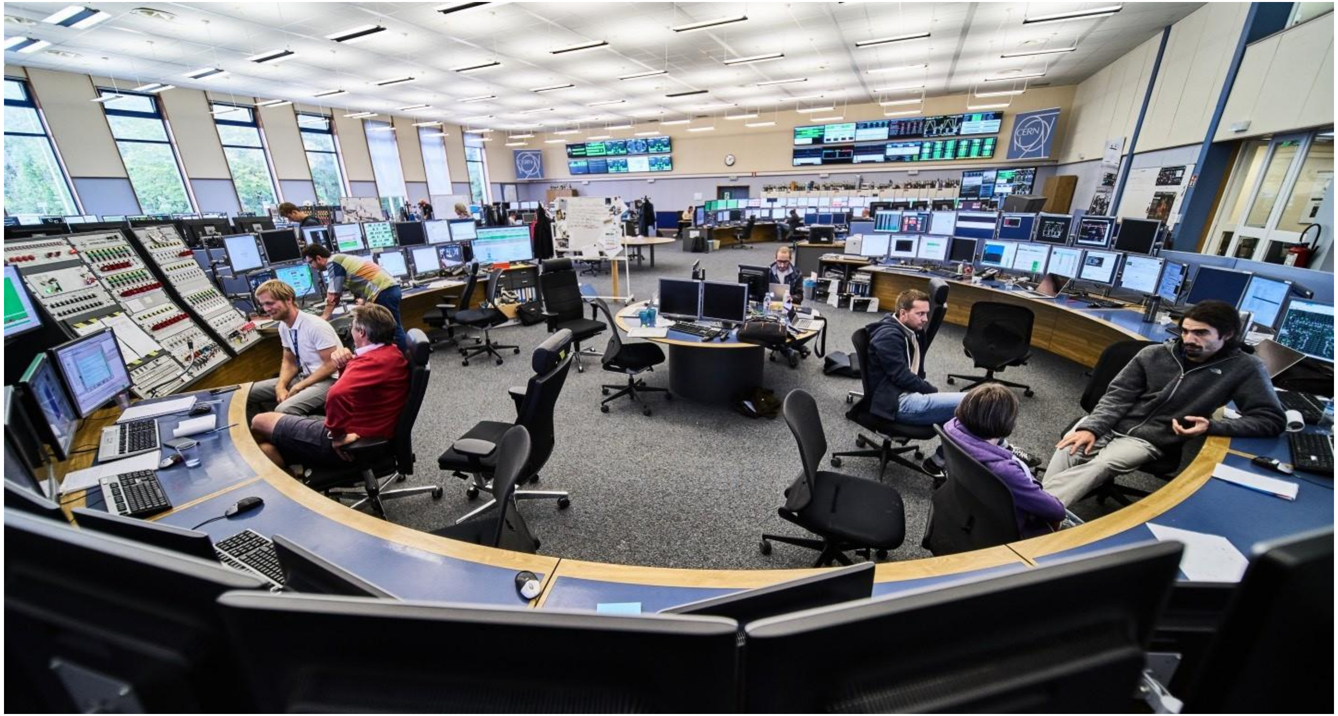


ISO New England Control Room

Control Rooms Nowadays

https://insights.samsung.com/2021/07/08/understanding-the-big-picture-for-a-modern-control-room-design/

Real-life Control Room 2020



CERN - https://home.cern/sites/home.web.cern.ch/files/2018-06/ccc.jpg

Future?

https://www.barco.com/en/inspiration/news-insights/2020-05-25-5-key-trends-in-control-rooms

Definitions

- SCADA
  - Supervisory Control And Data Acquisition
- Control Room
  - Room serving as an operation center from which operators can monitor and control systems
- Operator Workstation
  - Equipment used by operators to control and monitor a process (front-end)
- Servers
  - Back-end server linking the field devices and operator workstation
- Field Devices
  - Devices closed to the monitored process bringing data to/from the operator workstations

SCADA Functionalities 1/2

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

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

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

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

SCADA Functionalities 2/2

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

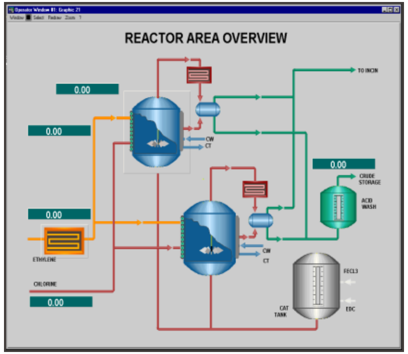
6. Measurements processing
   - calculate derived values (limit supervision, trending)

7. Logging
   - keep logs on the operation of the automation system

8. Reporting
   - generate incident reports

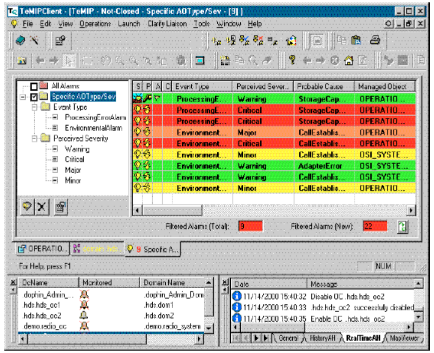
9. Interfacing to planning & analysis functions:
   - Forecasting, Simulation, historian, etc.

Operator Workstation Three Functions



current state

alarms and events



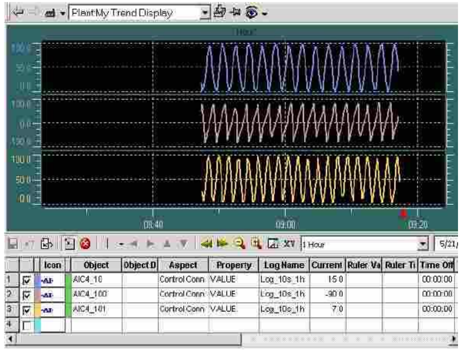
S	P	A	C	Event Type	Perceived Sever...	Probable Cause	Managed Object
				ProcessingE...	Warning	StorageCap...	OPERATIO...
				ProcessingE...	Critical	StorageCap...	OPERATIO...
				ProcessingE...	Critical	StorageCap...	OPERATIO...
				Environment...	Major	CallEstablis...	OPERATIO...
				Environment...	Critical	CallEstablis...	OPERATIO...
				Environment...	Minor	CallEstablis...	OSI_SYSTE...
				Environment...	Warning	AdapterError	OSI_SYSTE...
				Environment...	Warning	CallEstablis...	OSI_SYSTE...
				Environment...	Minor	CallEstablis...	OPERATIO...

Filtered Alarms (Total): 9 Filtered Alarms (New): 22

For Help, press F1

OcName	Monitored	Domain Name
.dophin_Admin_...		.dophin_Admin_Dom
.hds.hds_oc1		.hds.dom1
.hds.hds_oc2		.hds.dom2
.demo.radio_oc		.demo.radio_system

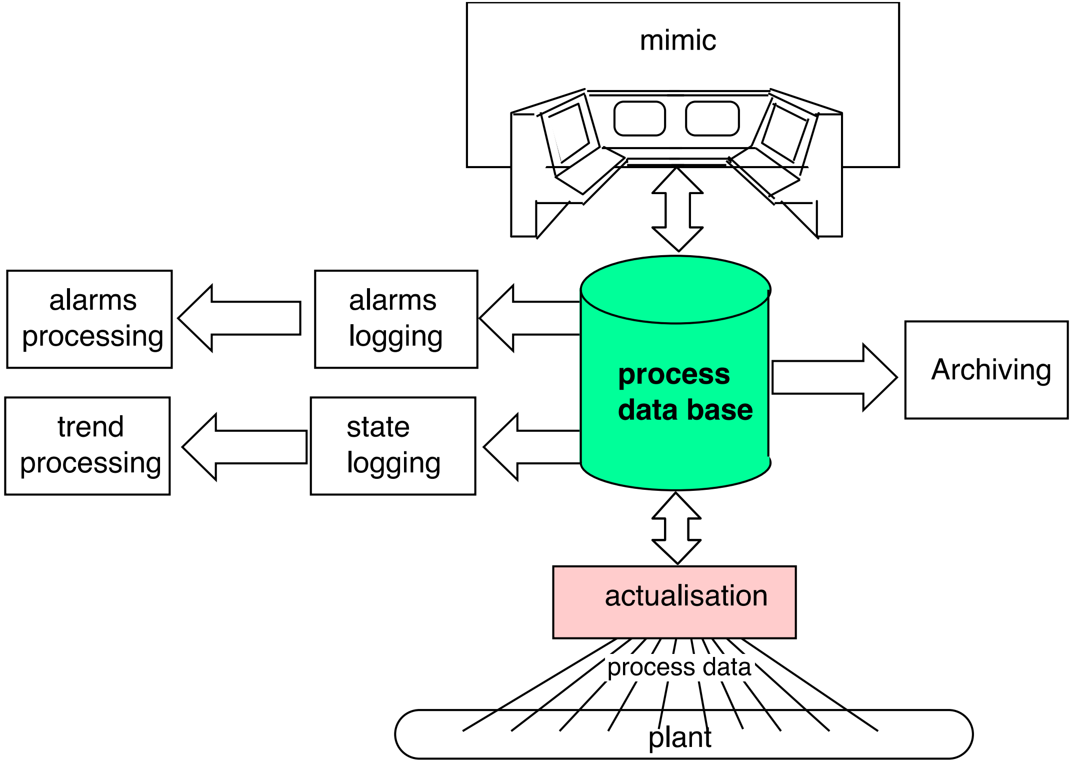
Date	Message
11/14/2000 15:40:32	Disable OC .hds.hds_oc2
11/14/2000 15:40:33	.hds.hds_oc2 successluly disabled
11/14/2000 15:40:35	Enable OC .hds.hds_oc2



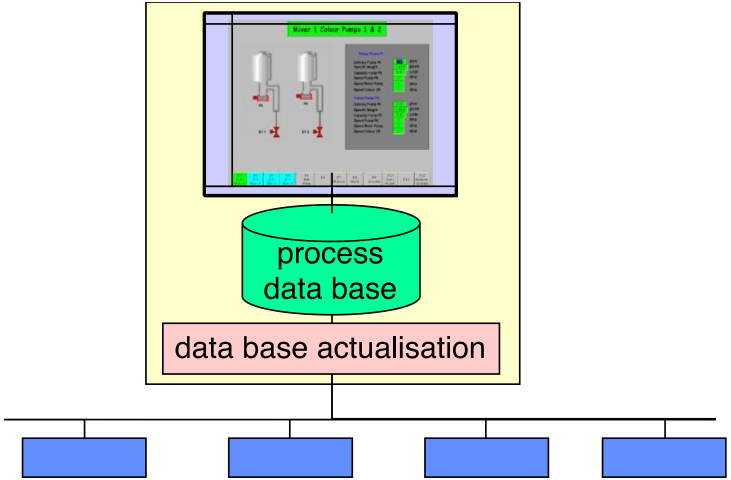
		Icon	Object	Object D	Aspect	Property	Log Name	Current	Ruler Va	Ruler Ti	Time Off
1	☑	AI	AIC4_10		Control Conn	VALUE	Log_10s_1h	15.0			00:00:00
2	☑	AI	AIC4_100		Control Conn	VALUE	Log_10s_1h	-30.0			00:00:00
3	☑	AI	AIC4_101		Control Conn	VALUE	Log_10s_1h	7.0			00:00:00
4	□										

trends and history

Elements of Operator Workstation



Process DataBase



- Process data represent the **current state** of the plant
- Older values are irrelevant and are overwritten by new ones
  - It is the role of the historical database to store previous values
- Process data are actualized either by
  - polling (the synoptic view fetches data regularly from the database (or from the devices)
  - events (the devices send data that changed to the database, which triggers the views)
- Process database != Historical data base

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 UA, 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

Human Machine Interface

Engineering

- Device model
  - How physical devices are modeled into the process database
- Configuration of the plant
  - Bind new devices, assign names and addresses to devices, set alarm threshold, archive, etc.
- Layout
  - Synoptic view design
  - Overall operational view organization (navigation)
- Command Sequences
  - Command language
- Protocol Definition
  - What is an event and when/where should it be registered?
- Mainly used during engineering and commissioning phase and afterwards during maintenance

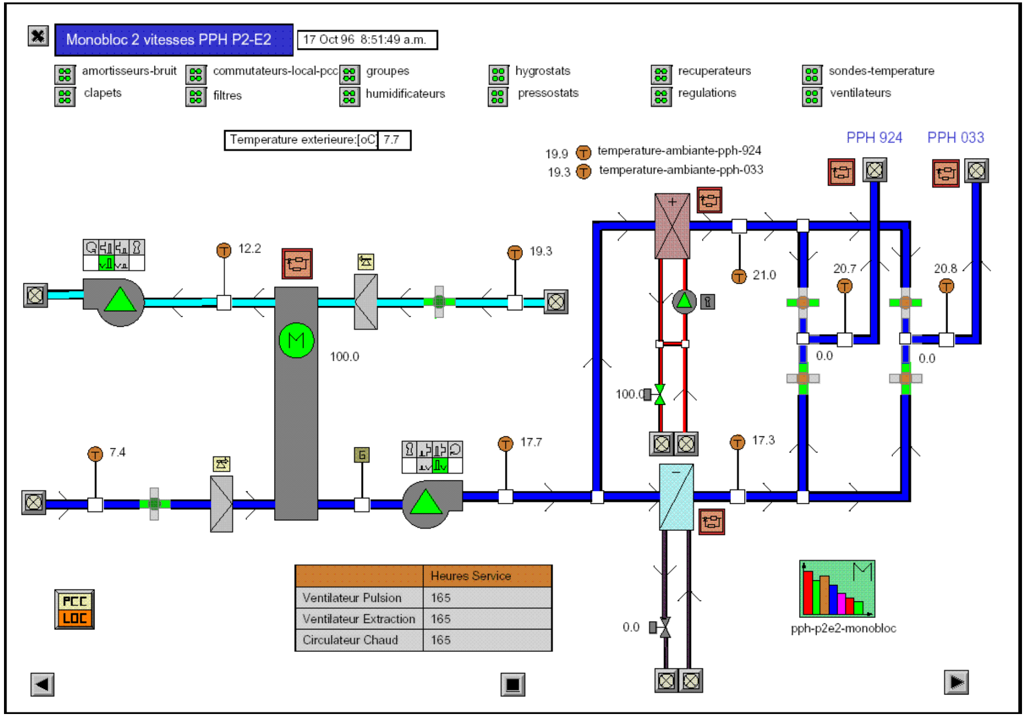
Human Machine Interface

Process Operation

- Representation of process plant
  - Lamps, indicators, trends, alarms, maintenance messages, etc.
- Recording process variables and events with timestamp
- Sending of commands to the process
- Record all actions
- Device selection (lock devices)
- Administration (access rights)
- Status of the SCADA itself
  - Meta-supervision

HMI Example

EPFL Air Conditioning



Monobloc 2 vitesses PPH P2-E2

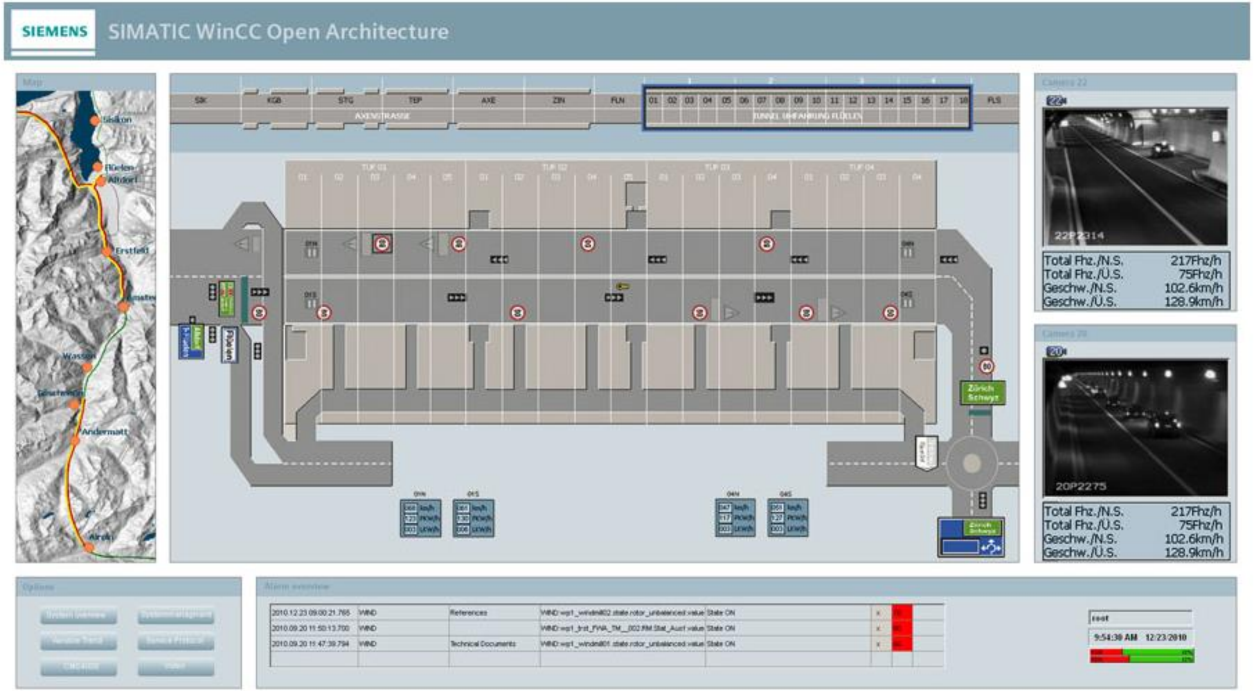
17 Oct 96 8:51:49 a.m.

