FEBRUARY 15, 2017

Risk Management

Anchorage Users Group

Risk Management

Introduction

AJ Smith

Business Development – Advanced Services (OGC)

ABB since 10/1997

3rd time at Anchorage User's Group

Advanced Services – Optimize stable performance, Increase declining performance

- Cyber Security
- Control Loop Performance
- Control System Performance
- Alarm Management
- Batch Optimization
- Boiler Optimization
- etc

Risk Management

Definition

"The first step in the risk management process is to acknowledge the reality of risk. Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning."

Charles Tremper

Risk Management

Definition

Risk = (Threat x Vulnerability) x Consequence

Probability **Impact**

Threats:

- Operator Effectiveness
- Cyber Security
- Poor Process Control
- Device Failures
- Poor Alarm Management
- DCS System Performance

Risk Management

Introduction

"Risk is 'exciting' but management is 'boring'."

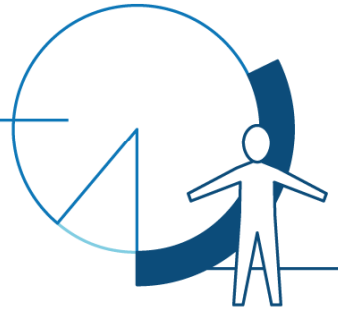
Keith Baxter

Risk Management Tools

System Performance

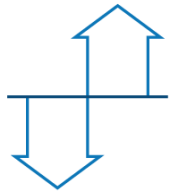
On avarage 5% of global annual productivity is lost, due to unscheduled downtime.

80% of unscheduled shutdowns are preventable...



...of which 40% are caused by humans

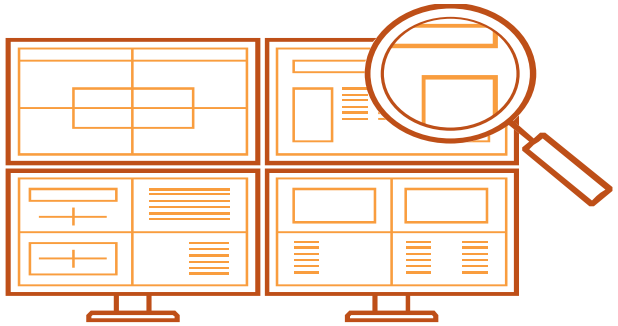
How do we tackle this opportunity to maximize production and quality, and minimize risks of accidents and unscheduled downtime?



Risk Management

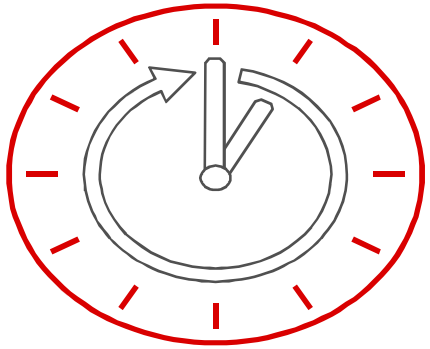
System Performance

Issues may…



Be hidden until they become emergencies

- Running out of disk space
- Failed redundant components that no one notices
- Disk failure where backups are not usable
- Malware infection

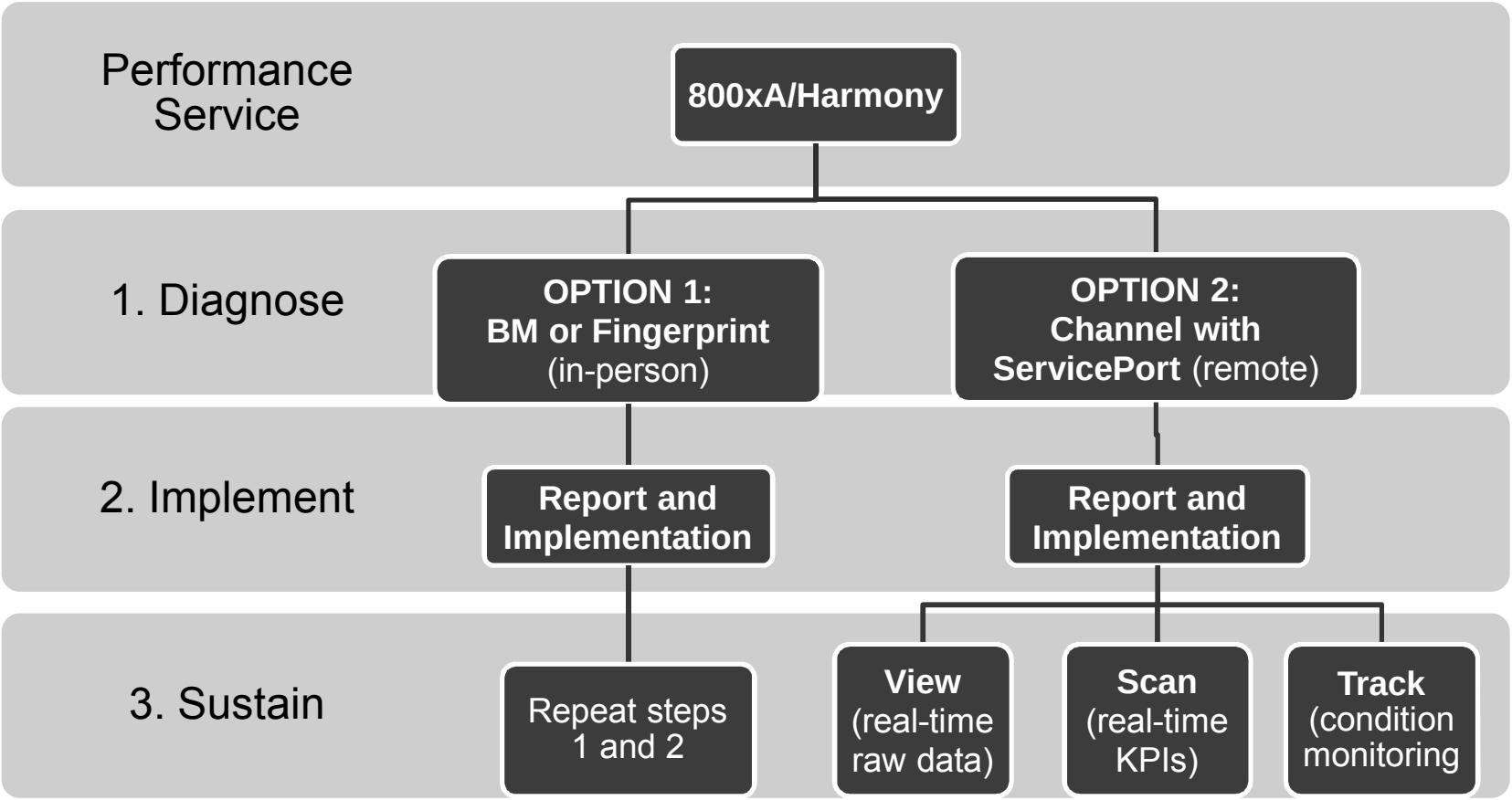


Develop so gradually that poor performance seems normal

- Computer slowdowns due to disk fragmentation
- Deterioration in communications due to degraded connections
- Power glitches causing intermittent behavior