Temperature exterieure:[oC] 7.7

	Heures Service
Ventilateur Pulsion	165
Ventilateur Extraction	165
Circulateur Chaud	165

HMI Example

Tunnel Traffic



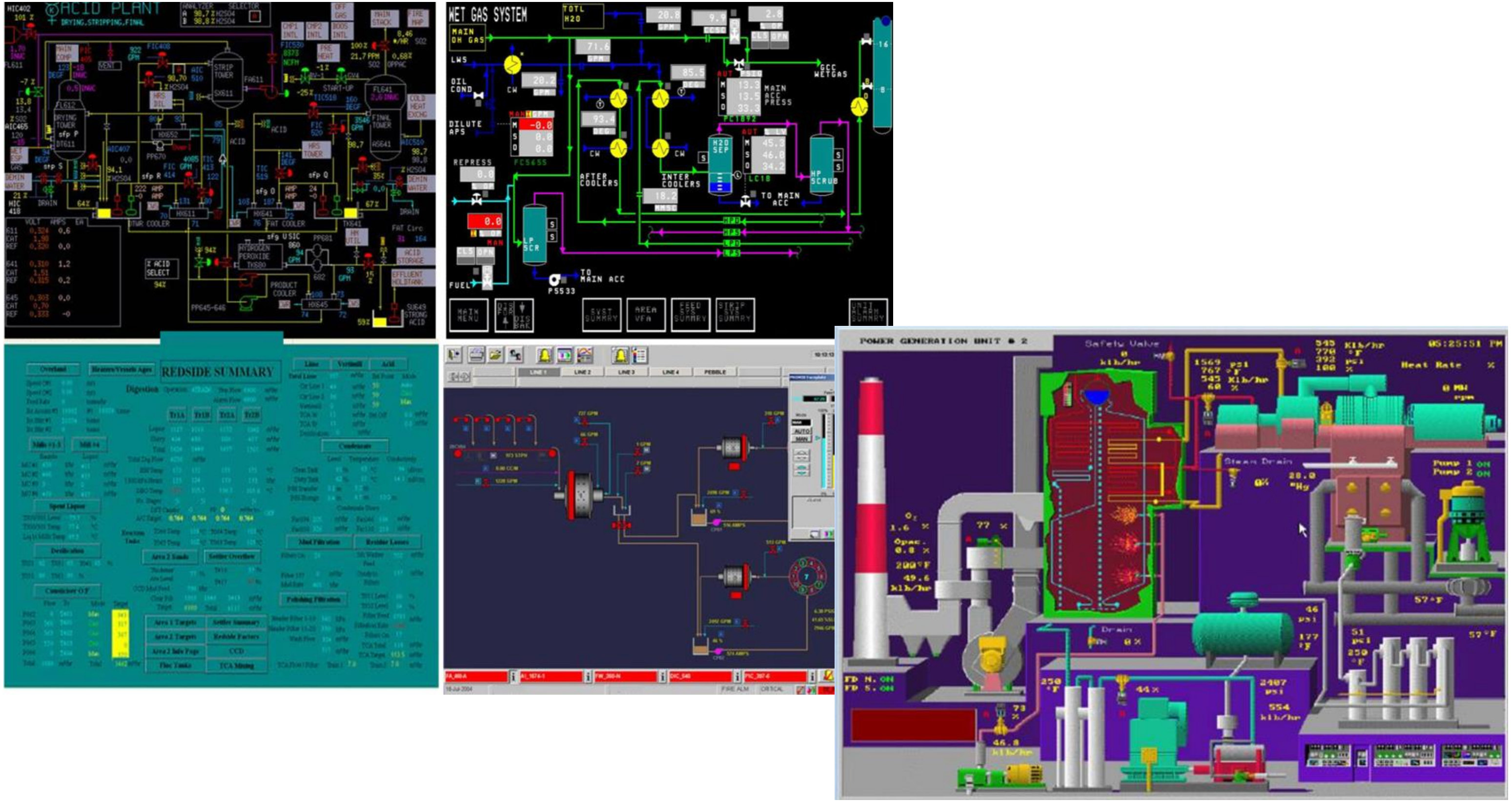
Total Fhz./N.S. 217Fhz/h
Total Fhz./Ü.S. 75Fhz/h
Geschw./N.S. 102.6km/h
Geschw./Ü.S. 128.9km/h

Total Fhz./N.S. 217Fhz/h
Total Fhz./Ü.S. 75Fhz/h
Geschw./N.S. 102.6km/h
Geschw./Ü.S. 128.9km/h

```
2010.12.23 09:00:21.765  WIND  References           WIND:wp1_windmill02.state.rotor_unbalanced.value  State ON  x
2010.09.20 11:50:13.700  WIND                       WIND:wp1_frst_FWA_TM__002.RM.Stat_Aus1.value      State ON  x
2010.09.20 11:47:39.794  WIND  Technical Documents  WIND:wp1_windmill01.state.rotor_unbalanced.value  State ON  x
```

root
9:54:30 AM 12/23/2010

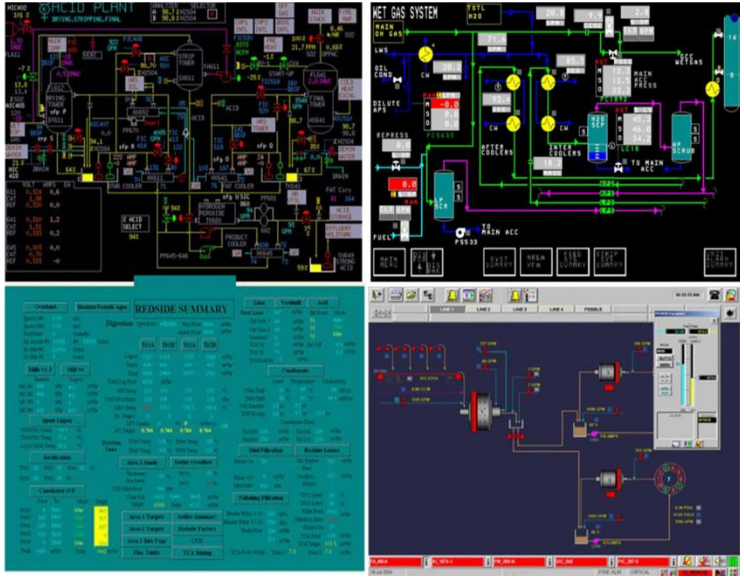
More common HMI



Common HMI Mistakes

1. Numbers sprinkled on the screen
2. Inconsistent, improper use of colors
3. Too many color coding
4. No trends
5. No condition information
6. No global overview
7. 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

Blood Test Results	
Test	Results
HCT	31.7%
HGB	10.2 g/dl
MCHC	32.2 g/dl
WBC	40.1x10^9 /L
GRANS	6.5x10^9 /L
L/M	2.7x10^9 /L
PLT	150x10^9 /L

How good/bad are the results?

Data is not information

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	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

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

Data is not information

Blood Test Results

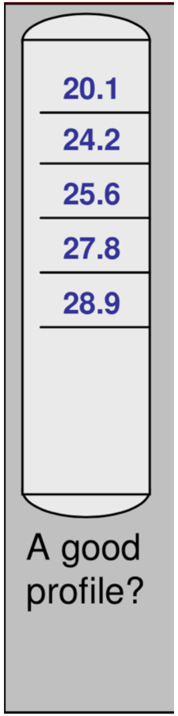
Test	Results	Range	Indicator Low – Normal - High
HCT	31.7%	24.0 – 45.0	□ 🟩 □
HGB	10.2 g/dl	8.0 – 15.0	□ 🟩 □
MCHC	32.2 g/dl	30.0 – 36.9	□ 🟩 □
WBC	40.1x10^9 /L	5.0 – 18.9	□ □ 🟥
GRANS	6.5x10^9 /L	2.5 – 12.5	□ 🟩 □
L/M	2.7x10^9 /L	1.5 – 7.8	□ 🟩 □
PLT	150x10^9 /L	175 – 500	🟥 □ □

Data is not information

Blood Test Results

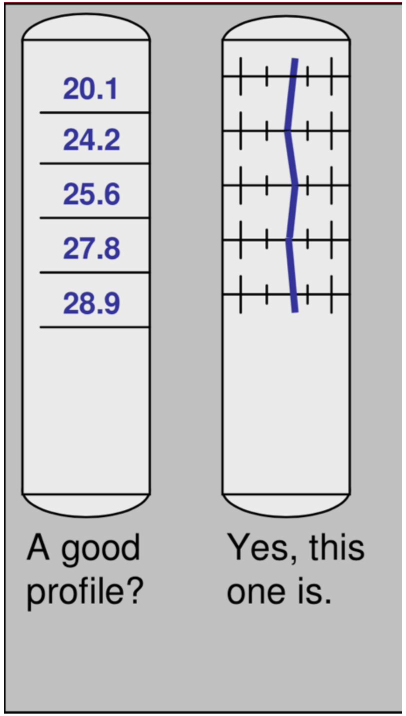
Test	Results	Range	Indicator + Trend Low – Normal - High
HCT	31.7%	24.0 – 45.0	□ 🟩 □ ↗
HGB	10.2 g/dl	8.0 – 15.0	□ 🟩 □ →
MCHC	32.2 g/dl	30.0 – 36.9	□ 🟩 □ ↘
WBC	40.1x10^9 /L	5.0 – 18.9	□ □ 🟥 →
GRANS	6.5x10^9 /L	2.5 – 12.5	□ 🟩 □ ↘
L/M	2.7x10^9 /L	1.5 – 7.8	□ 🟩 □ ↗
PLT	150x10^9 /L	175 – 500	🟥 □ □ →

Application to Industrial Examples



A good profile?

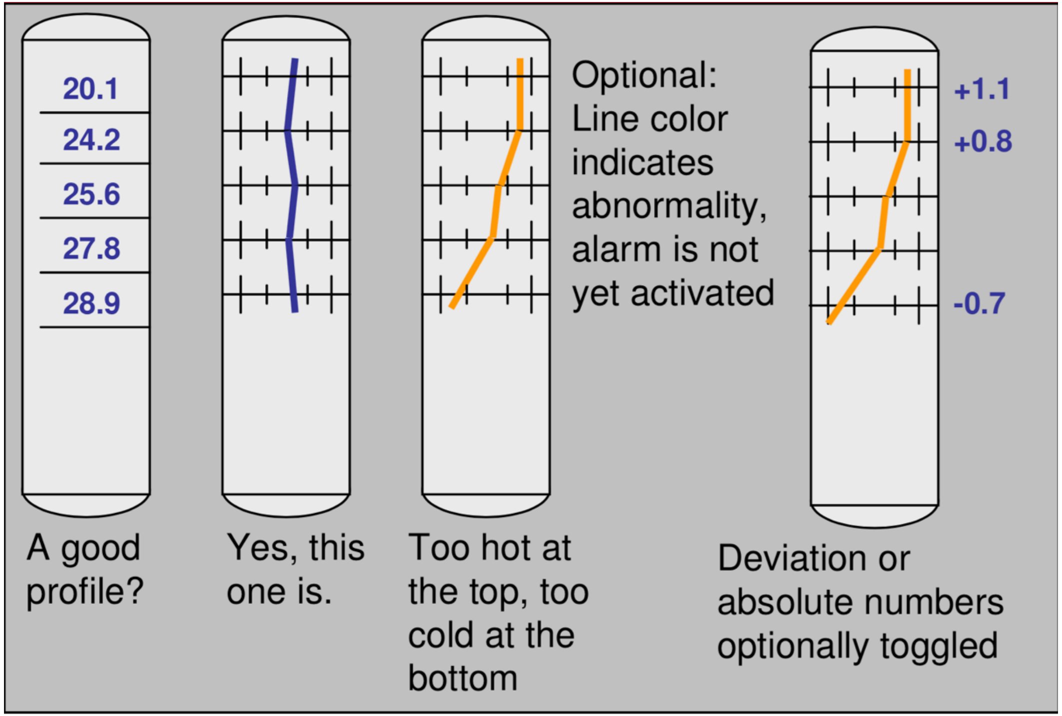
Application to Industrial Examples



A good profile?

Yes, this one is.

Application to Industrial Examples



A good profile?

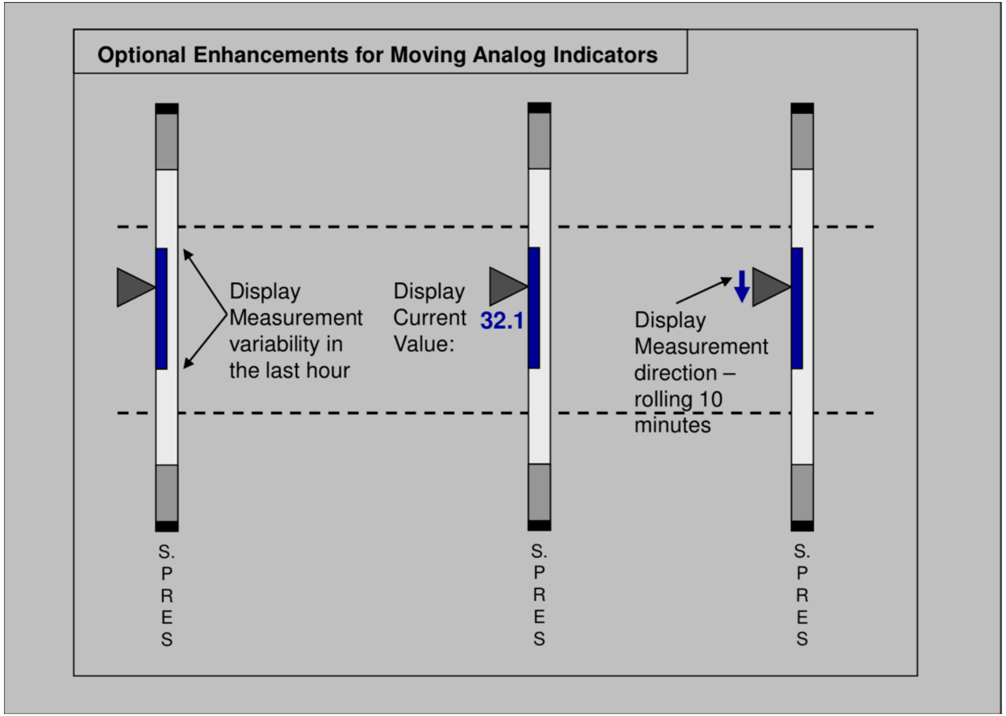
Yes, this one is.

Too hot at the top, too cold at the bottom

Optional: Line color indicates abnormality, alarm is not yet activated

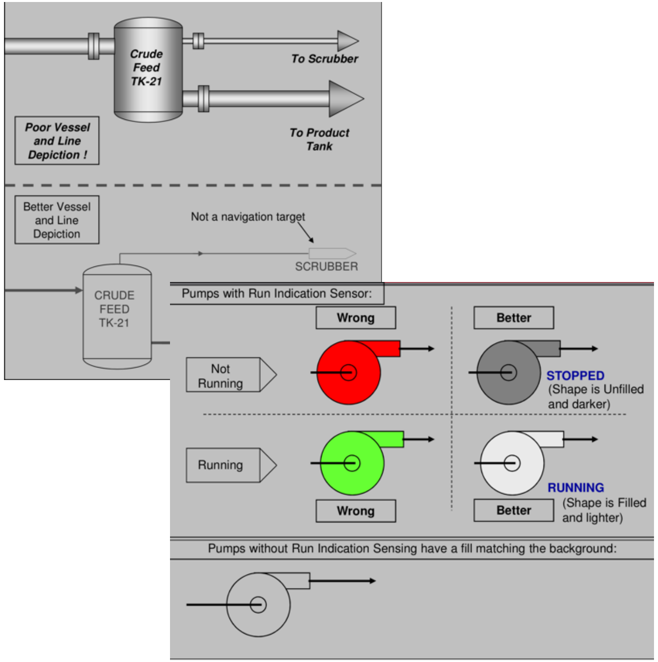
Deviation or absolute numbers optionally toggled

Application to Industrial Examples

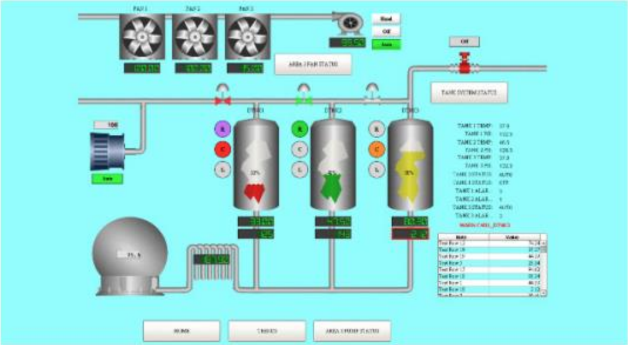

Optional Enhancements for Moving Analog Indicators
Display Measurement variability in the last hour
Display Current Value:
32.1
Display Measurement direction – rolling 10 minutes
S. P R E S
S. P R E S
S. P R E S

HMI Recommendations

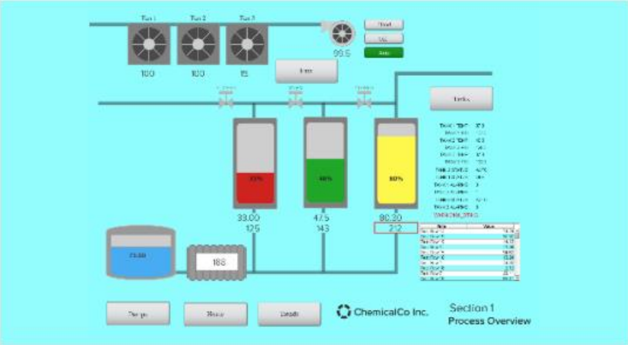
- Get rid of unnecessary details
- Don’t get fancy (avoid 3D objects)
- Bright/Saturated colors are for abnormal conditions only
- Red/Green colors are usually bad choices
  - ~8% of the population is color blind
- Remove Unnecessary Animation
  - Animation is often a distraction rather than a benefit to the user
- CAPITAL LETTERS TAKE LONGER TO READ


Crude Feed TK-21
To Scrubber
To Product Tank
Poor Vessel and Line Depiction !
Better Vessel and Line Depiction
Not a navigation target
SCRUBBER
CRUDE FEED TK-21
Pumps with Run Indication Sensor:
Wrong
Better
Not Running
STOPPED (Shape is Unfilled and darker)
Running
Wrong
Better
RUNNING (Shape is Filled and lighter)
Pumps without Run Indication Sensing have a fill matching the background:

HMI recommendations in practice



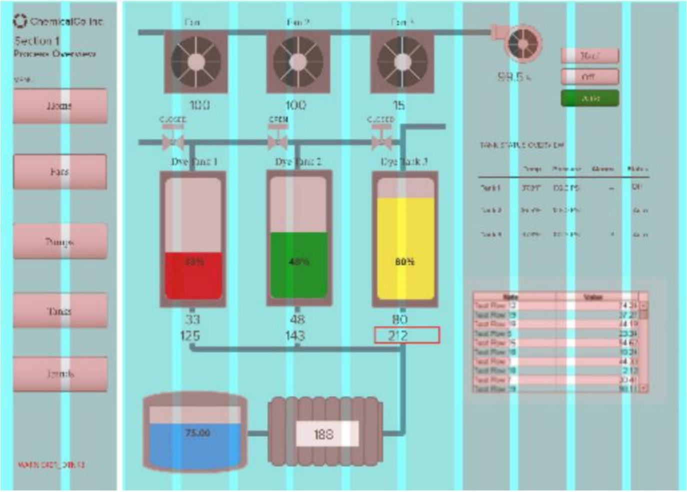
Before



After

More Recommendations

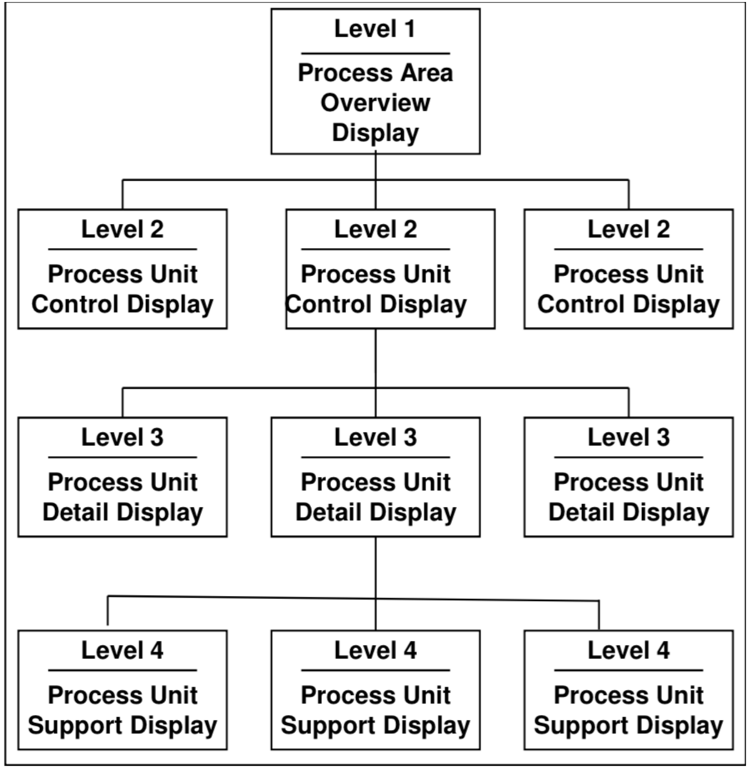
- Use grids to add rhythm and order
- Use columns to break the HMI into sections
  - Columns use alignment and grids to divide a space into vertical sections. These sections determine the flow and the spaces dedicated to certain elements of your HMI design.
  - The 12-column grid is the most commonly used layout
- For example
  - the first column span is for navigation
  - the middle column span is for primary information
  - and third column span is for secondary information
- Use Icons or Images With a Similar Look
- Keep Your Data Formatting the Same (date, time)
- Use the Same Terminology (e.g., submit/send buttons)



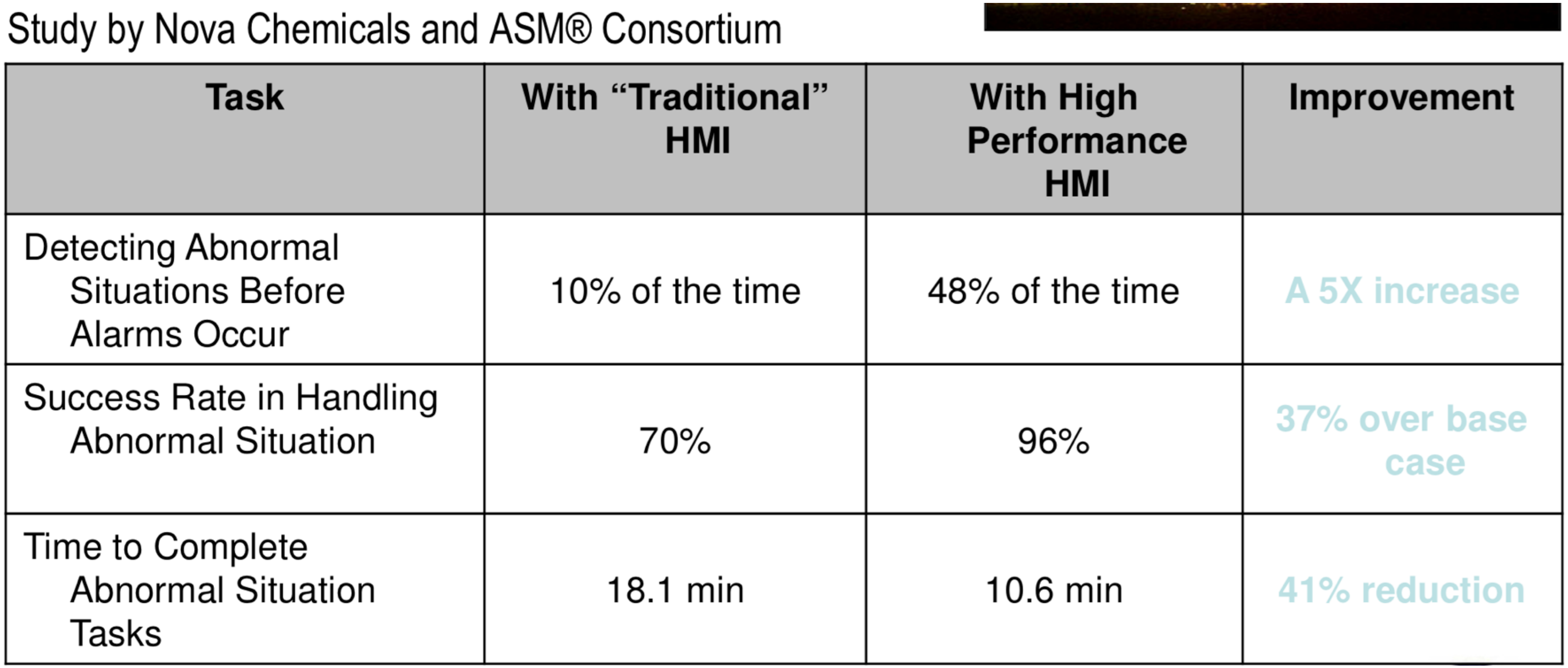
HMI Organization

- 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**


Level 1
Process Area Overview Display
Level 2
Process Unit Control Display
Level 2
Process Unit Control Display
Level 2
Process Unit Control Display
Level 3
Process Unit Detail Display
Level 3
Process Unit Detail Display
Level 3
Process Unit Detail Display
Level 4
Process Unit Support Display
Level 4
Process Unit Support Display
Level 4
Process Unit Support Display

Importance of well designed HMI

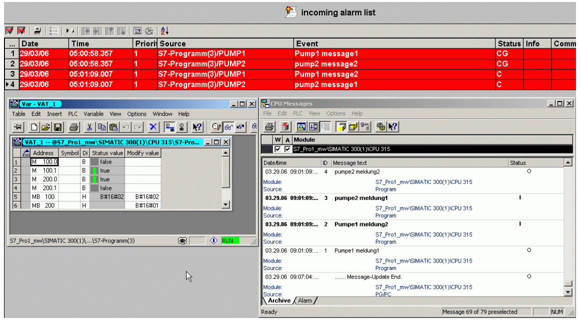


Study by Nova Chemicals and ASM® Consortium

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

Alarms & Events

- What is an alarm? An event?
- How should they be defined?
- How should they be visualized?
- How should they be managed?



incoming alarm list

...	Date	Time	Priorit	Source	Event	Status	Info	Comm
1	29/03/06	05:00:58.357	1	S7-Programm(3)/PUMP1	Pump1 message1	CG		
2	29/03/06	05:00:58.357	1	S7-Programm(3)/PUMP2	pump2 message2	CG		
3	29/03/06	05:01:09.007	1	S7-Programm(3)/PUMP1	Pump1 message2	C		
▸4	29/03/06	05:01:09.007	1	S7-Programm(3)/PUMP2	pump2 message1	C		

Var - VAT_1

VAT_1 -- @S7_Pro1_mw\SIMATIC 300(1)\CPU 315\S7-Pro...

	Address	Symbol	Di	Status value	Modify value
1	M 100.0		B	false	
2	M 100.1		B	🟩 true	
3	M 200.0		B	🟩 true	
4	M 200.1		B	false	
5	MB 100		H	B#16#02	B#16#02
6	MB 200		H		B#16#01

S7_Pro1_mw\SIMATIC 300(1)\...\S7-Programm(3) RUN

CPU Messages

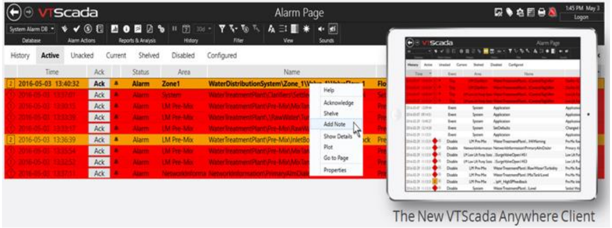
W	A	Module
☑	☑	S7_Pro1_mw\SIMATIC 300(1)\CPU 315

Date/time	ID	Message text	Status
03.29.06 09:01:09:...	4	pumpe2 meldung2	O
Module:		S7_Pro1_mw\SIMATIC 300(1)\CPU 315	
Source:		Program	
03.29.06 09:01:09:...	**3**	**pumpe2 meldung1**	I
Module:		S7_Pro1_mw\SIMATIC 300(1)\CPU 315	
Source:		Program	
03.29.06 09:01:09:...	**2**	**Pumpe1 meldung2**	I
Module:		S7_Pro1_mw\SIMATIC 300(1)\CPU 315	
Source:		Program	
03.29.06 09:01:09:...	1	Pumpe1 meldung1	O
Module:		S7_Pro1_mw\SIMATIC 300(1)\CPU 315	
Source:		Program	
03.29.06 09:07:04:...		.... Message-Update End.	O
Module:		S7_Pro1_mw\SIMATIC 300(1)\CPU 315	
Source:		PG/PC	

Archive / Alarm

Ready — Message 69 of 79 preselected — NUM

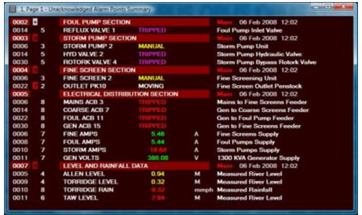
Table Edit Insert PLC Variable View Options Window Help
File Edit PLC View Options Help



VTScada — Alarm Page

	Time	Ack		Status	Area	Name
2	2016-05-03 13:40:32	Ack	▲	Alarm	Zone1	WaterDistributionSystem\Zone_1\V...
1	[illegible]	Ack	▲	Alarm	System	WaterTreatmentPlant\Clarifiers\Settle...
1	[illegible]	Ack	▲	Alarm	LM Pre-Mix	WaterTreatmentPlant\Pre-Mix\MixTan...
1	[illegible]	Ack	▲	Alarm	LM Pre-Mix	WaterTreatmentPlant\..\RawWater Tu...
1	[illegible]	Ack	▲	Alarm	LM Pre-Mix	WaterTreatmentPlant\Pre-Mix\RawW...
2	2016-05-03 13:36:39	Ack	▲	Alarm	LM Pre-Mix	WaterTreatmentPlant\Pre-Mix\InletBo...
1	[illegible]	Ack	▲	Alarm	LM Pre-Mix	WaterTreatmentPlant\Pre-Mix\MixTan...
1	[illegible]	Ack	▲	Alarm	LM Pre-Mix	WaterTreatmentPlant\Pre-Mix\MixTan...
1	[illegible]	Ack	▲	Alarm	NetworkInforma	NetworkInformation\PrimaryAlmDiale...

The New VTScada Anywhere Client



1. Page 1 - Unacknowledged Alarm Points Summary

0002		FOUL PUMP SECTION			Main 06 Feb 2008 12:02
0014	5	REFLUX VALVE 1	TRIPPED		Foul Pump Inlet Valve
0003		STORM PUMP SECTION			Main 06 Feb 2008 12:02
0006	3	STORM PUMP 2	MANUAL		Storm Pump Unit
0014	5	HYD VALVE 2	TRIPPED		Storm Pump Hydraulic Valve
0030	5	ROTORK VALVE 4	TRIPPED		Storm Pump Bypass Rotork Valve
0004		FINE SCREEN SECTION			Main 06 Feb 2008 12:02
0006	3	FINE SCREEN 2	MANUAL		Fine Screening Unit
0022	2	OUTLET PK10	MOVING		Fine Screen Outlet Penstock
0005		ELECTRICAL DISTRIBUTION SECTION			Main 06 Feb 2008 12:02
0006	8	MAINS ACB 3	TRIPPED		Mains to Fine Screens Feeder
0014	8	COARSE ACB 7	TRIPPED		Gen to Coarse Screens Feeder
0022	8	FOUL ACB 11	TRIPPED		Gen to Foul Pump Feeder
0030	8	GEN ACB 15	TRIPPED		Gen to Fine Screens Feeder
0006	7	FINE AMPS	5.46	A	Fine Screens Supply
0008	7	FOUL AMPS	5.44	A	Foul Pumps Supply
0010	7	STORM AMPS	18.64	A	Storm Pumps Supply
0011	7	GEN VOLTS	380.08	V	1300 KVA Generator Supply
0007		LEVEL AND RAINFALL DATA			Main 06 Feb 2008 12:02
0005	4	ALLEN LEVEL	0.94	M	Measured River Level
0009	4	TORRIDGE LEVEL	0.32	M	Measured River Level
0010	8	TORRIDGE RAIN	9.32	mmph	Measured Rainfall
0011	6	TAW LEVEL	7.94	M	Measured River Level

Why a good alarms management is critical?

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

- Main issues
  - Avalanche of alarms
  - Too many constant alarms
  - Alarms not understood by operators
  - Too many critical alarms

Alarm Management Issue Example #1

- Texaco Refinery Incident, Milford Haven, UK, 1994:
  - https://www.hse.gov.uk/comah/sragtech/casetexaco94.htm
  - Explosion and fire of 20 tons of flammable hydrocarbons five hours after an electrical storm
  - 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

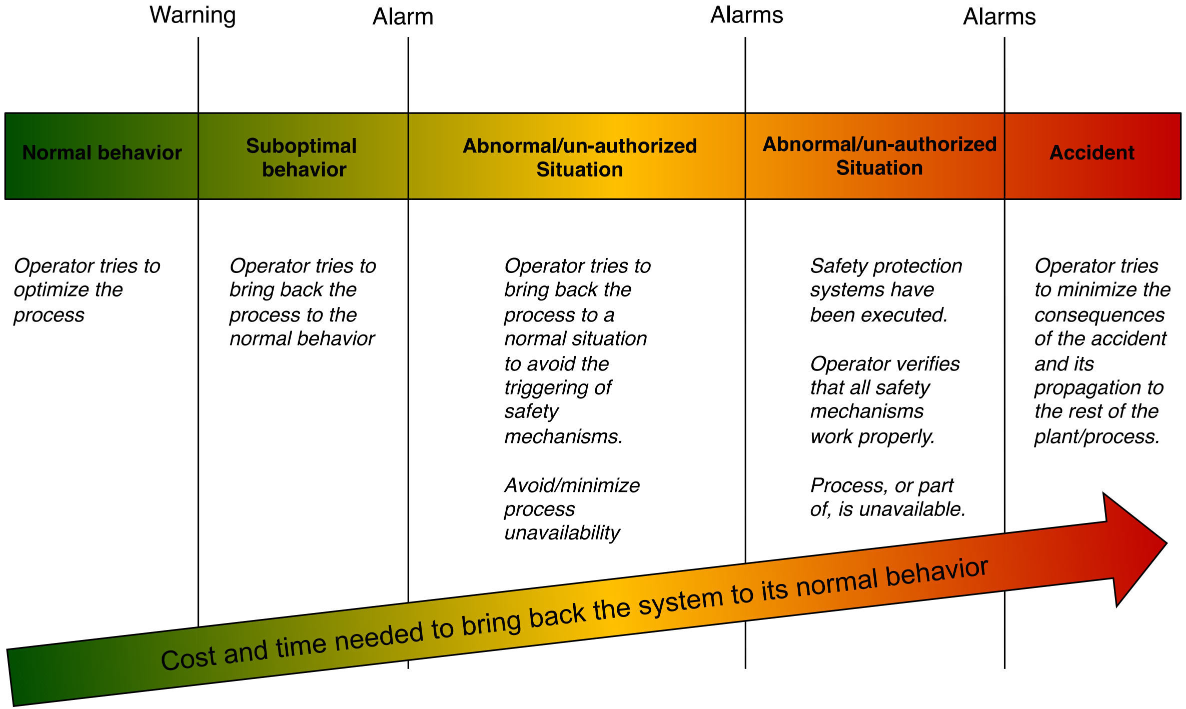
Alarm Management Issue Example #2

- Esso Longford, Australia (1998):
  - Esso natural plant gas in Lonford, Victoria, Australia
  - Pressure vessel ruptured resulting in a conflagration
  - Fire lasting for two days affecting most of the plant
  - 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
  - https://en.wikipedia.org/wiki/Esso_Longford_gas_explosion

Alarm Management Issue Example #3

- Chemical plant incident, FR
  - http://www.aria.developpement-durable.gouv.fr/outils-dinformation/films/film-alarme-toxique-en-salle-de-controle/ (french)
  - Misinterpretation of alarms transforming a usual hardware failure into an accident

Identification of Process States


Warning
Alarm
Alarms
Alarms
Normal behavior
Suboptimal behavior
Abnormal/un-authorized Situation
Abnormal/un-authorized Situation
Accident
Cost and time needed to bring back the system to its normal behavior

Operator tries to optimize the process

Operator tries to bring back the process to the normal behavior

Operator tries to bring back the process to a normal situation to avoid the triggering of safety mechanisms.