Risk Management Tools

System Performance

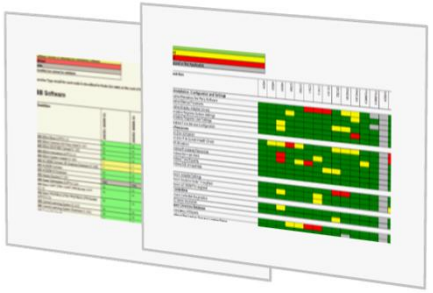


Risk Management Tools

System Performance

Benchmark Report

Status Overview



- Control system KPI status verification
- An easy to read ‘Traffic Light ‘ control system report
- Effective tool for identifying performance issues
- Analyzes most relevant system parameters and KPI’s
- Shows the system status and highlight deviations and potential risks

Risk Management Tools

800xA System Performance

Benchmark Report

Status Overview

Automatic data collection

Automatic data analysis

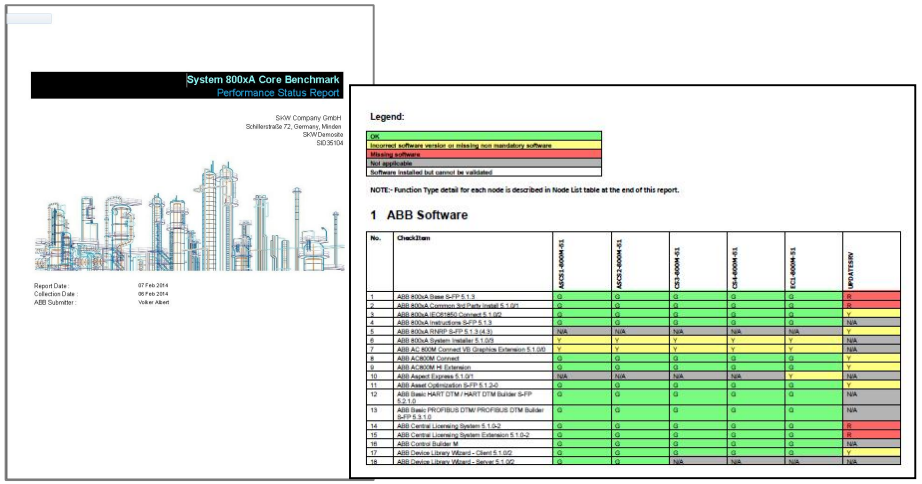
Automatic report generation

Easy-to-use tool

- Summarizing results in table format with short KPI definition
- Traffic light assessment
  - good
  - ambiguous
  - incorrect