Avoid/minimize process unavailability

Safety protection systems have been executed.

Operator verifies that all safety mechanisms work properly.

Process, or part of, is unavailable.

Operator tries to minimize the consequences of the accident and its propagation to the rest of the plant/process.

Definitions

- Alarms
  - An audible and/or visual **indication** to the operator that an equipment malfunction, process deviation or other **abnormal condition**.
  - It **requires a response/action** within a short period of time.
  - E.g. *Tank full & spilling.*
- Events
  - Informative indication of **normal, or abnormal**, process/function which if ignored does not put the process in danger.
  - E.g. *Periodic maintenance required, user logged in, temperature increases*

Alarm Properties

- **Time stamp**
  - What is the semantic of the timestamp?
  - Time at which it has been displayed in the alarm screen?
  - Time at which the alarm has been received at the SCADA level?
  - Time at which it has been detected by the low level sensor?
- **Priority**
  - Characterize the importance level of an alarms.
  - Usually 3 levels are enough (4 max)
- **Title**
  - E.g. *High temperature Tank1*
- **Description**
  - Detail of the alarm (building, name, etc.)
- **Remedial action**
  - What should be done by the operators
  - An alarm without remedial action is not an alarm…

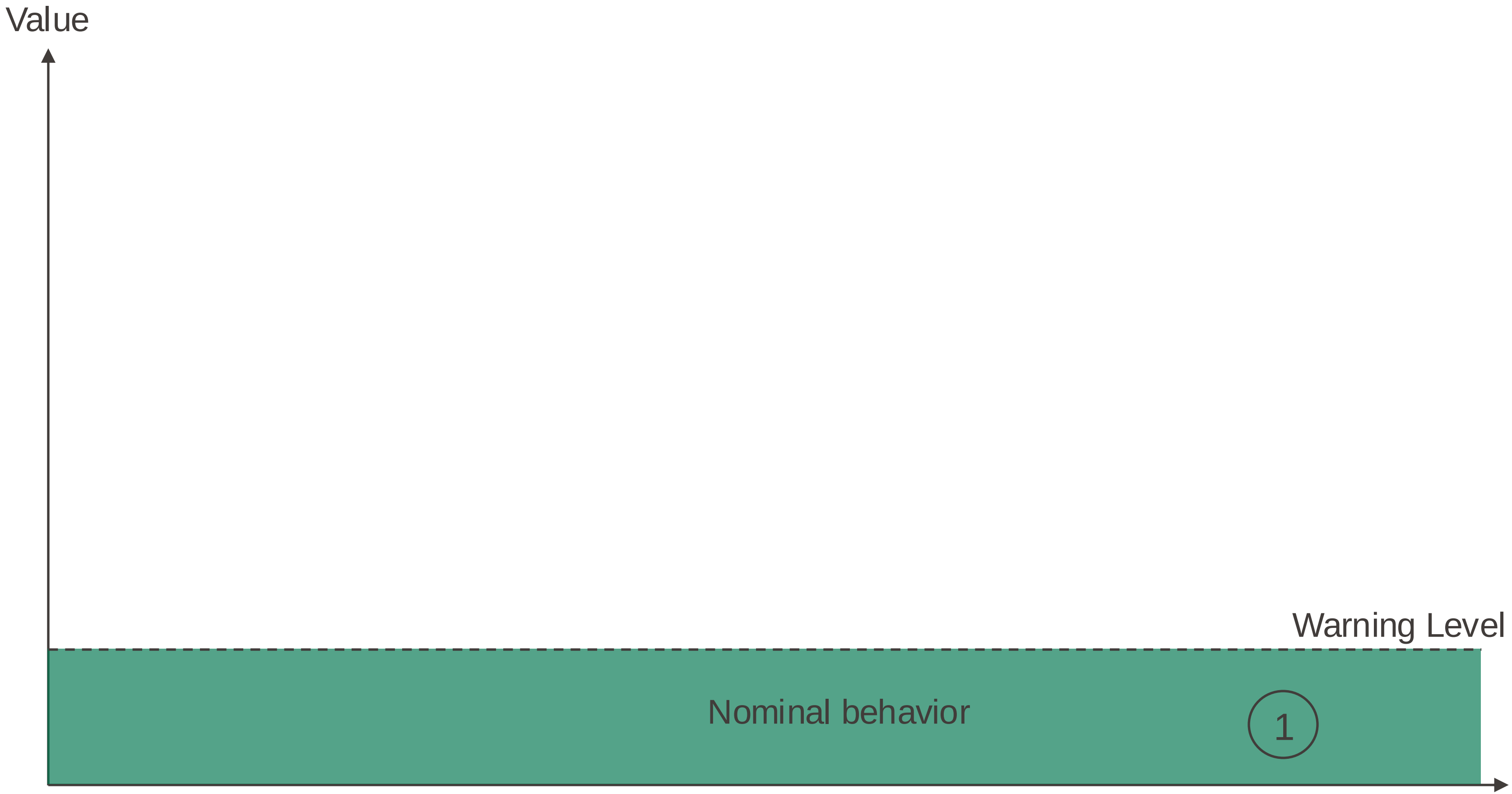
Alarm Types

- **On levels/statuses**
  - Typical for analog measurements or set points

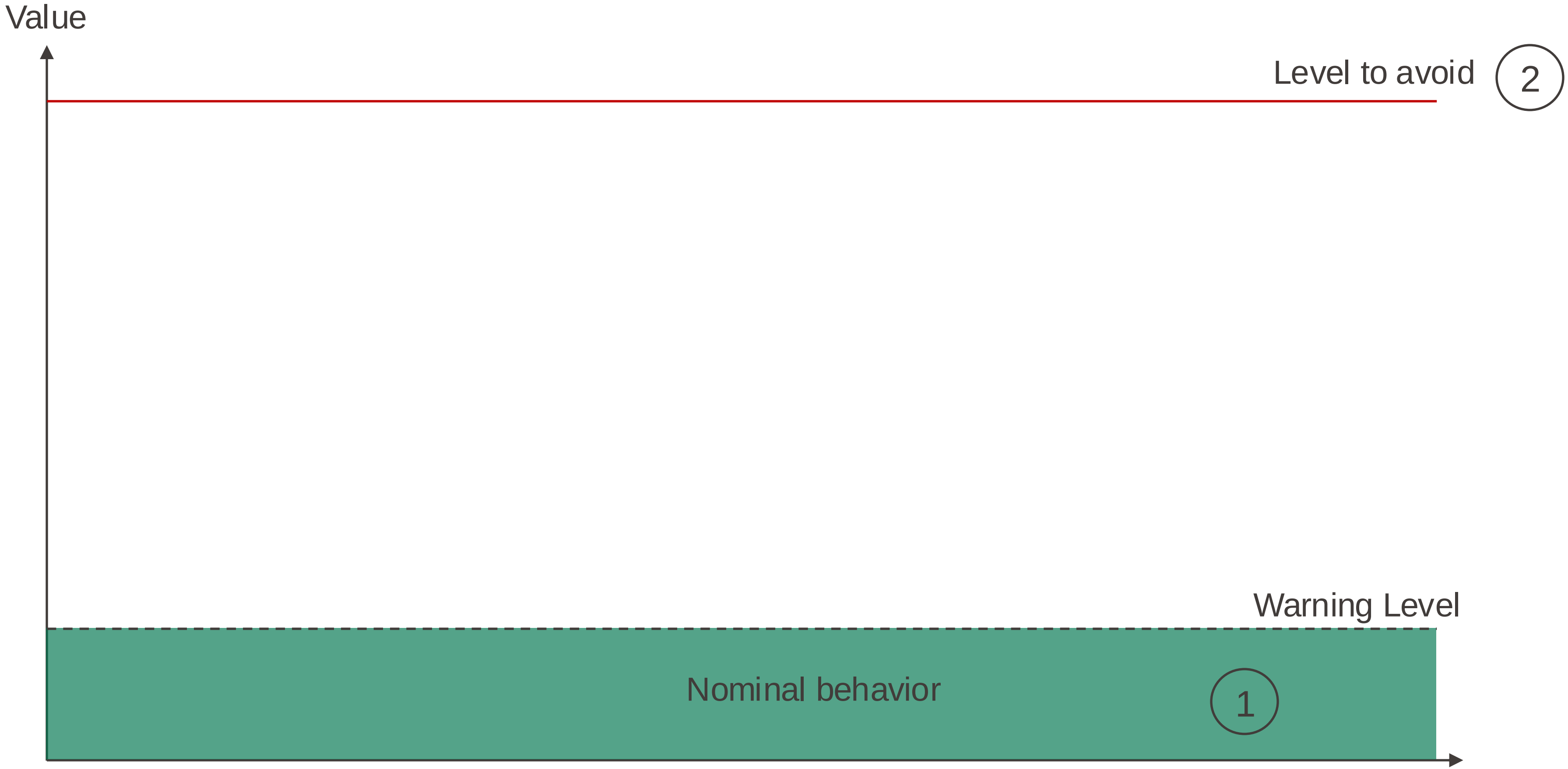
- **On deviation**
  - Deviation between a set point and the sensor feedback
  - Difference between two redundant sensors

- **On rate change**
  - dx/dt
  - E.g. *temperature increases more than 1 degree per minute*

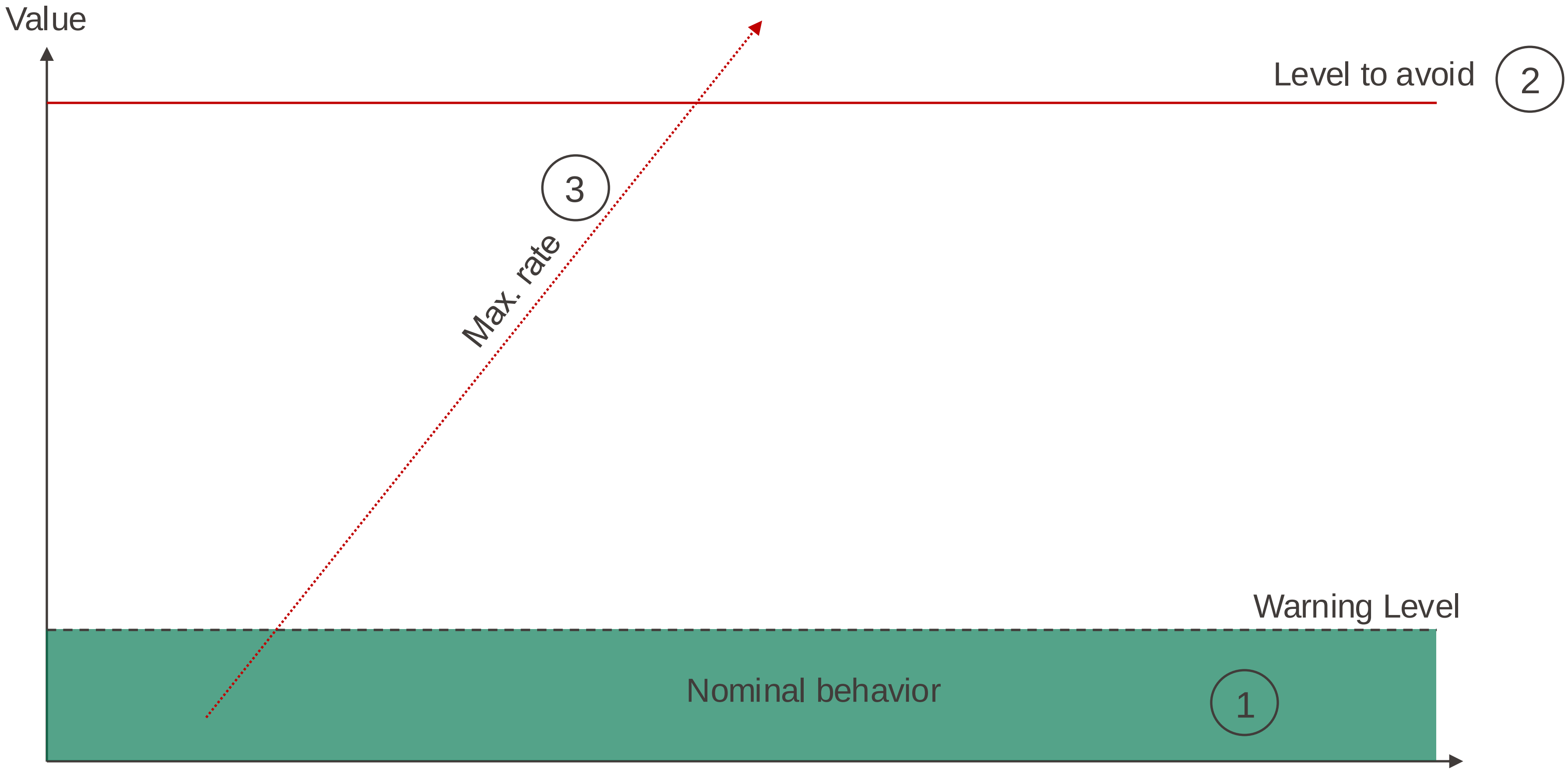
How to define alarm levels



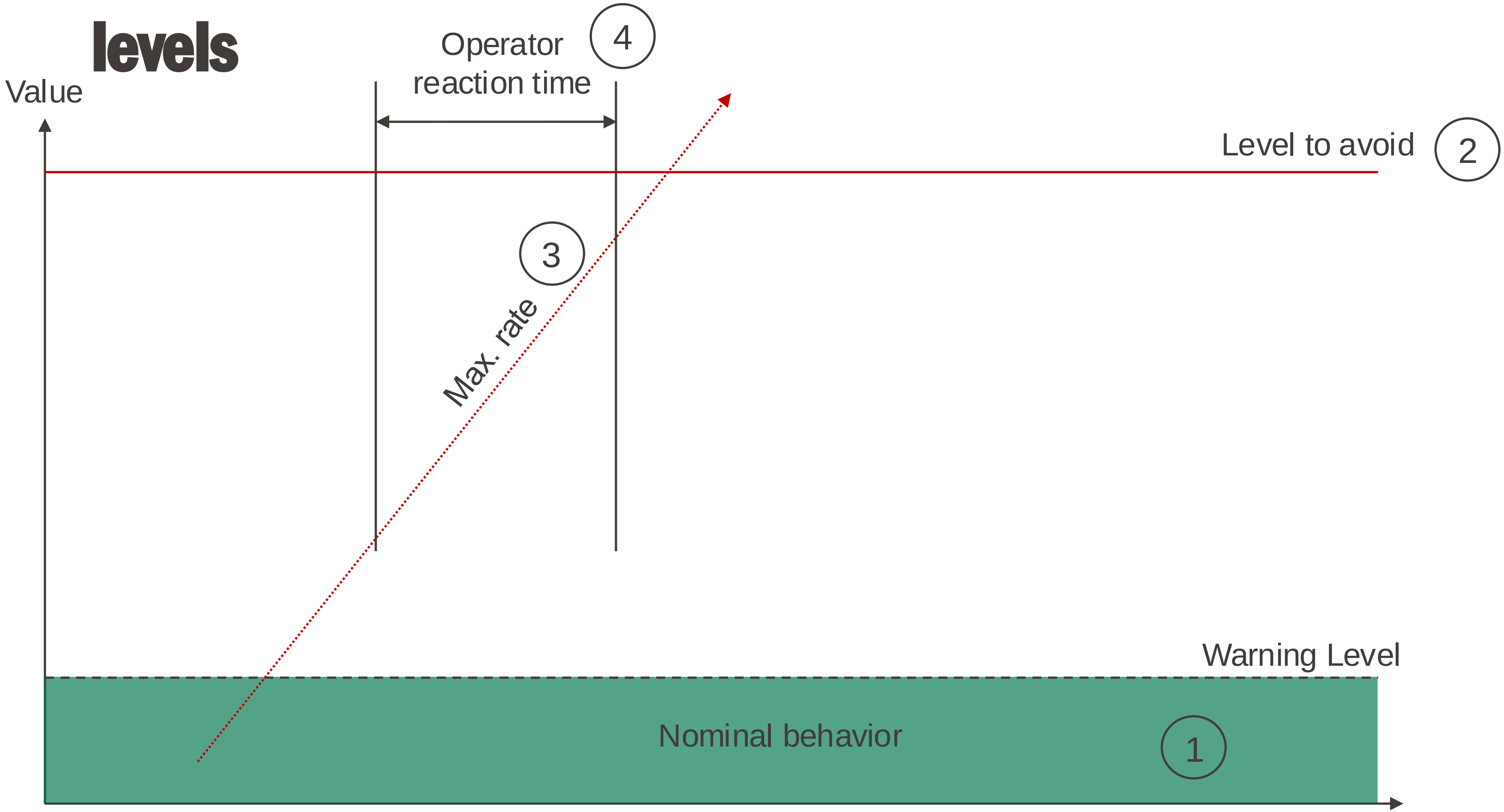
How to define alarm levels



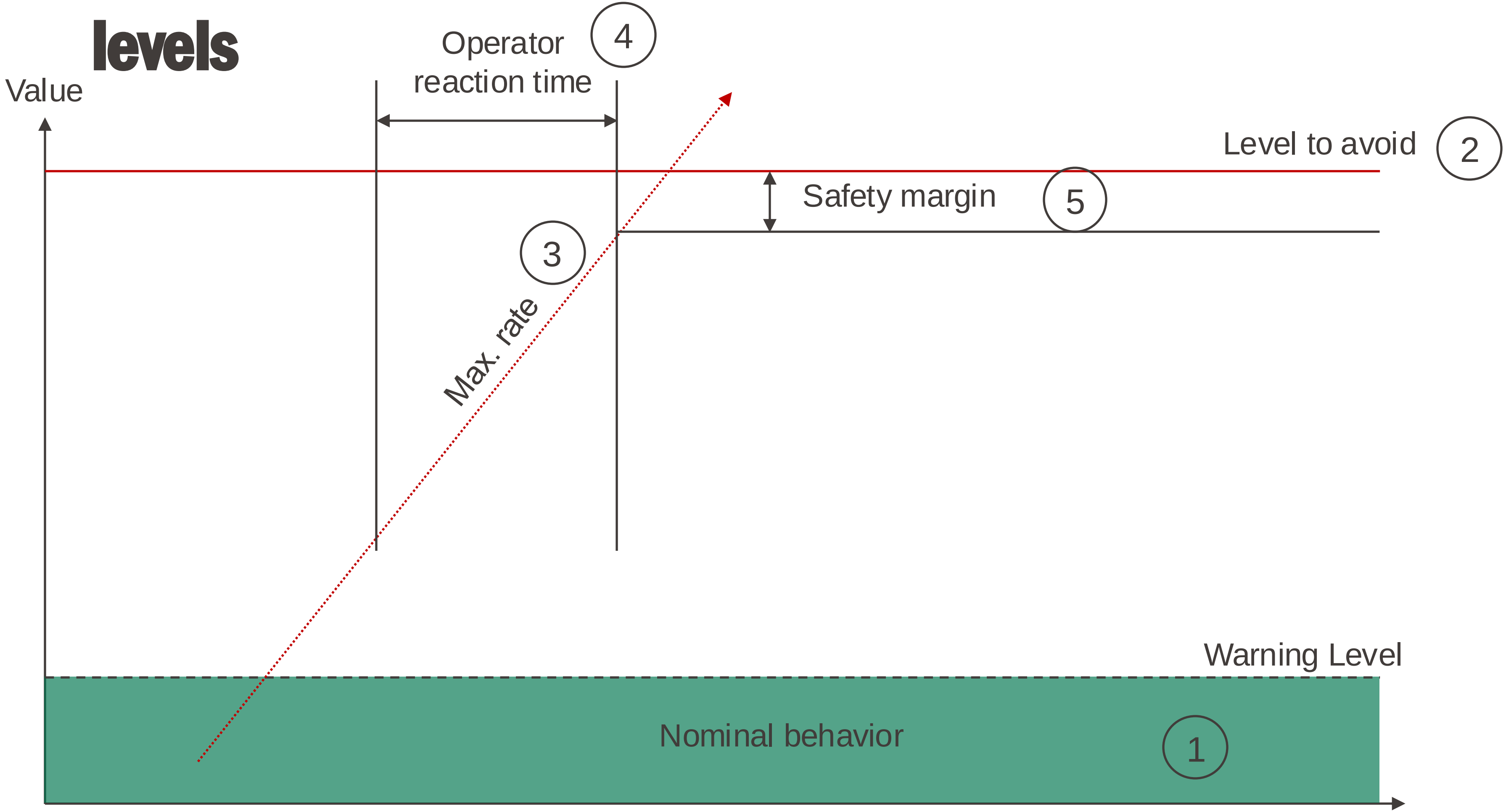
How to define alarm levels



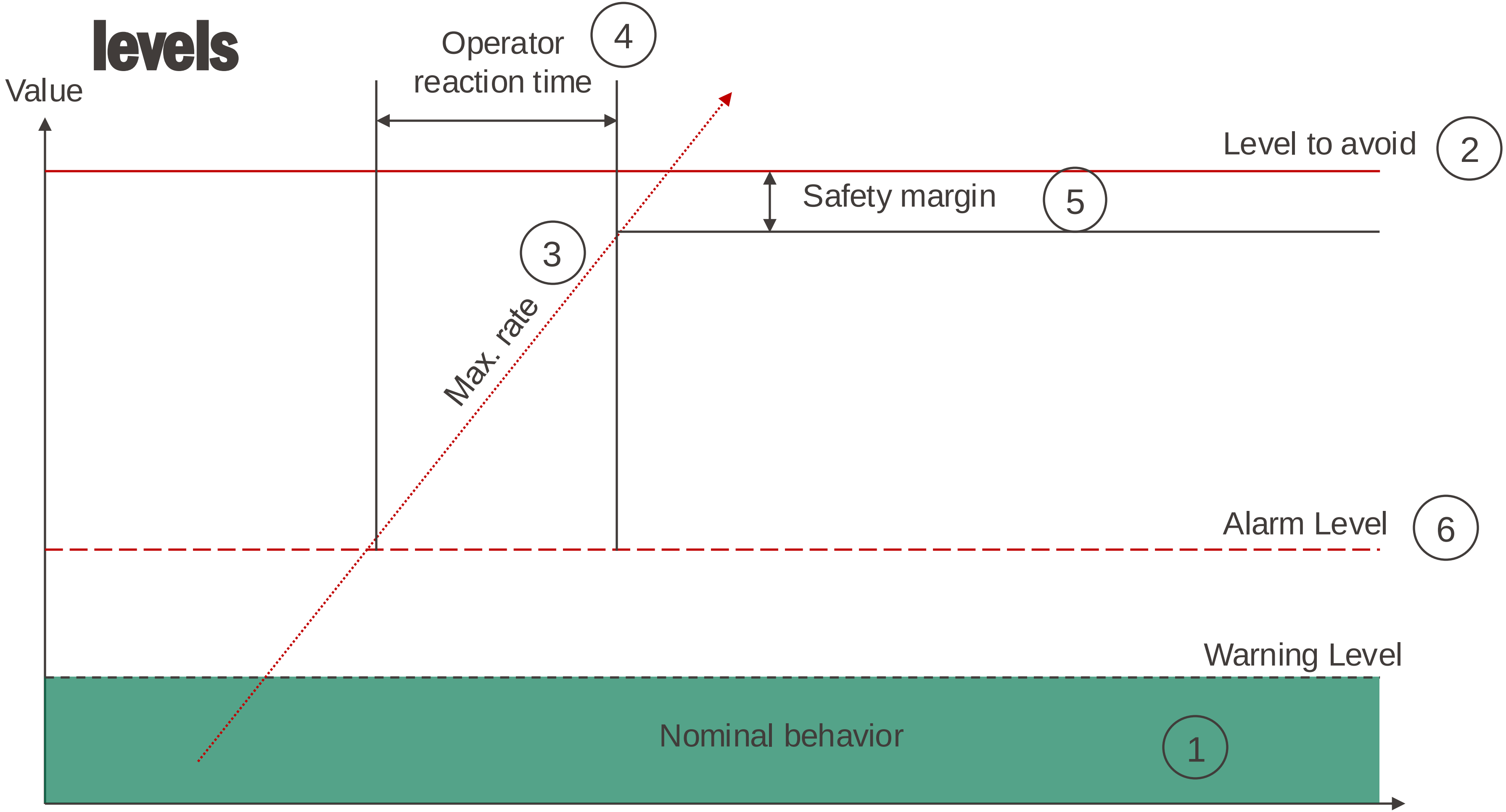
How to define alarm levels



How to define alarm levels



How to define alarm levels



How to define alarm levels?

Alarm Level

=

Critical Level

-

Safety Margin

-

Operator Reaction Time * Max Rate

Alarms Prioritization

Consequences of the alarms in terms of persons, environment, cost, hardware

Reaction Time	Low Impact	Major Impact	Severe Impact
< 10 minutes	Medium	High	High
10 to 20 minutes	Low	Medium	Medium
> 25 minutes	Low	Low	Medium
> 40 minutes	No alarm	No alarm	No alarm

Time during which the operator can perform the mitigation actions. Time depends on the process/equipment.

Performance Critera
ISA 18.2

- Nominal frequency
  - Less than 1 alarm / 10 minutes per operator
- Maximal frequency
  - 1 alarm / 5 minutes per operator
- Avalanche situation
  - More than 10 alarms in 10 minutes
- End of avalanche situation
  - Less than 5 alarms in 10 minutes
- Recommended average number of active alarms
  - Less than 10

Alarm management techniques aim at achieving these levels of performance!

Alarm Management Standards 1/2

- EEMUA Publication 191
  - “*EEMUA Publication 191 Alarm systems - a guide to design, management and procurement*”
  - First published in 1999, last update in 2013
  - http://www.eemua.org/Products/Publications/Print/EEMUA-Publication-191.aspx
  - https://cds.cern.ch/record/1646801?ln=en (not yet at the CERN library)
  - EEMUA is the engineering equipment and materials users association based in UK
  - Members seem to be more from the oil&gas industry (e.g. BP, Exxon, Mobil, Shell, Total, Total)
  - First international recommendations on alarm management (not a standard)

- NAMUR NA 102
  - “*Alarm Management*”
  - Published in 2008
  - http://www.namur.net/en/recommendations-and-worksheets/current-nena.html
  - NAMUR is an international association of automation technology users based in Germany
  - Members seem to be more from the chemical/pharmatical industry (e.g swiss members are BASF, Roche, Novartis)

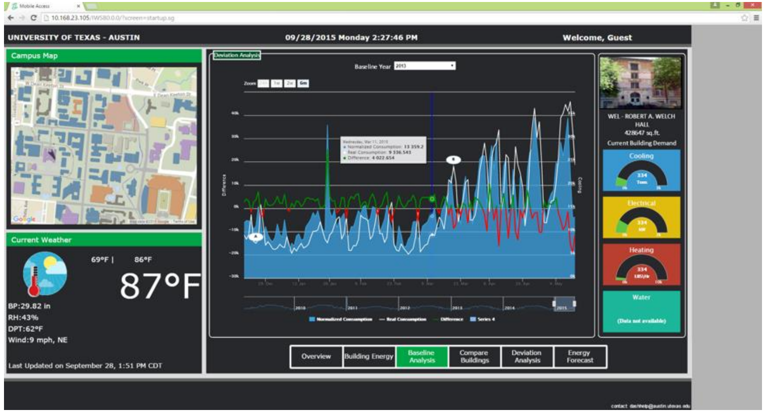
Alarm Management Standards 2/2

- ANSI/ISA-18.2
  - “*Management of Alarm Systems for the Process Industries*”
  - Published in 2009
  - Full content: https://cds.cern.ch/record/1393440/files/ANSI-ISA-18-2-2009.pdf
  - Supposed to be built on the work of all the other standards (EEMUA, NAMUR, ASM)
  - American National Standards Institute – International Society of Automation

- IEC 62682 Ed. 1.0
  - “*Management of alarm systems for the process industries*”
  - Published in 2014
  - Second edition forecasted for January 2023
  - Lead by the same people as ISA-18.2
  - https://webstore.iec.ch/publication/7363&preview=1

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
  - Amount of the data to store and plot
  - E.g. 1.5 TB of data for CERN’s SCADA power system
  - Performance limited by the underlying archiving infrastructure

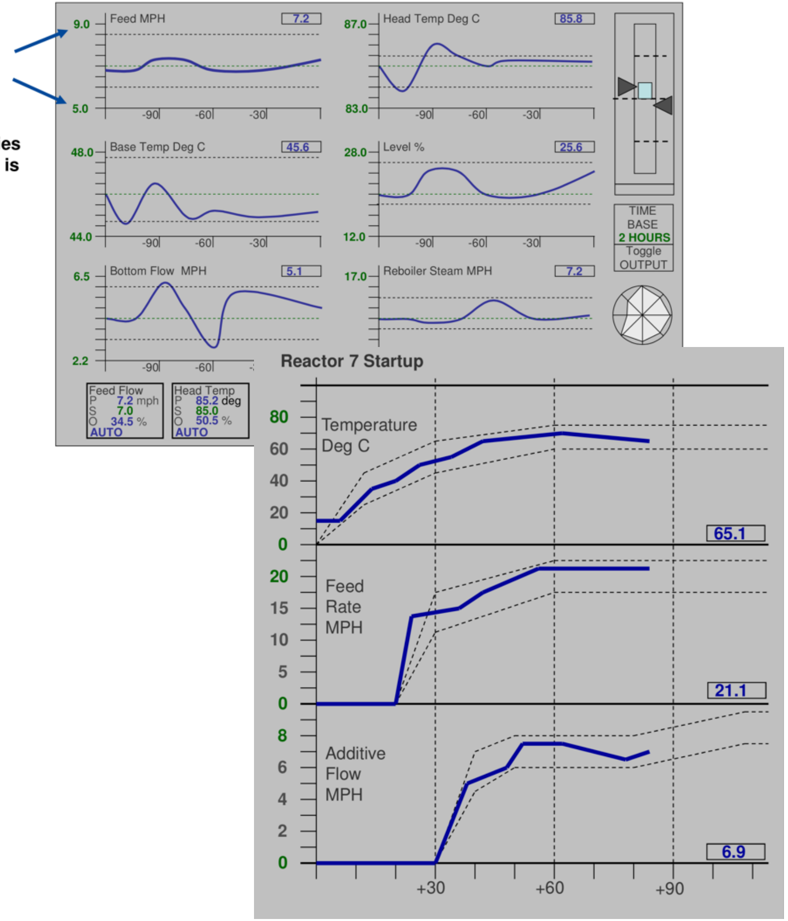


Indusoft
http://www.indusoft.com/blog/2016/01/04/trends-in-automation-trends-to-watch-in-2016/

Trends
More than values

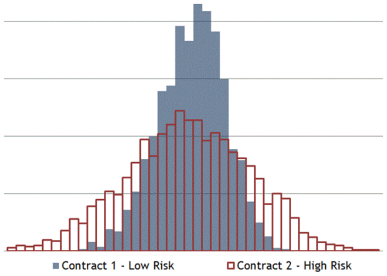
- Should always allow operators to answer
  - How does the system evolve over time
  - How far is the system from its boundaries

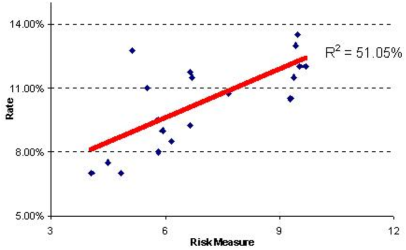
- Proper Auto-ranges
- Show boundaries of “What is good”

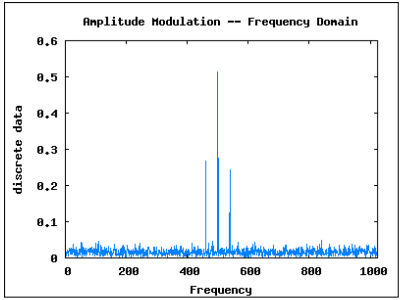


Archiving & Historian for analysis

- 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
  - SAIFI
    - System Average Interruption Frequency Index
  - SAIDI
    - System Average Interruption Duration Index







More SCADA functionalities

- printing logs and alarms (hard-copy)
- reporting
- display documentation and on-line help
- notifications via email and SMS, voice, video (webcams)
- access to non-process databases (e.g. weather forecast)
- optimisation functions
- communication with other control centres
- personal and production planning (can be on other workstations)
- web-access

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
- Big Data, AI (AI assisted operator, AI engineering/tunning, etc.)
- 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 & SCADA