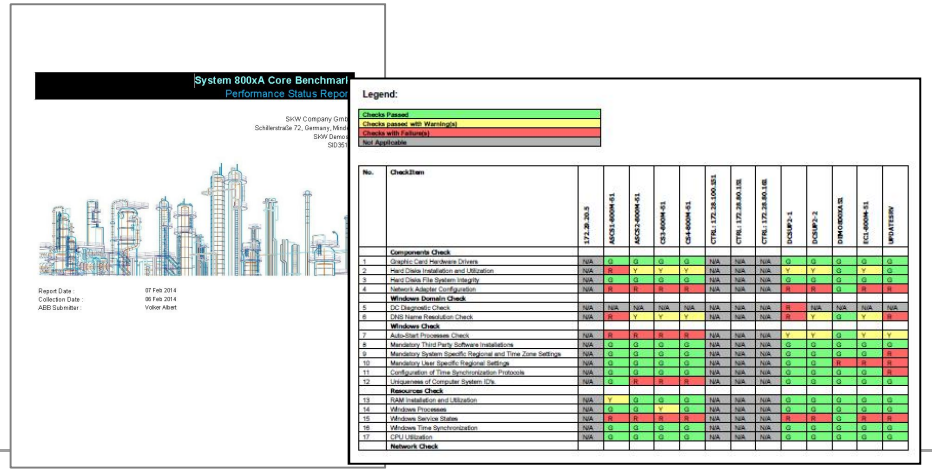
Risk Management Tools

800xA System Performance



Software Status Report

- Validates the software installation against the requirements of ABB releases

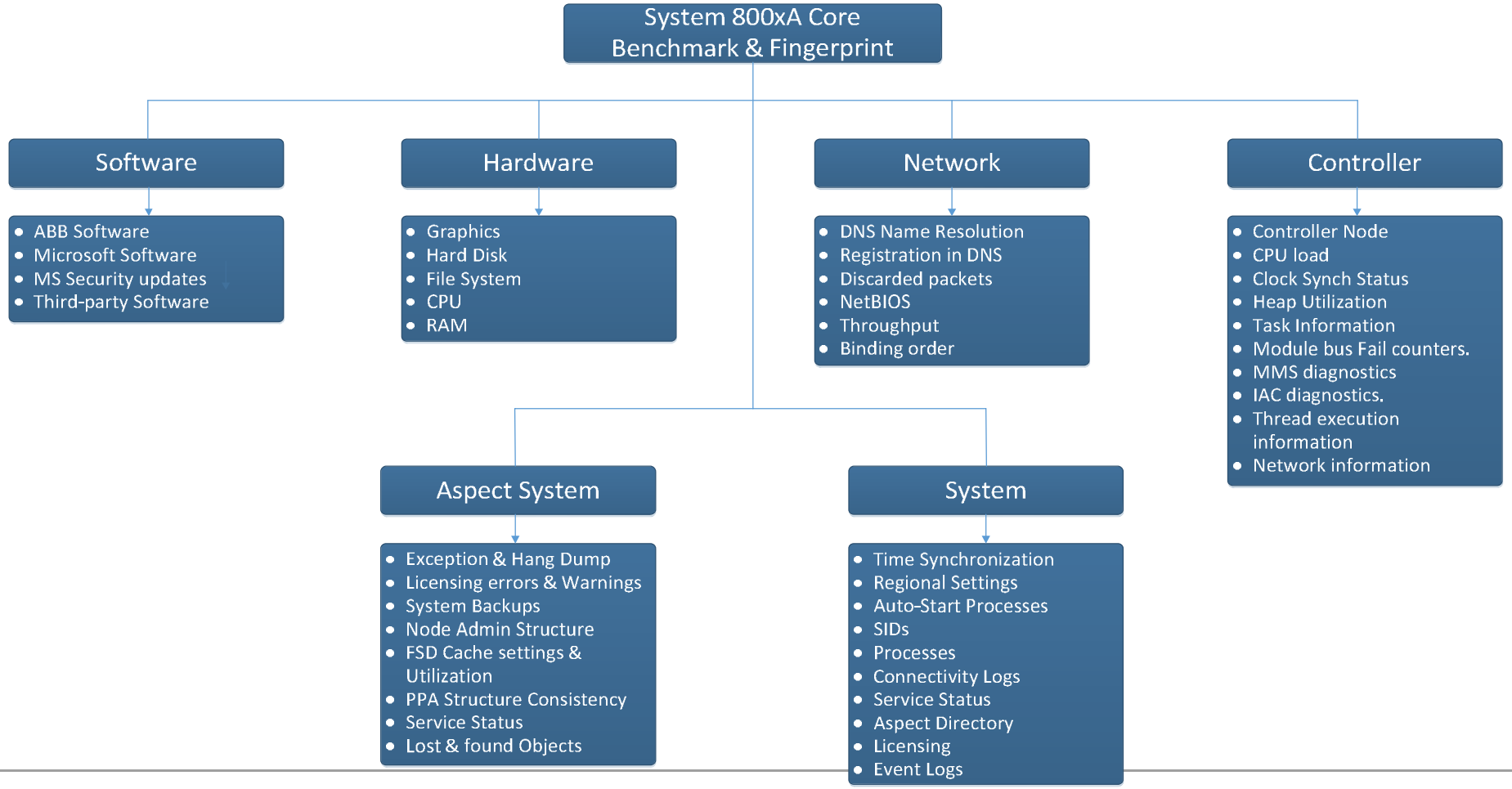


Performance Status Report

- Validates hardware and software components and runtime parameters against system requirements and best practices

Risk Management Tools

800xA System Performance



Risk Management Tools

Harmony System Performance

- Shows the system status and highlights deviations and potential risks
- Traffic light assessment
  - good
  - ambiguous
  - incorrect

No.	Node ID	Node LIS/NIS Firmware Status	Loop Channel 2 Receive Error Rate %	Node Output XR Saturation %	Node Memory Utilization %	Node I/O Bus Saturation %	Received XRs per Packet Since Reset	LIS Poll Busy NAK Count
45	DefaultDCS.Loop_11.Node_98	N/A	N/A	N/A	N/A	N/A	N/A	N/A
46	DefaultDCS.Loop_11.Node_99	R	G	G	G	G	G	G
47	DefaultDCS.Loop_12.Node_1	G	G	G	G	G	G	G
48	DefaultDCS.Loop_12.Node_10	Y	G	G	G	G	G	G
49	DefaultDCS.Loop_12.Node_11	Y	G	G	G	G	G	G
50	DefaultDCS.Loop_12.Node_12	Y	G	G	G	G	G	G
51	DefaultDCS.Loop_12.Node_13	G	G	G	G	G	G	G
52	DefaultDCS.Loop_12.Node_14	G	G	G	G	G	G	G
53	DefaultDCS.Loop_12.Node_15	G	G	G	G	G	G	G
54	DefaultDCS.Loop_12.Node_16	G	G	G	G	G	G	G
55	DefaultDCS.Loop_12.Node_17	G	G	G	G	G	G	G
56	DefaultDCS.Loop_12.Node_18	G	G	G	G	G	G	G
57	DefaultDCS.Loop_12.Node_19	G	G	G	G	R	G	G
58	DefaultDCS.Loop_12.Node_2	Y	G	G	G	G	G	G
59	DefaultDCS.Loop_12.Node_20	G	G	G	G	G	G	G
60	DefaultDCS.Loop_12.Node_21	Y	G	G	G	G	G	G
61	DefaultDCS.Loop_12.Node_22	Y	G	G	G	G	G	G
62	DefaultDCS.Loop_12.Node_24	Y	G	G	G	G	G	G
63	DefaultDCS.Loop_12.Node_25	Y	G	G	G	G	G	G
64	DefaultDCS.Loop_12.Node_3	G	G	G	G	G	G	G
65	DefaultDCS.Loop_12.Node_38	G	G	G	G	G	G	G
66	DefaultDCS.Loop_12.Node_4	G	G	G	G	G	G	G
67	DefaultDCS.Loop_12.Node_40	Y	G	N/A	G	N/A	G	G
68	DefaultDCS.Loop_12.Node_42	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Example Benchmark Report

3 Summary of findings

3.1 Benchmark Gap Analysis

The system health is measured with technical finding´s checklist. The summary of those finding is shown below.

Alarm Benchmark Summary per Evaluation Module

Name	Good	Warnings	Problems	Priority
Loop Channel 1 Receive Error Rate %	114	0	0	1
Loop Channel 2 Receive Error Rate %	113	0	1	1
Excessive Incoming GMI traffic (avg/sec)	113	0	1	2
LIS Poll Busy NAK Count	113	0	0	2
Average Node CPU Utilization %	113	1	0	3
Node I/O Bus Saturation %	100	6	1	3
Node Input XR Saturation %	100	7	0	3
Node Memory Utilization %	104	8	3	3
Node Output XR Saturation %	107	0	0	3
Received XRs per Packet Since Reset	107	0	7	3
Node LIS/NIS Firmware Status	49	52	14	4
Total	**1133**	**74**	**27**	

Table 5.Node Performance Issues

Name	Good	Warnings	Problems	Priority
Average System Free Time %	124	24	102	2
Maximum Segment Cycle Time Deviation %	214	8	23	2
Average Segment CPU Utilization %	189	35	21	2
Module Firmware Status	189	199	72	3
Controller RAM Utilization %	123	6	10	3
Controller NVRAM Utilization %	139	0	0	3
Segment Checkpoint Overrun Count	186	59	0	3
Total	**1164**	**331**	**228**	

Table 6.Module Performance Issues

Name	Good	Warnings	Problems	Priority
Node Environment Status	168	0	0	1
Control way Bus Failure	407	0	0	1
NVRAM Failure	250	0	0	1
Central Loop Received Errors on Channel 2	12	0	0	2
Serial Link 2 Bad	6	0	0	2
Digital Station Status Bad	250	0	0	3
Central and Satellite Ring I/O Out of Specification	8	0	10	4
Communication Status Problem	135	0	27	4
I/O Out of Specification	149	0	106	4
Total	**1385**	**0**	**143**	

Table 7.Module Status Issues

ABB 23

Risk Management Tools

Harmony System Performance

Minimum Requirement to install Data Collector	
CPU	Dual Intel Pentium III, or single core Pentium 4 or higher
Memory	256 MB free RAM
Hard disk	50 MB of free space (after all prerequisites are installed)
Communicatio n Ports	As required by CIU specification
Harmony Rack equipment	Dedicated CIU (ICI03, ICI12, ICI13 or IET800) using SCSI, RS232 or TCP-IP

Data Collector (HD200) **supported platforms (*)**
Windows 7 (32 and 64bit)
Windows Server 2008 (32 and 64bit)
Windows 8.1 (64bit)
Windows Server 2012 (64bit)

(*) Data Collector HD200 communicates with the Harmony hardware through HAPI 4.0, on 32 bit as well as 64 bit machines.
HAPI 4.0 does not support Windows-XP.