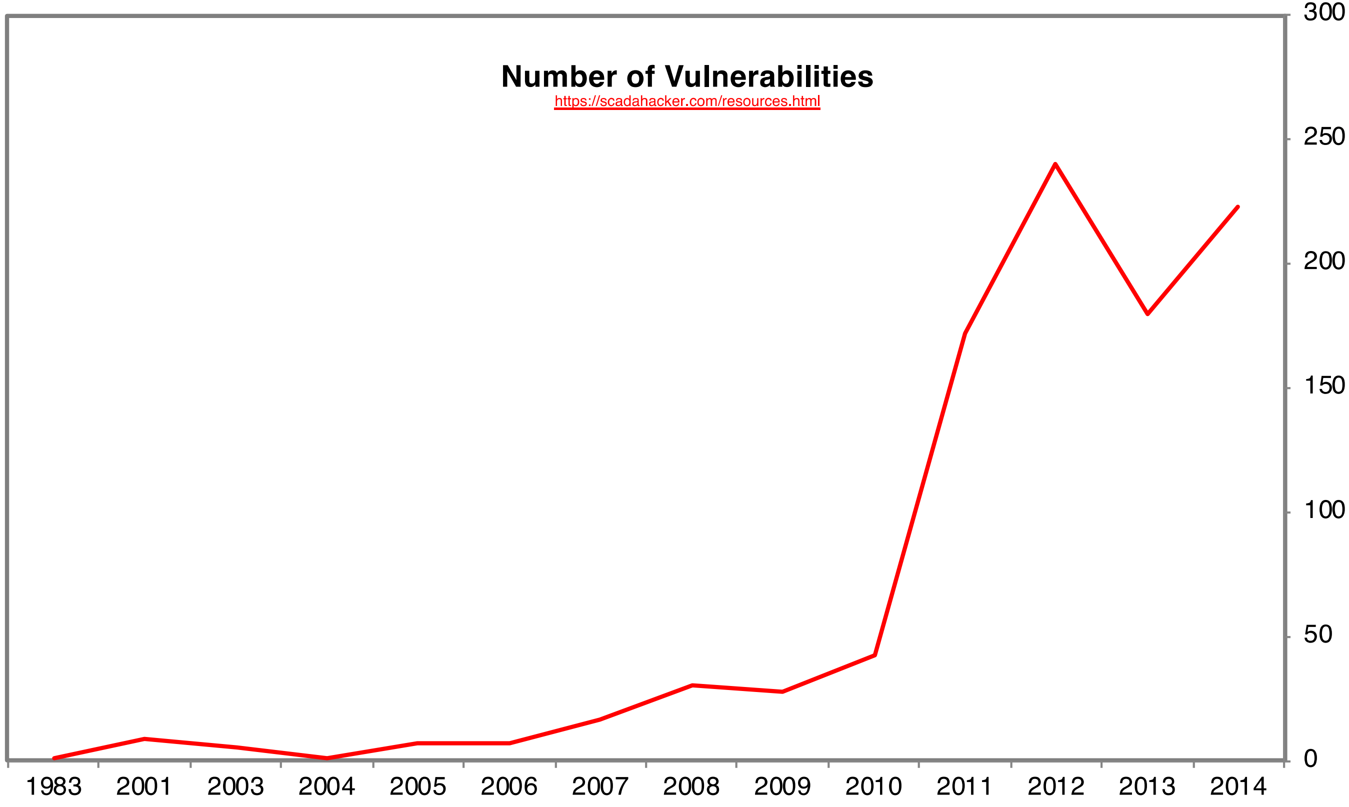
SCADA Cyber Security Context

- Historically SCADA systems have been closed/isolated systems
  - Custom made & proprietary protocols and systems
- Control networks are converging towards corporate networks
  - Business requirements, decision support systems, cost reduction
- Standardization of SCADA components
  - Protocols, hardware, OS, databases, graphical libraries, web technologies, etc.
  - Proprietary field buses replaced by Ethernet LAN and TCP/IP
  - VPN connections from outside for remote maintenance
  - Extensive use of open source libraries or softwares
- Extensive use of ICT protocols & applications
  - HTTP, FTP, SSH, SMTP, SNMP, etc.
  - Wireless LAN, Notebooks, USB sticks
- Poorly secured systems
  - Communications with no authentication
  - Very little encryption
  - Unrestricted access
  - Default password

Incidents

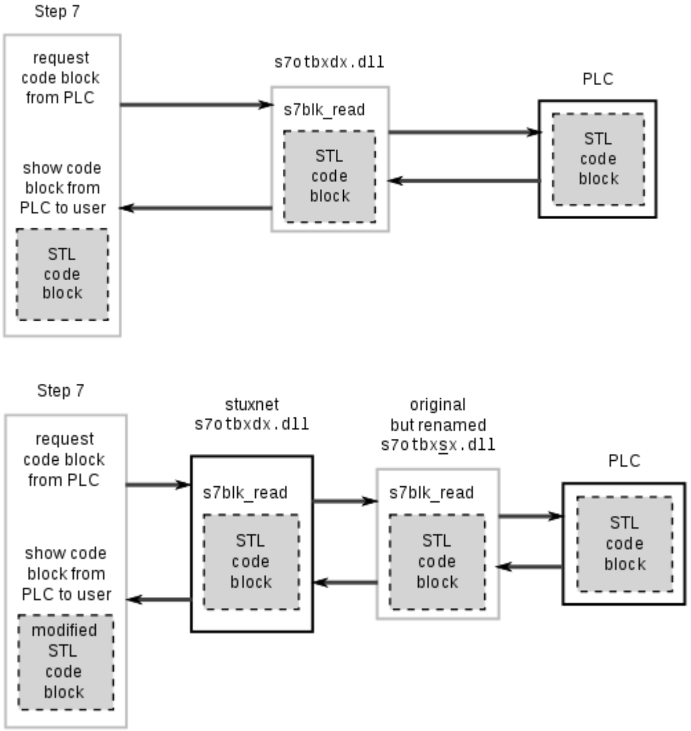
- ~2000
  - Siberia: ICT attack on air defence system
  - Iraq: attacks on banking and communication systems
- 2005
  - Greece: ICT intrusion in mobile communication system by foreign intelligence
  - USA: various electrical blackouts on a regional scale by cyber attacks
- 2007
  - Estonia: prolonged attack against many national organizations (finance, public admnistration, medi)
- 2008
  - Syria, Georgia: cyber attack targeting air defense system and C&C centres in support of conventional operations
- 2009
  - USA: Video feeds of drones (Iraq) intercepted
- 2010
  - Iran: stuxnet
- 2012
  - Worldwide: red october (*https://securelist.com/blog/incidents/57647/the-red-october-campaign/*)
- 2014
  - Germany: attack of an unmanned steel mill resulting in massive damages
- 2018
  - - «*c.a. 40% of industrial control system (ICS) were attacked by malicious software at least once in the first half of 2018.*» https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h1-2018/87913/
- 2021
  - Water treatment facility intrusion in Florida
  - https://edition.cnn.com/2021/02/13/us/florida-hack-remote-access/index.html

Trends


Number of Vulnerabilities
https://scadahacker.com/resources.html
300
250
200
150
100
50
0
1983
2001
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014

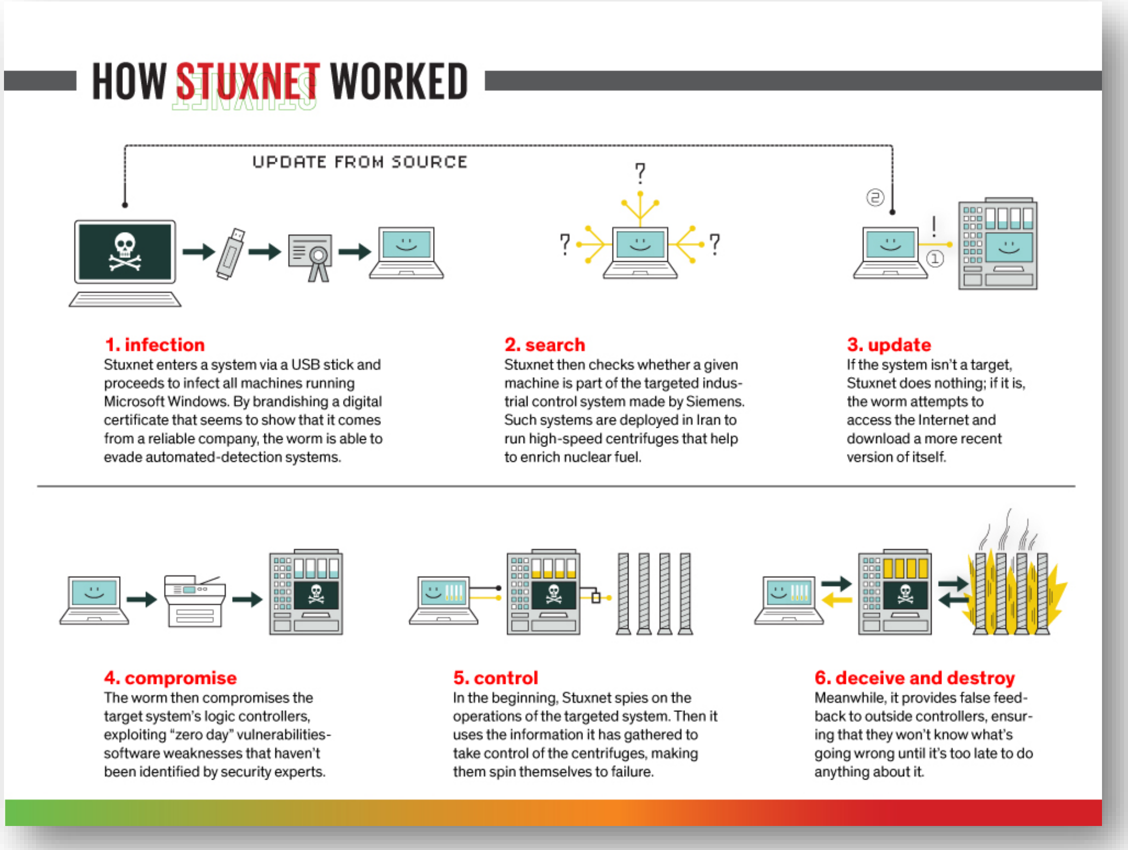
Stuxnet - Overview

- Worm discovered in June 2010
- Targeted specific PLCs controlling specific frequency converter drives
- Initially spread through USB keys
- Spreads via Windows using 4 0-day vulnerabilities, but targets PLC
- Man in the middle attack:
  - Replaces the communication libraries (DLL)
  - sends faked (pre-recorded) sensor values so the system does not shutdown when abnormal situation is encountered
  - Varies the speed of the centrifuges over months to slowly wear them out and inhibit uranium enrichment while in the meantime everything looks good at the SCADA level



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

Stuxnet - Propagation



HOW STUXNET WORKED

1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

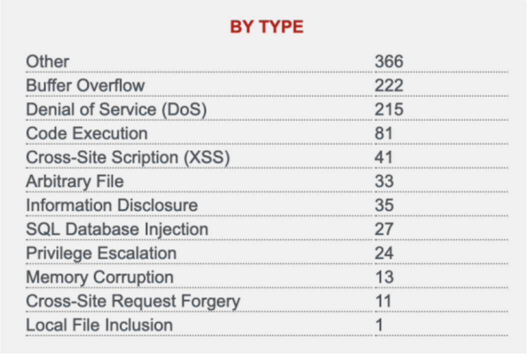
5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

SCADA Attacks

- 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.



BY TYPE

Other	366
Buffer Overflow	222
Denial of Service (DoS)	215
Code Execution	81
Cross-Site Scription (XSS)	41
Arbitrary File	33
Information Disclosure	35
SQL Database Injection	27
Privilege Escalation	24
Memory Corruption	13
Cross-Site Request Forgery	11
Local File Inclusion	1

Vulnerabilities by Type (2000-2015)
https://scadahacker.com/resources.htm

Security Strategies 1/2

- Laptop and removable drive
  - No personal computer on the process/technical network
  - No removable 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

Security Strategies 2/2

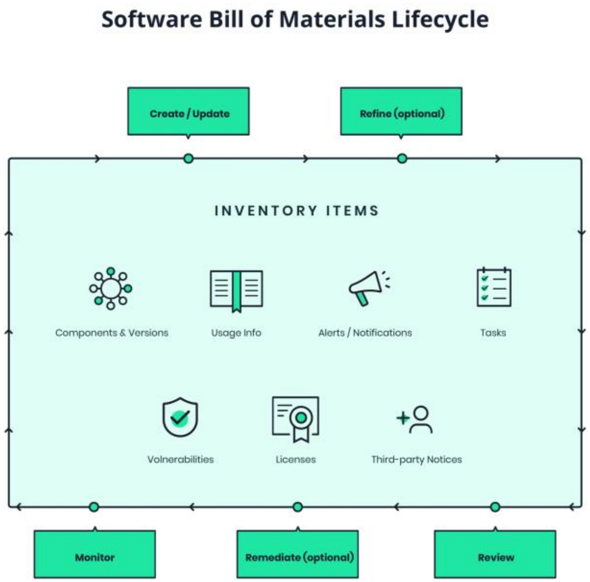
- Defense in depth
  - Identification, Classification and Categorization
  - Electronic Security Controls and Measures
  - Physical Security Controls and Measures
  - Security Review/Audits
  - Incident Response Training

- Be aware of new vulnerabilities and apply patches
  - Vulnerability Databases
    - ICS-CERT, NVD, CVE, Bugtraq, OSVDB, Mitre Oval Repositories, exploit-db, Siemens Product CERT
  - ATT&CK for Industrial Control Systems
    - https://collaborate.mitre.org/attackics/index.php/Main_Page
  - **Threat Landscape for Supply Chain Attacks, ENSIA**
    - https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

- Be aware of current incidents
  - RISI (Not updated since 2015)
    - http://www.risidata.com/
  - USA ICS-CERT
    - https://ics-cert.us-cert.gov/
  - https://www.misp-project.org/communities/

Asset Management and SBOM

- But how can you know if a vulnerability applies to you?
- Need for a proper asset management
  - List of assets installed or in production
- Need for Software Bills Of Materials (SBOM) for each asset
  - List of software and libraries used in an industrial products
  - Equivalent to the list of ingredients when buying food at the supermarket
  - Required by the EU to be provided by manufacturers in 2027…
- Should be an integral part of the asset management



https://apiiro.com/blog/practical-guide-to-sbom/

Cyber Security Standards

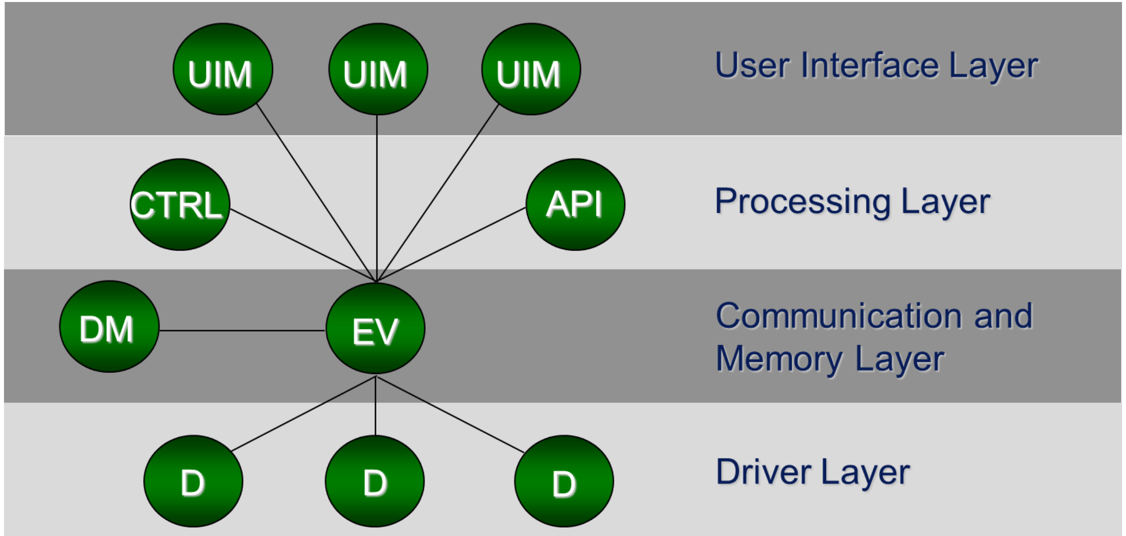
- Know the security standard applicable to the industry
  - E.g. IEC 62351 for most protocols used in power system industry
  - E.g. Transportation Security Administration (TSA), Pipeline Security Guidelines, April 2011
  - NERC (power industry), NIST, NRC (nuclear plant)
  - Framework for Improving Critical Infrastructure Cybersecurity, NIST
    - https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
  - IEEE 1888.3-2013: Standard for Ubiquitous Green Community Control Network: Security
    - Security requirements, system security architecture definitions, and a standardized description of authentication and authorization, along with security procedures and protocols, are specified. This standard can help avoid unintended data disclosure to the public and unauthorized access to resources, while providing enhanced integrity and confidentiality of transmitted data in the ubiquitous green community control network.
  - IEEE 1686-2013: Standard for Intelligent Electronic Devices Cyber Security Capabilities
    - The functions and features to be provided in intelligent electronic devices (IEDs) to accommodate critical infrastructure protection programs are defined in this standard. Security regarding the access, operation, configuration, firmware revision and data retrieval from an IED are addressed. Communications for the purpose of power system protection (teleprotection) are not addressed in this standard.
  - IEEE P1711: Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links
  - IEEE P2030.102.1: Standard for Interoperability of Internet Protocol Security (IPsec) Utilized within Utility Control Systems

SCADA Examples

Siemens WinCC OA

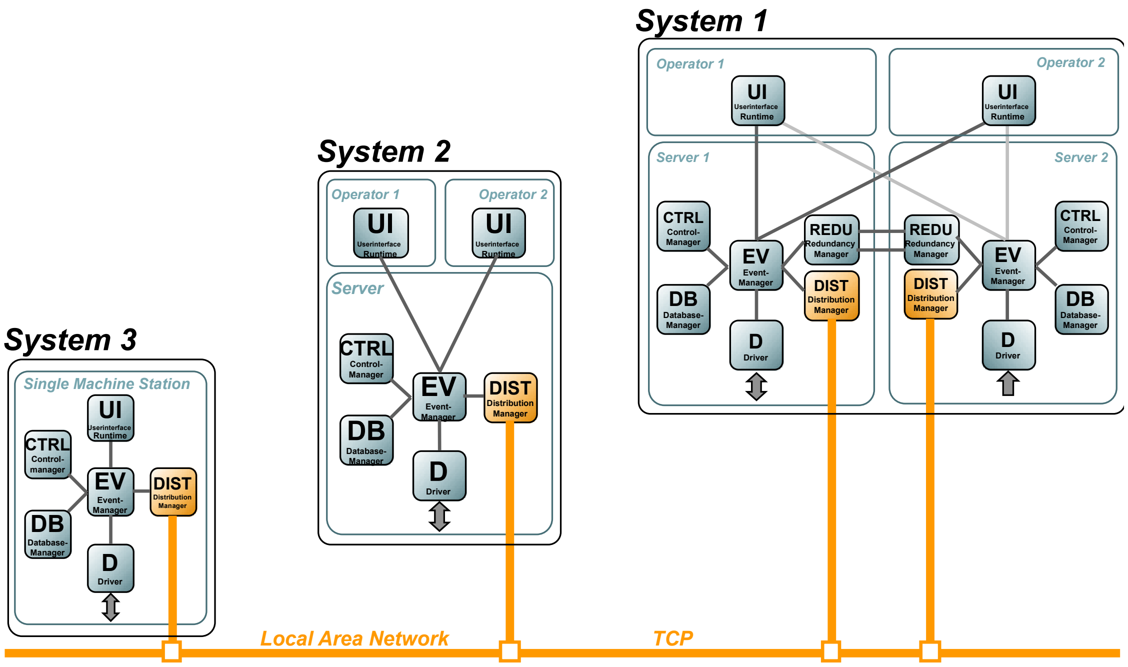
- SIMATIC WinCC Open Architecture is a Siemens product
- Basis of most industrial supervision systems at CERN
- Framework to build a SCADA system
  - Not bound to any domain
  - Include main traditional SCADA functionalities:
    - Engineering (device creation, device settings, etc.)
    - Acquisition (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