Risk Management Tools

Harmony System Performance

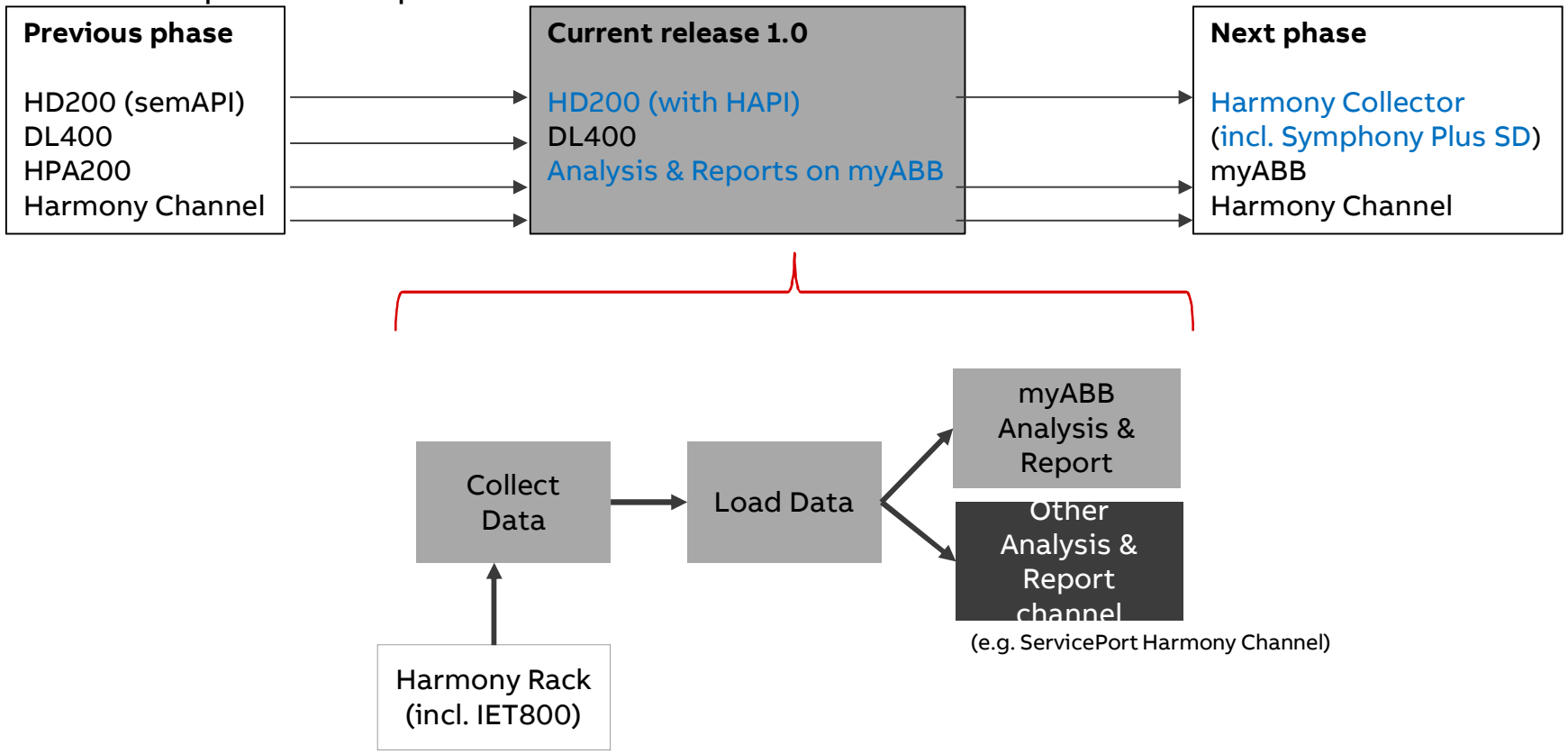
Supported modules (Harmony Rack)

INPIM01	NLSM01	IMMFP01/IMMFP11
CTM01	INPCT01	IMMFP02/IMMFP12
INAMM01	INPCI02	IMMFP03
IMAOM01	NGCM01	IMMFP04
NCOM	CTT	BRC100
IMCOM	CBC01	BRC200
IMQRC	CSC01	BRC300
CLC	INIPT01	BRC400
IMLMM01	INIPT02	HAC
INNPM12/Plant loop	HNCC	INNPM01/11/12
BIM	INICT01	INNPM22
INAMM02	MCP02	HNPM
INPTM01	INICT03	HAC NPM
INPCI01	INIET800	PBUG01
NMFC	INICT12	NLCM02
IMMFC	INICT13	NLCM03
INLMM02	NSBM01	IMCPM02/03
IMMPC01	SCM01	INSEM01
INBTM01	INIIT01/02/03	CIC01
NLCM01		SLC01/21

Risk Management Tools

Harmony System Performance

Current scope and next phase



Blue color: new developments.

Risk Management

Definition

"If you do not actively attack the risks, they will actively attack you."

Tom Gib

Risk Management

Definition

Safety Culture:

“Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you.” Theodore Roosevelt

"You want a valve that doesn't leak and you try everything possible to develop one. But the real world provides you with a leaky valve. You have to determine how much leakiness you can tolerate." Arthur Rudolph

"By definition, risk-takers often fail. So do morons. In practice it's difficult to sort them out." Scott Adams

"To make a mistake is only human; to persist in a mistake is idiotic." Roman Cicero

“Luck is unreliable.” Amanda Ripley

Risk Management Tools

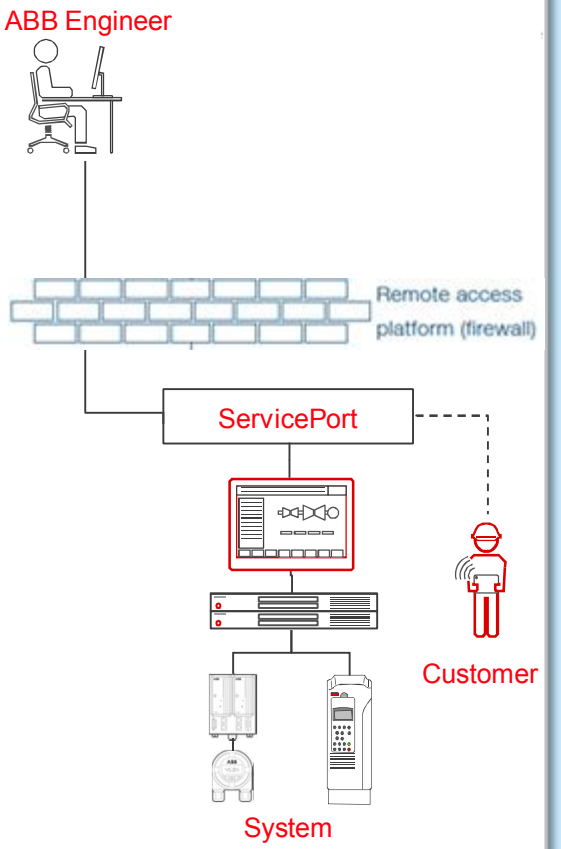
System Performance - Service Port

Features

- Automatic, non-invasive data gathering and analysis
- Remote access allows ABB to monitor system
- Ability to connect to multiple systems from one ServicePort
- Can be installed on stand-alone server or virtual environment
- ServicePort Explorer Client allows multiple users to access single ServicePort within network
- Configurable Track rules can send email notifications when KPIs exceed thresholds

Benefits

- Identifies trends to mitigate equipment and process issues
- Decreases cost of identifying issues
- Minimizes risk of system upsets
- Remote access reduces response times and travel expenses



Risk Management Tools

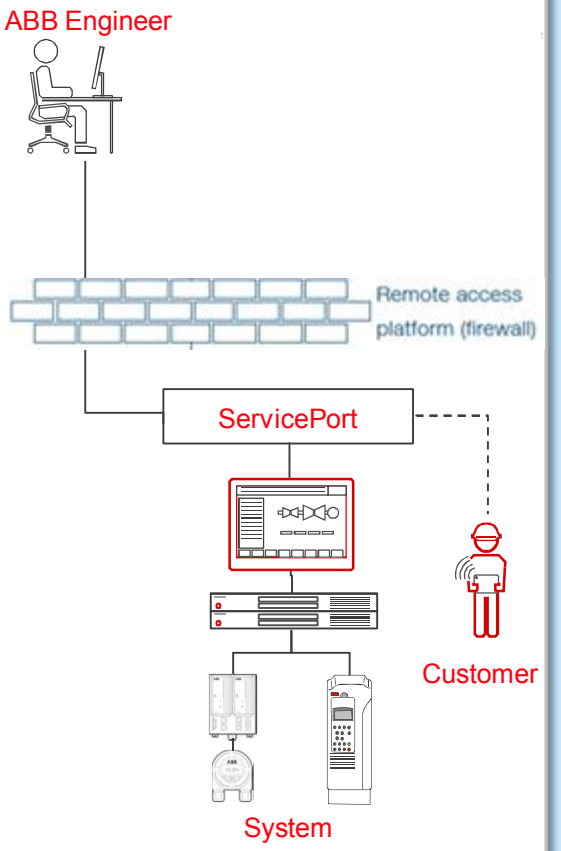
System Performance - Service Port

Deliverables

- 2 reports in year 1, 1 report in years 2 and 3
- Periodic maintenance/technical checks
- Remote support
- Server maintenance
- Remote training following commissioning and on demand

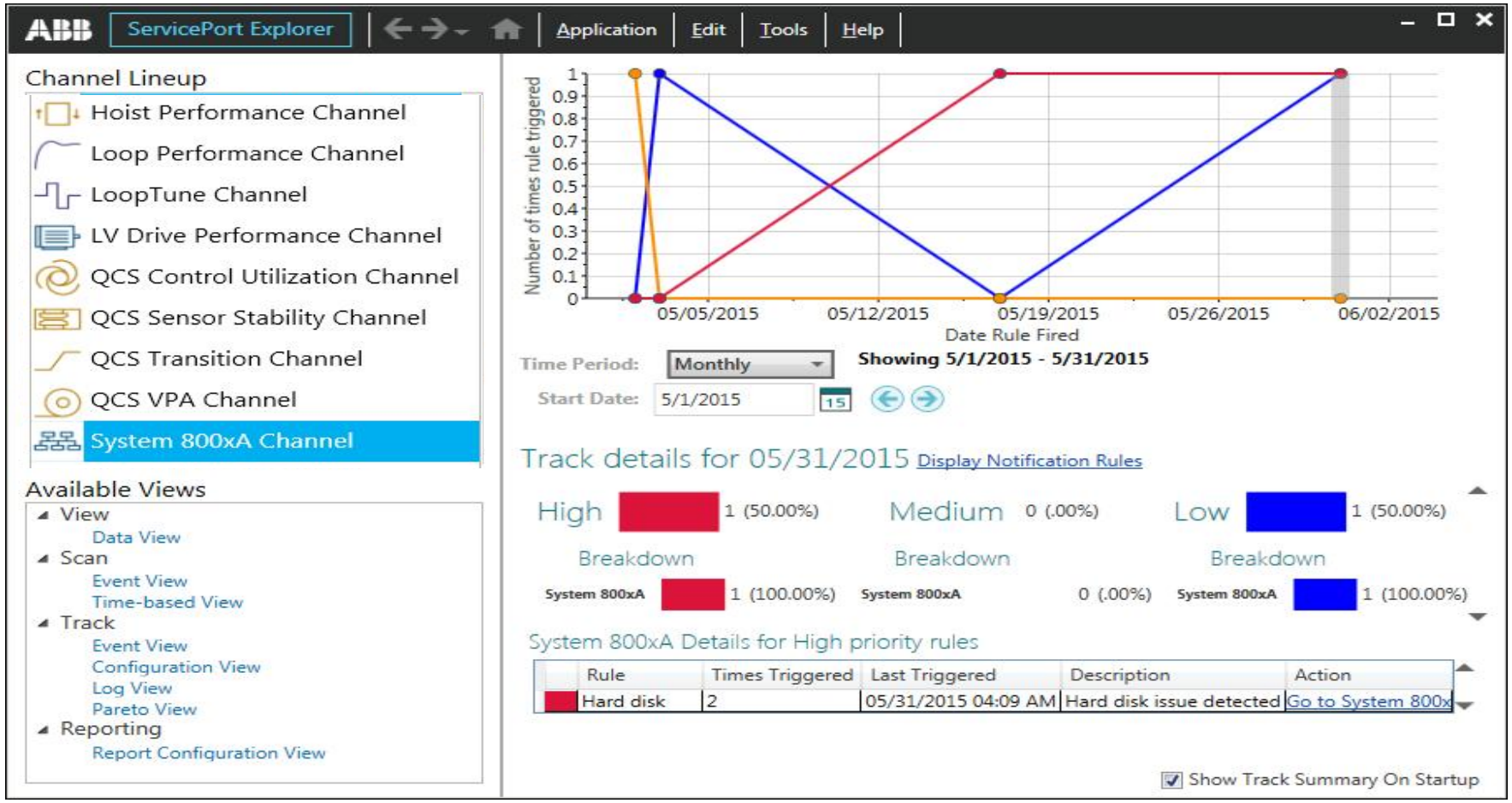
ABB Residents

- ABB residents are trained following commissioning
- ServicePRO tasks tied to ServicePort