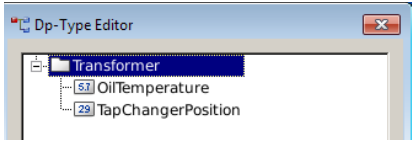
WinCC OA Architecture

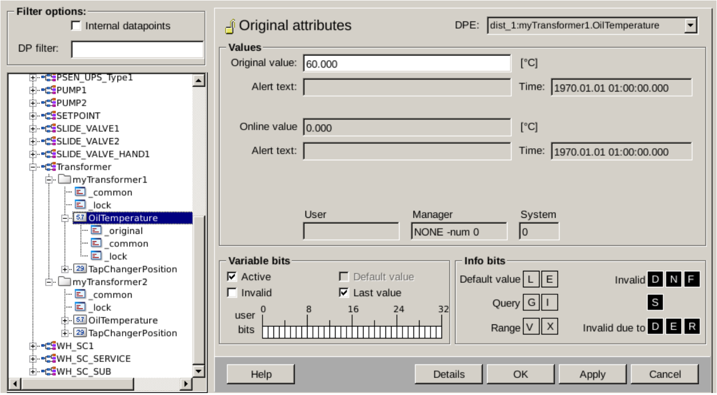


Copyright – WinCC OA ETM Siemens

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




Filter options:
☐ Internal datapoints
DP filter:

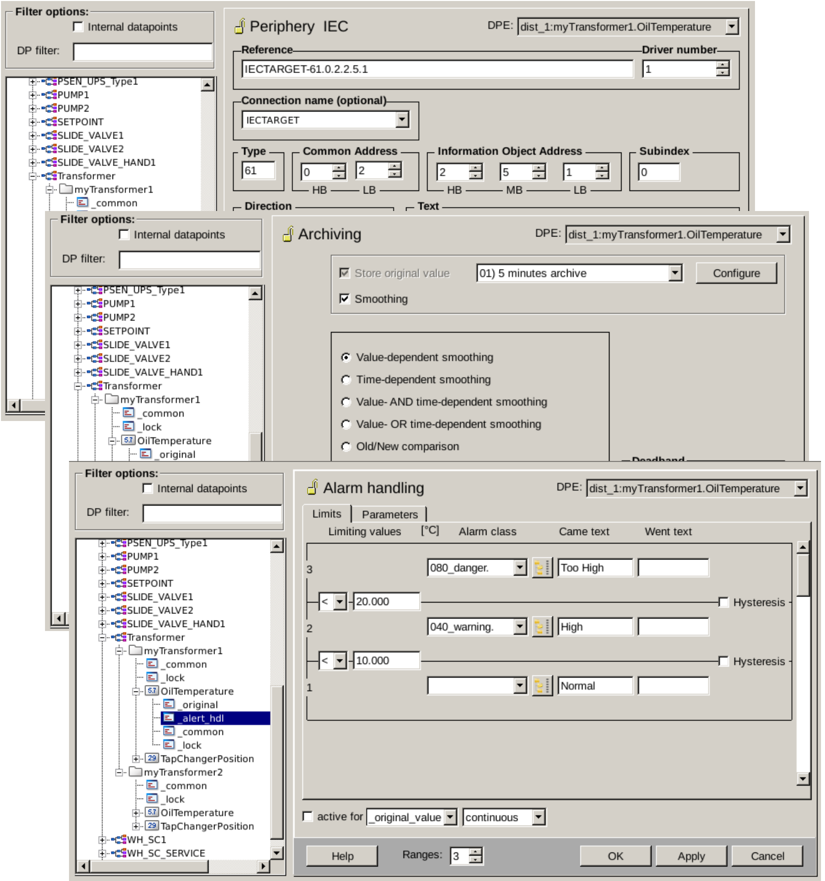
Original attributes
DPE: dist_1:myTransformer1.OilTemperature

Values
Original value: 60.000 [°C]
Alert text:
Time: 1970.01.01 01:00:00.000
Online value 0.000 [°C]
Alert text:
Time: 1970.01.01 01:00:00.000
User
Manager NONE -num 0
System 0

Variable bits
☑ Active
☐ Invalid
☐ Default value
☑ Last value

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)



Filter options: □ Internal datapoints
DP filter:

PSEN_UPS_Type1
PUMP1
PUMP2
SETPOINT
SLIDE_VALVE1
SLIDE_VALVE2
SLIDE_VALVE_HAND1
Transformer
myTransformer1
_common
_lock
OilTemperature
_original
_alert_hdl
_common
_lock
TapChangerPosition
myTransformer2
_common
_lock
OilTemperature
TapChangerPosition
WH_SC1
WH_SC_SERVICE

Periphery IEC — DPE: dist_1:myTransformer1.OilTemperature

Reference: IECTARGET-61.0.2.2.5.1 — Driver number: 1

Connection name (optional): IECTARGET

Type: 61 — Common Address: 0 (HB), 2 (LB) — Information Object Address: 2 (HB), 5 (MB), 1 (LB) — Subindex: 0

Direction — Text

Archiving — DPE: dist_1:myTransformer1.OilTemperature

☑ Store original value — 01) 5 minutes archive — Configure

☑ Smoothing

● Value-dependent smoothing
○ Time-dependent smoothing
○ Value- AND time-dependent smoothing
○ Value- OR time-dependent smoothing
○ Old/New comparison

Deadband

Alarm handling — DPE: dist_1:myTransformer1.OilTemperature

Limits | Parameters

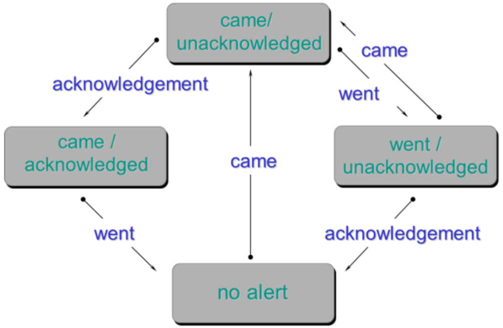
	Limiting values [°C]	Alarm class	Came text	Went text	
3		080_danger.	Too High		
	< 20.000				□ Hysteresis
2		040_warning.	High		
	< 10.000				□ Hysteresis
1			Normal		

□ active for _original_value — continuous

Help — Ranges: 3 — OK — Apply — Cancel

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



came/ unacknowledged

came

acknowledgement

went

came / acknowledged

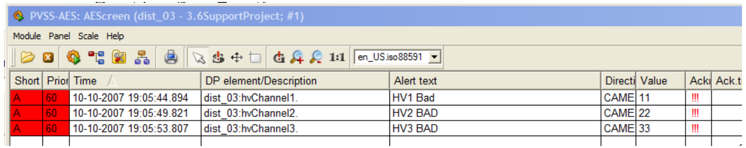
came

went / unacknowledged

went

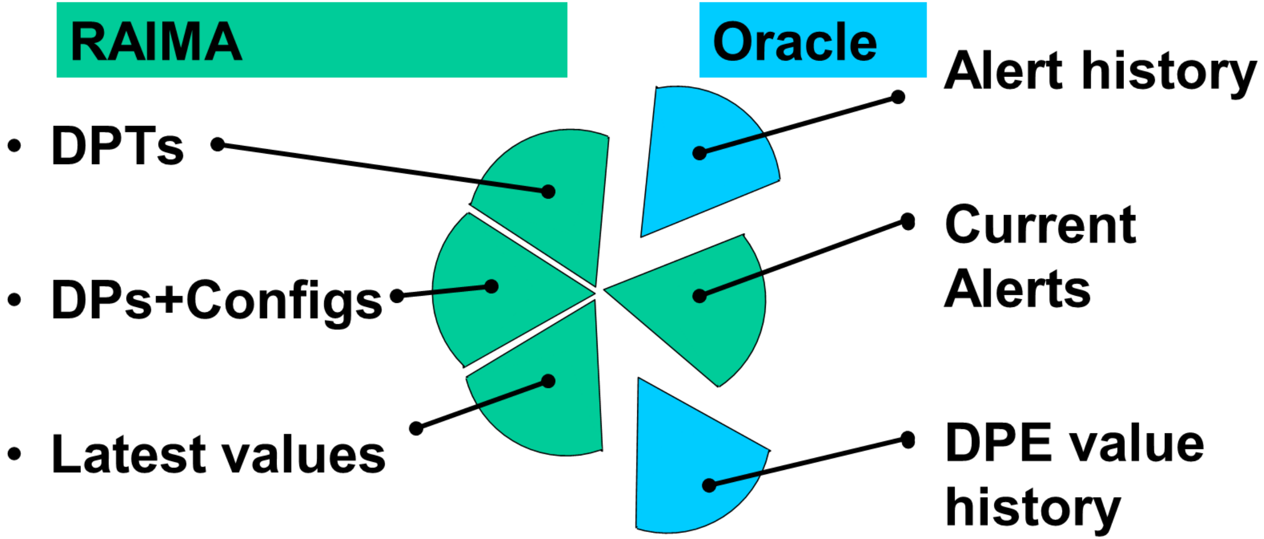
acknowledgement

no alert



Short	Prior	Time	DP element/Description	Alert text	Directi	Value	Ackı	Ack.t
A	60	10-10-2007 19:05:44.894	dist_03:hvChannel1.	HV1 Bad	CAME	11	!!!	
A	60	10-10-2007 19:05:49.821	dist_03:hvChannel2.	HV2 BAD	CAME	22	!!!	
A	60	10-10-2007 19:05:53.807	dist_03:hvChannel3.	HV3 BAD	CAME	33	!!!	

WinCC OA – Archiving



RAIMA

- DPTs
- DPs+Configs
- Latest values

Oracle

Alert history

Current Alerts

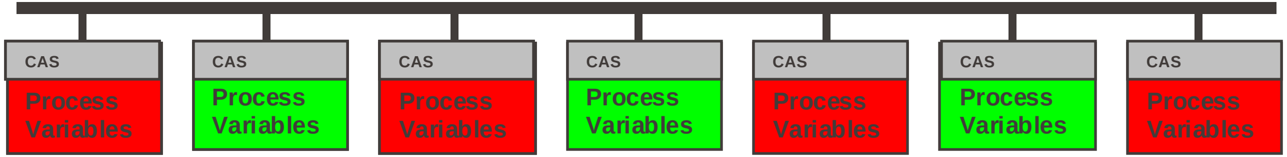
DPE value history

Copyright – WinCC OA ETM Siemens

EPICS

EPICS - Introduction

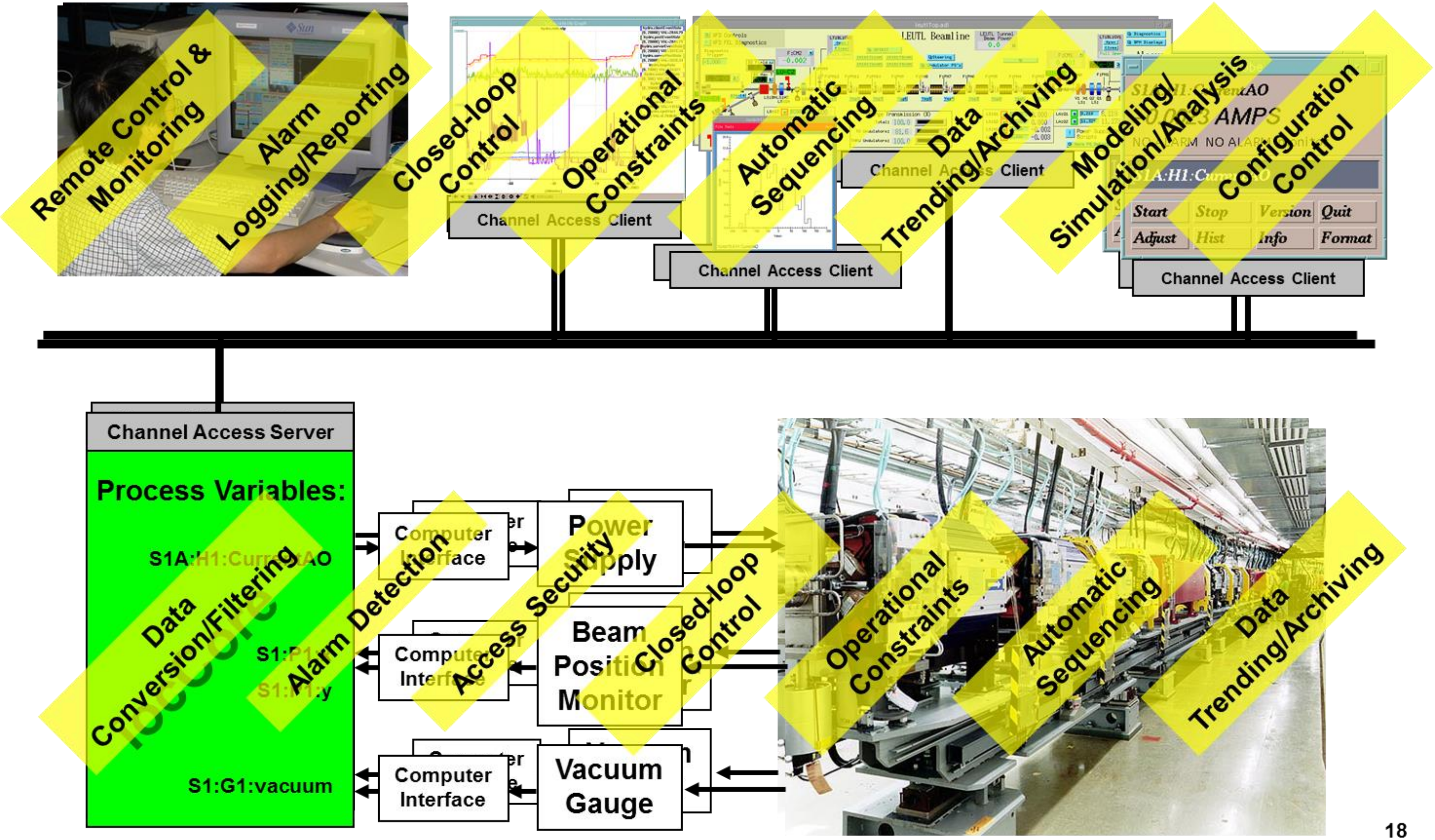
- Experimental Physics and Industrial Control System is an open source software lead by Argonne National Laboratory
- Main domains of application are scientific instruments
  - Particle accelerators, telescopes, etc.
- Set of software components and tools to create a control system
- Network based client/server 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



Remote Control & Monitoring

Alarm Logging/Reporting

Closed-loop Control

Operational Constraints

Automatic Sequencing

Data Trending/Archiving

Modeling/ Simulation/Analysis

Configuration Control

Channel Access Client

Channel Access Client

Channel Access Client

Channel Access Client

Channel Access Server

Process Variables:

S1A:H1:CurrentAO

S1:P1

S1:M1:y

S1:G1:vacuum

Data Conversion/Filtering

Alarm Detection

Access Security

Closed-loop Control

Computer Interface

Computer Interface

Computer Interface

Power Supply

Beam Position Monitor

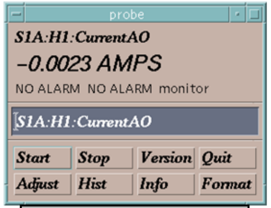
Vacuum Gauge

Operational Constraints

Automatic Sequencing

Data Trending/Archiving

Epics
Data Acquisition



S1A:H1:CurrentAO

-0.0023 AMPS

NO ALARM NO ALARM monitor

S1A:H1:CurrentAO

Channel Access Client

CA Client

CA Server

Channel Access Server

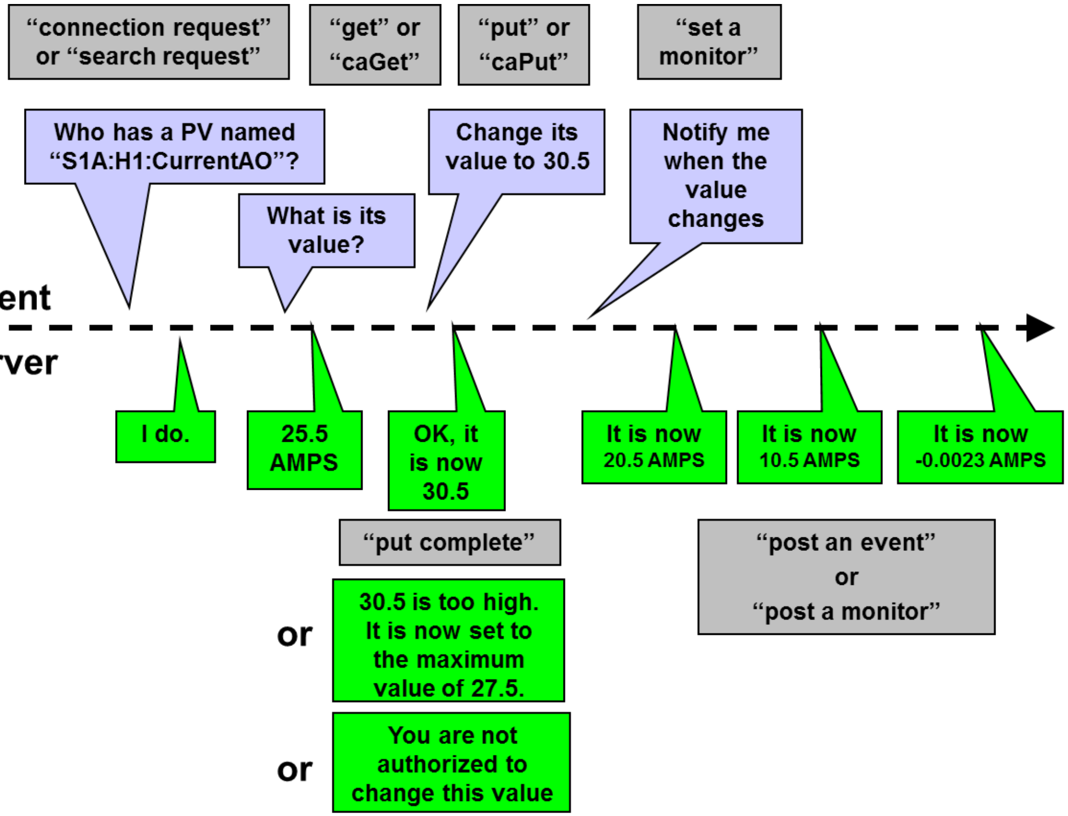
Process Variables:

S1A:H1:CurrentAO

S1:P1:x

S1:P1:y

S1:G1:vacuum



"connection request" or "search request"

Who has a PV named "S1A:H1:CurrentAO"?