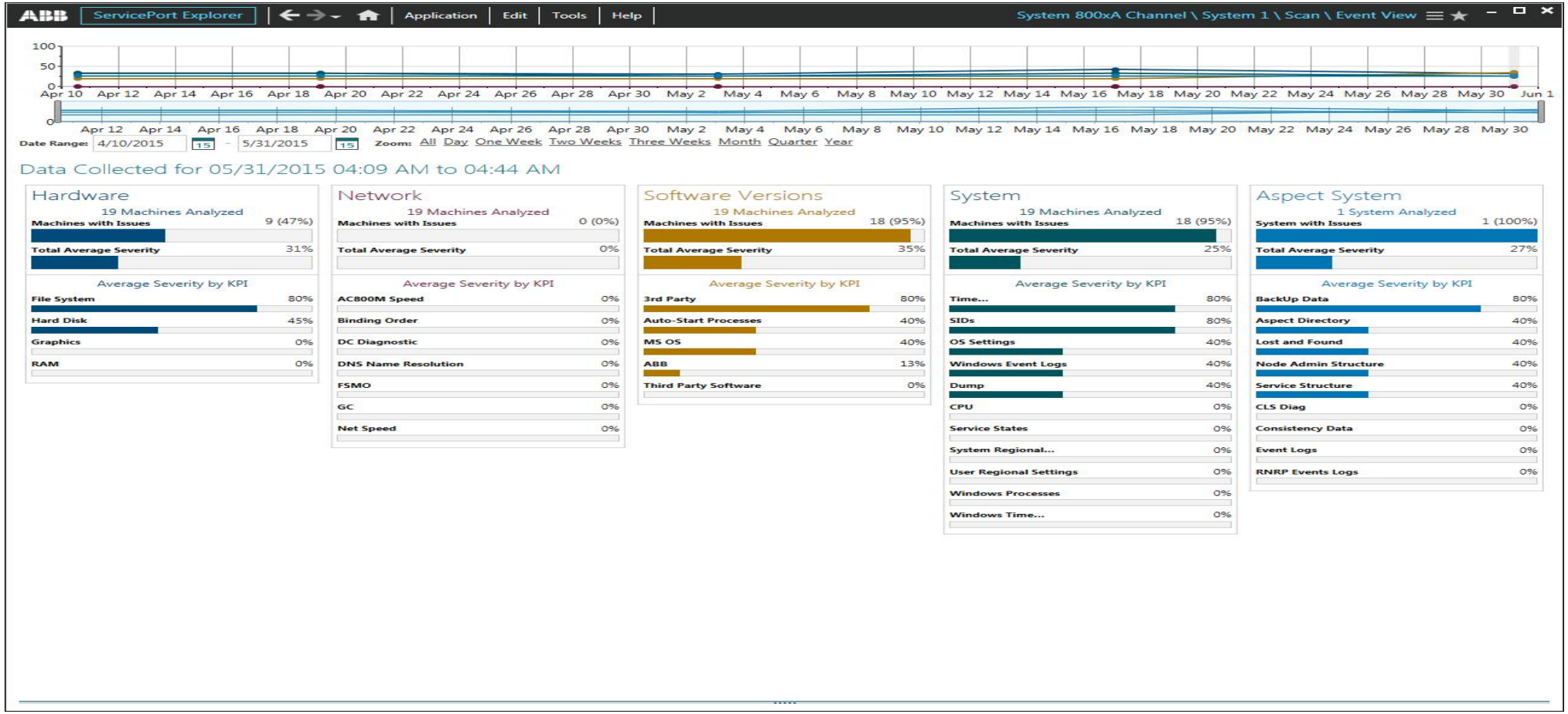
Risk Management Tools

System Performance - Service Port



Risk Management Tools

System Performance - Service Port



Risk Management Tools

System Performance - Service Port

ABB | ServicePort Explorer | Application | Edit | Tools | Help | System 800xA Channel \ System B \ View \ Data View

Time Intervals
- 5/10/2015 3:14:10 AM
- 5/3/2015 3:14:05 AM
- 4/26/2015 3:05:05 AM
- 4/19/2015 3:05:00 AM
- 4/12/2015 3:04:46 AM

Devices
- System
  - D1
- Machines
  - D1-400CS24-033
  - D1-400CS24-034
  - D1-800CS24
  - D1-800CS24
  - D1-AO24-05
  - D1-AS24-01
  - D1-AS24-01
  - D1-AS24-01
  - D1-DC24-00
  - D1-DC24-00
  - D1-ES24-13
  - D1-ES24-13
  - D1-RS24-05
  - D1-WP24-07
  - D1-WP24-07
  - D1-WP24-07
- Controller
  - 172.16.88.15

Hardware | Network | Software Versions | System | Aspect System | AC800M

Memory

AvailablePhysic	VirtualMemory	VirtualMemoryl	TotalPhysicalM	PageFileSizeMB	VirtualMemoryl	PageFilePeakUs	PageFileName	PageFileCurren
1545	4732	6363	3071	3370	1631	88	C:\pagefile.sys	50

Checkdisk

Disks

Machine Name: AH-AS4-011

Date: 5/31/2015 4:09:19 AM

Copy to Clipboard

Finding #1

The disk usage is above 60%. Caution: this is a disk partition which is used as 800xA Temp Data disk.

Explanation

Disk usage is approaching the value of 75%, which shall not be exceeded.

Impact

The disk defragmentation may become slow or even impossible if the free disk space is too low, resulting in performance loss. If the disk usage comes near to 100%, the 800xA applications on this node may crash.

Severity

4

Recommendation

Delete unnecessary files on the disk, if possible. If this is not possible, replace the disk or disk partition by a larger one.

Reference

3BSE034678-510, Rev C, page 42.

Finding #2

Disk Defragmentation is recommended

Diagnosis

ChkdskComments
Windows found problems with the file system.Run CHKDSK with the /F (fix) option to correct these.

oofFolders	DefragRecomm	UsedMB
3310	No	22285

BitsPixel	Description	PCBrand
34 32	VMware SVGA II	VMware, Inc.
38		

Risk Management

Alarm Management

“ “If you treat risk management as a part-time job, you might soon find yourself looking for one.”

Deloitte

Risk Management

Alarm Management

Too many alarms implemented without formal review

+

No understanding of the subsequent operator burden

=

Operators are overloaded beyond their design limit

Pre-digitization (1960) = 100 alarms per operator

Digitized (2000+) = 4,000 alarms per operator

Risk Management

Alarm Management

"... the more reliable and greater the scope of automation, the greater the demand on the operator when it fails."

- Users are being pacified.
- Important clues are overlooked or misinterpreted.

Modern digital control systems hide most of the process from the operator and alarms are required to direct the operator's attention as well as annunciate problems.

Risk Management

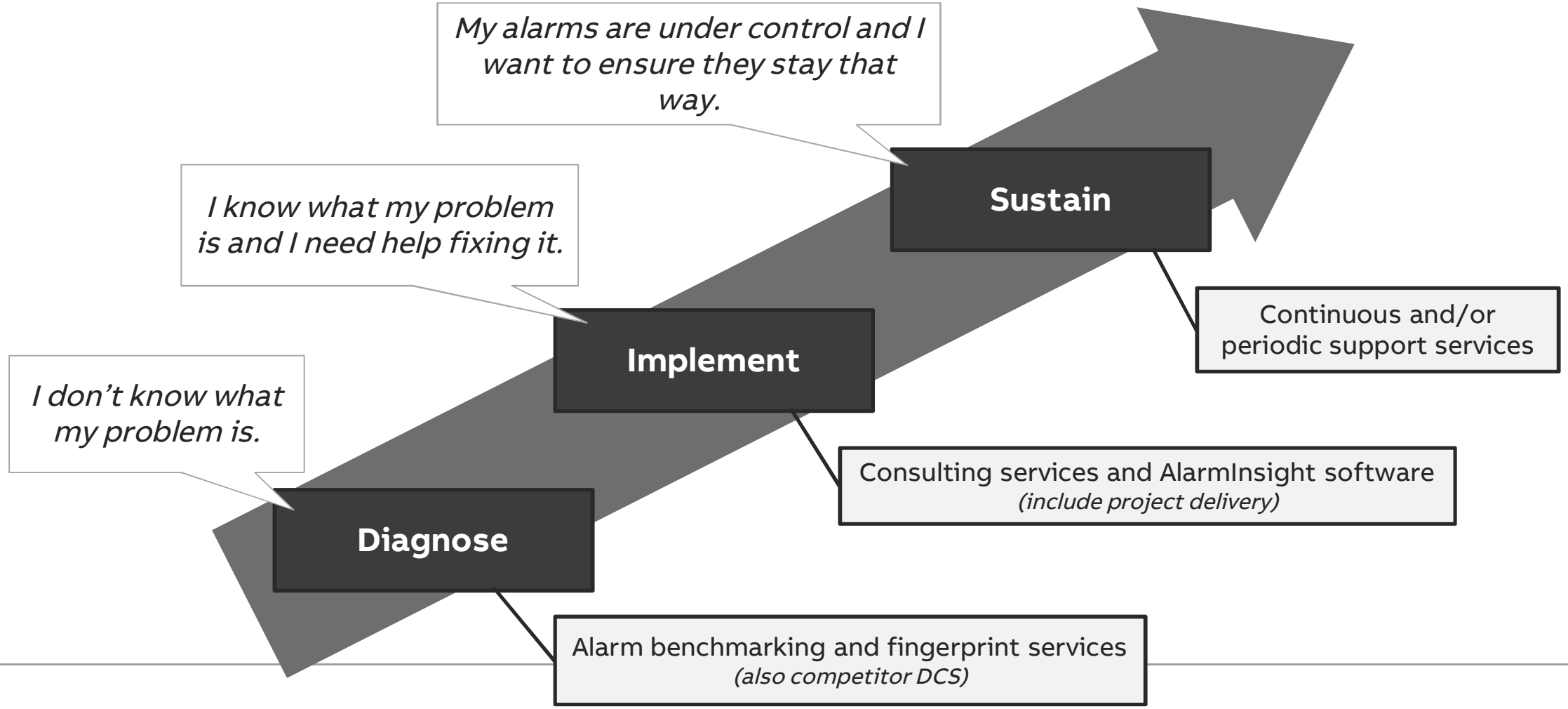
Alarm Management

Impact

- Long lists of alarms make it difficult to identify important alarms
- Nuisance alarms move in and out of alarm states, reduce operator confidence, and can be overlooked
- Control room environment, layout, sound, and HMI can affect alarm management
- Government regulators and Insurers are now trained in identifying good alarm management.
- **Studies show a re-design of alarm management can produce up to 5-8% of process throughput in potential benefit, which can be up to $8M for a typical plant**
  - **By making operators more aware of critical alarms**
  - **Quicker response**

Risk Management Tools

Alarm Management



Risk Management Tools

Alarm Management

Alarm Benchmark and Fingerprint reports analyze gathered alarm data against ISA 18.2 and EEMUA 191 standards and report on the gaps.

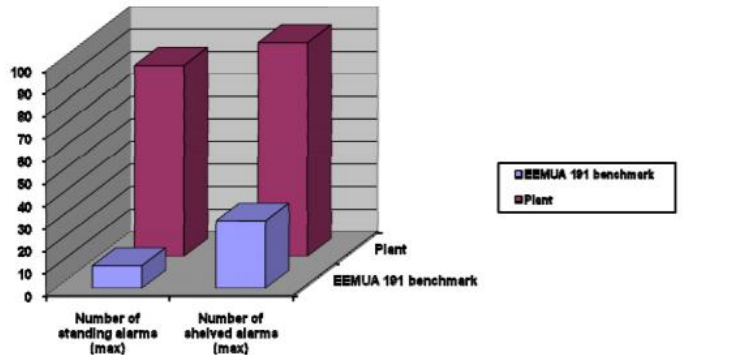


Figure 4 - Standing and Shelved Alarms

3.3 Distribution of Alarms

Check List

This section addresses the classification of alarms into different priority classes. Alarm priority analysis looks at the number of alarms occurring within each class and the number of configured (designed) alarms within each class.

For alarm priorities, the EEMUA 191 recommends a small number of priority levels, typically defined as: high, medium, and low. The EEMUA suggests a decreasing number of alarms as the priorities increase. A critical class can also be included, but should contain relatively few alarms. EEMUA guidelines suggest that

Analysis:

- Average & Peak Alarm Rates
- Standing & Shelved Alarms
- Distribution of Alarms
- Nuisance Alarms
- Operator Response Time

Risk Management

Definition

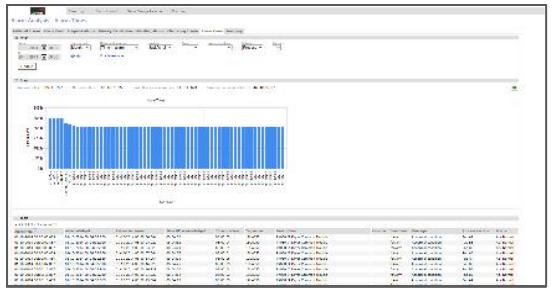
"To make a mistake is only human;
to persist in a mistake is idiotic."