I do.

"get" or "caGet"

What is its value?

25.5 AMPS

"put" or "caPut"

Change its value to 30.5

OK, it is now 30.5

"put complete"

or

30.5 is too high. It is now set to the maximum value of 27.5.

or

You are not authorized to change this value

"set a monitor"

Notify me when the value changes

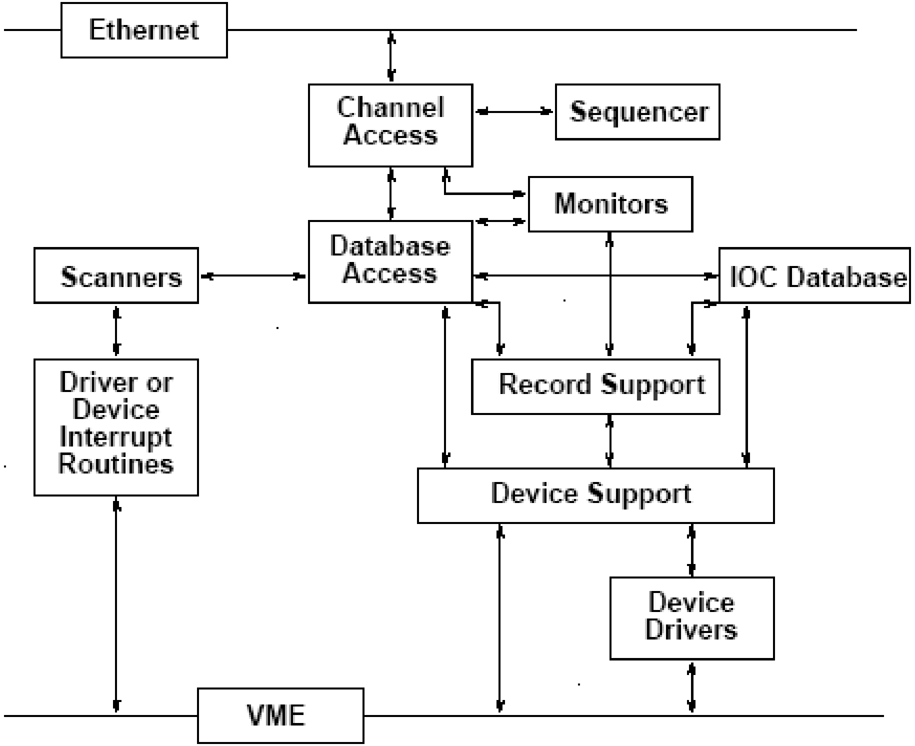
It is now 20.5 AMPS

It is now 10.5 AMPS

It is now -0.0023 AMPS

"post an event"
or
"post a monitor"

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

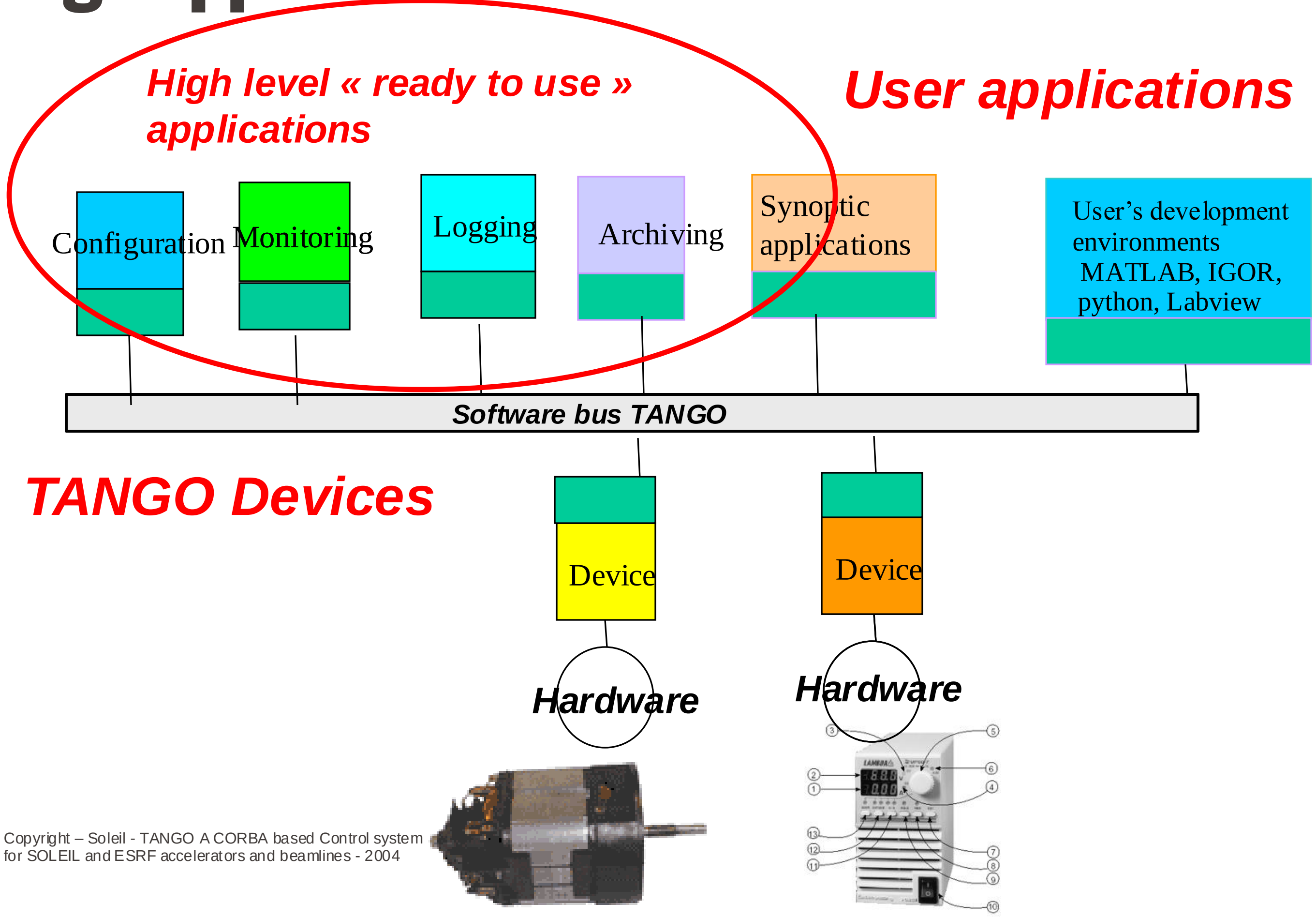
TANGO

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 device class which is hardware/software specific
  - Device supports **commands** (actions) and **attributes** (data) and **states**
  - Tango classes are merged in operating system process called Device Server
  - Device configuration parameters and network address stored in a database

Tango Applications



High level « ready to use » applications

User applications

Configuration

Monitoring

Logging

Archiving

Synoptic applications

User's development environments MATLAB, IGOR, python, Labview

Software bus TANGO

TANGO Devices

Device

Device

Hardware

Hardware

Copyright – Soleil - TANGO A CORBA based Control system for SOLEIL and ESRF accelerators and beamlines - 2004

Tango Device

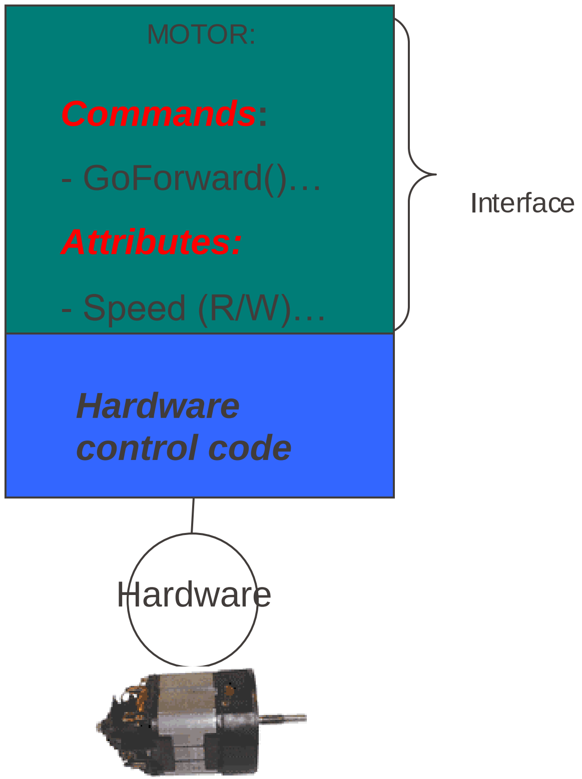
- Everything which needs to be controlled is modeled as a Device

- A Device can be
  - An equipment (e.g. power supply, pump, valve, etc.)
  - A set of equipment (e.g. three valves driven by the same controller)
  - A set of software functions
  - A group of equipment constituting a subsystem

- Modeling the equipment, being HW or SW, is the first fundamental step
  - A device must be self-consistent
  - Must enable the access to the features of the modeled device

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



MOTOR:

***Commands*:**

- GoForward()…

Attributes:

- Speed (R/W)…

Interface

Hardware control code

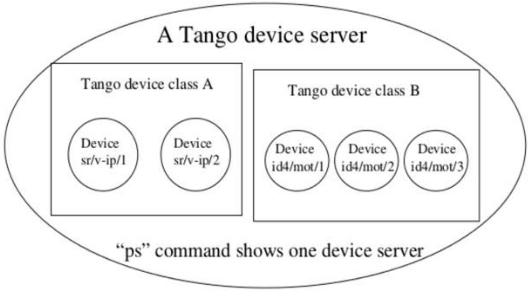
Hardware

Class, Device and Device Server

- Three closely related concepts
- Tango Class
  - A class defining the interface and implementing the device control of the implementation of a software algorithm
- Tango Device
  - Instance of a Tango Class giving access to the services of the class
- Tango Device Server
  - Operating System process in which one of more Tango Classes are executing, providing access to one or more Tango Devices

Device Server

- OS process where the Tango class(es) run
- Device Server configuration is stored in the Tango Database
- Device number and names for a Tango Class are defined within the database, not in the code
- Which Tango Class(es) are part of a Device Server process is defined in the database but also in the code
- Device Server can host several Tango Classes and each class can be instantiated several times

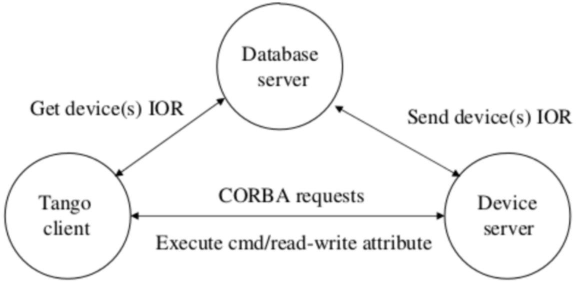


School on Tango Control System, 2016

Device Server Startup Sequence

- Device Server
  1. Contact the Tango Database to know which devices have to be created and managed based on the instance specified
  2. Register the devices
- Tango Client
  - Ask the Tango Database for devices
  - Connect to the Device Server

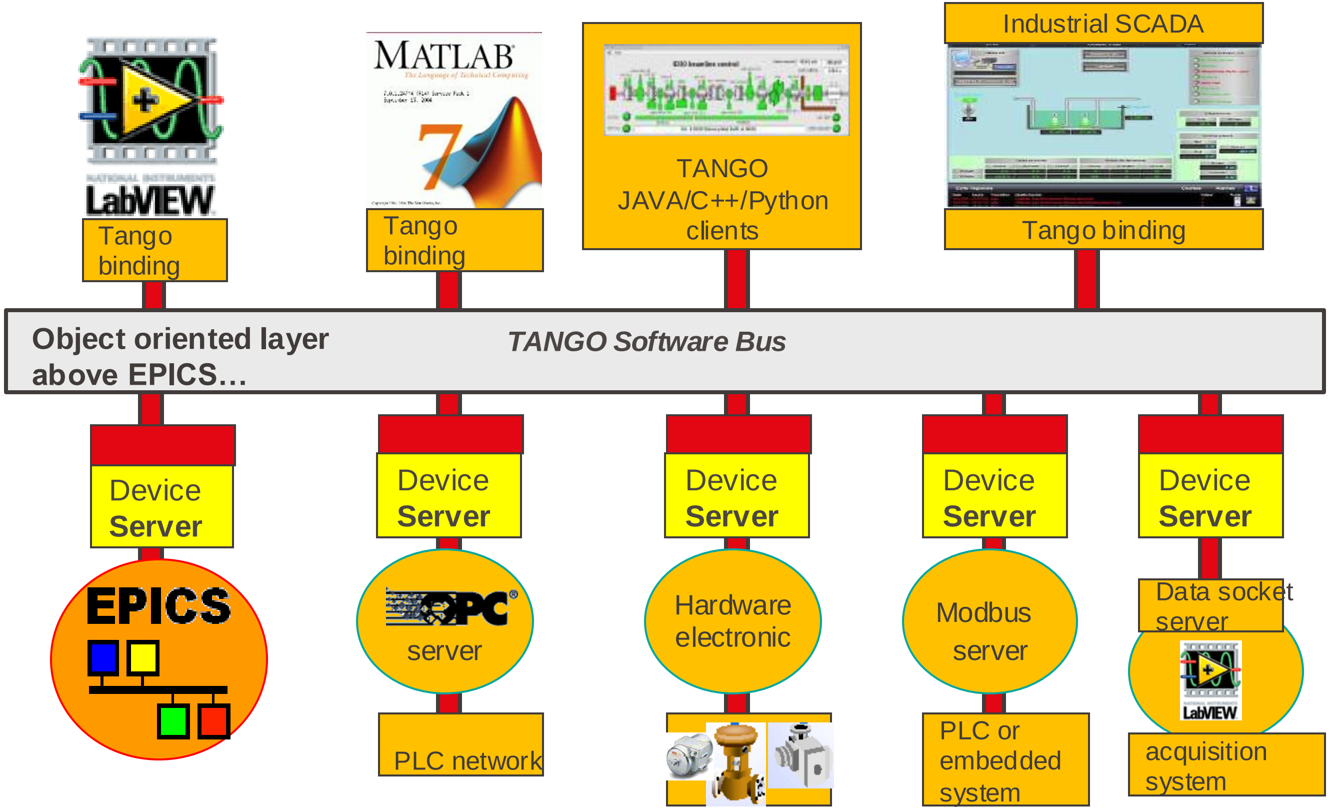
- Tango Database is only involved during the connection phase



Device Naming

- Each device has a unique name within the control system
- Name if the key to access the device
- Name is a characters string (a..z,0..9) composed by three fields separated by /
- The three fields are **domain, family** and **member**
  - domain/family/member
- Strings are case insensitive
  - LH/PSQ/1 and lh/psq/1 are the same

Tango Interoperability



Tango binding

Tango binding

TANGO JAVA/C++/Python clients

Industrial SCADA

Tango binding

Object oriented layer above EPICS…

TANGO Software Bus

Device **Server**

Device **Server**

Device **Server**

Device **Server**

Device **Server**

EPICS

OPC server

Hardware electronic

Modbus server

Data socket server

PLC network

PLC or embedded system

acquisition system

Main Tango Tools

- Taurus Designer
  - Qt Designer application to develop synoptic view
- Pogo
  - Develop device server in C++/Python
- Jive
  - Tango database browser and device testing tool
  - Manage Device Server and Devices
- 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/

Exam Questions Example

- What are the main functionalities of a SCADA?
- Cite some recommendations/good practices for HMI design
- What is the difference between an alarm and an event and how are these two types of information treated by the SCADA (Operator workplace)?
- How an alarm on level is defined?
- What is an Historian for SCADA and what is its purpose?
- What are SAIDI/SAIFI?