Cicero

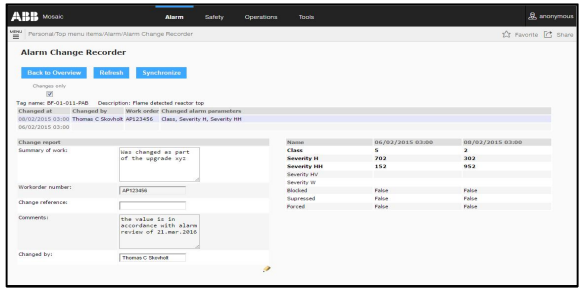
Risk Management Tools

Alarm Management - AlarmInsight

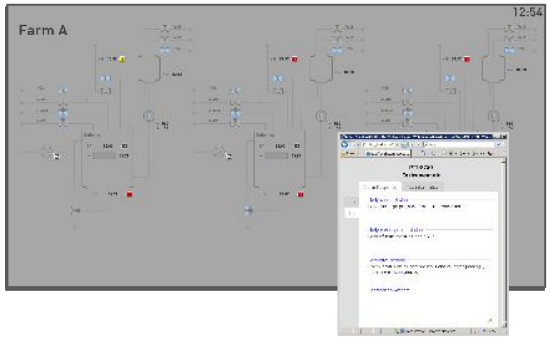
Event Log & Alarm Analysis & KPI



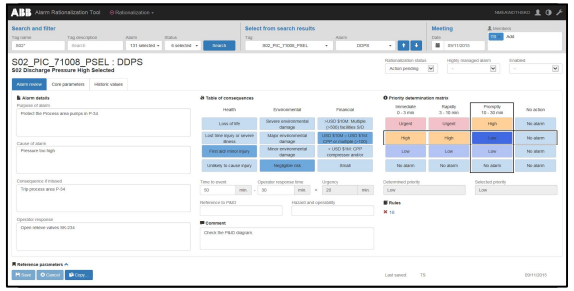
Alarm Change Recorder



Alarm Helper



Alarm Rationalization Tool



AlarmInsight® SW Portfolio

Events Alarms

Operator response / attributes

Enable efficient operator response to production disturbances

Risk Management Tools

Alarm Management – AlarmInsight

Alarm monitoring and analysis

Basic and enterprise data logging

- **KPI-Report/.pdf (KPI)**
  - Automatically generated KPI reports: daily, weekly, monthly
- **AlarmAnalysis (AA)**
  - Manually set filters, analyze and generate reports
- **EventLog Viewer (EL)**
  - Manually set filters, find root cause and sequence of events
- **Expert Tool (ET)**
  - Service tool for ad-hoc ,deep-dive analysis supporting improvement work: used in all phases (client)

Alarm management

Lifecycle management

- **Alarm Rationalization Tool**
  - Alarm Rationalization and Continuous Alarm reviews, Management of change/ Master Alarm Database (SQL)
  - Input for Alarm Helper and DCS bulk updates
  - *Both a services tool and on-site server implementation*
- **Alarm Change Recorder (ACR)**
  - Monitor changes to alarm attributes/ values in the distributed control system
  - Track changes during operation and modifications

Real-time information

Per site / for control room operator

- **AlarmHelper (AH)**
  - Operator support: How to react to an alarm and collect feedback from operators
  - *Context-sensitive presentation of input from Rationalization, design and modification work*

Basic: *Logging and alarm KPI reporting , log collection from multiple sources*

Enterprise features: *Multi-site alarm consolidation, office network reports, large datasets*

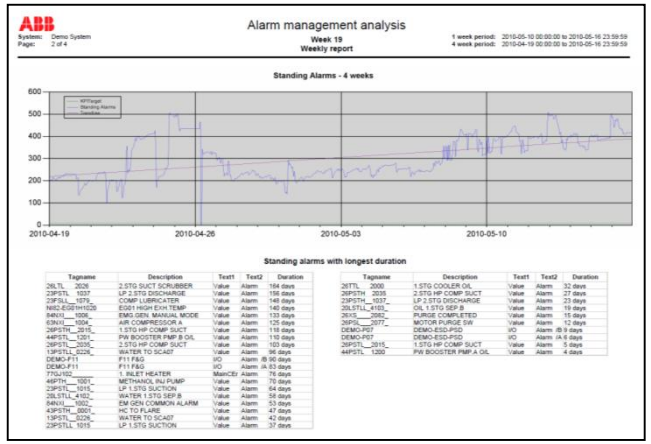
Risk Management Tools

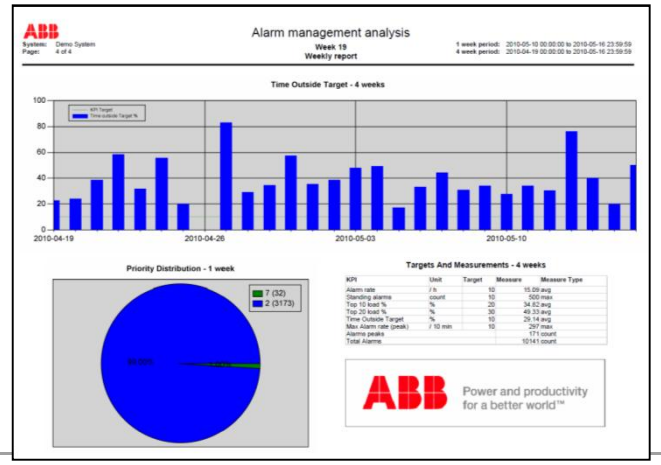
Alarm Management - AlarmInsight

Alarm and Event historian – providing long term storage of data for analysis

Alarm Performance KPI reports according to EEMUA 191 and ISA 18.2, available on web or distributed via email

Ease-of-use and ease-of-distribution make these reports an efficient tool for communicating alarm system health in the organization





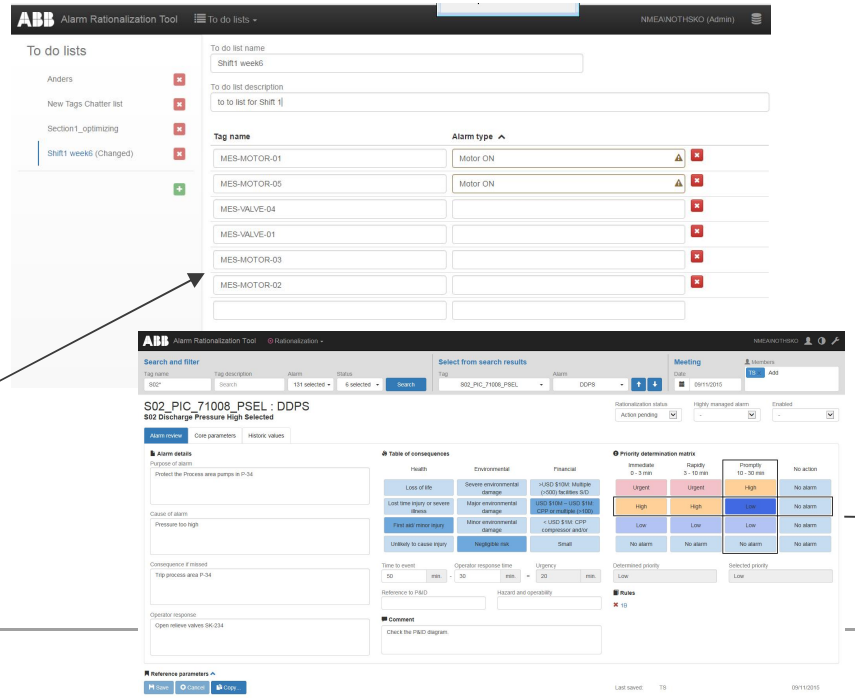
Risk Management Tools

Alarm Management - AlarmInsight

1.Monitor Alarm rates, pick top 10 alarms

Alarm KPI reports & Alarm Analysis

2. Enter top 10 alarms in “to do” lists into ART and have the last shift review the alarms.



ART

3. Update Alarm Helper texts & DCS with optimized attributed/ priorities

ART Excel file

ABB Alarm Rationalization Tool | Rationalization | NMEA\NODAROM

Search and filter

Tag name: Search | Tag description: Search | Alarm: 3 selected | Status: 5 selected | Search

Select from search results

Tag: Tag 3 | Alarm: L

Meeting

Date: 04/11/2015

Members: KH | Add

F02_LALL_51004 : LL

Inlet Header Boot No.1 LL Edit

Rationalization status: New | Highly managed alarm: - | Enabled: -

Rule: Assign a rule

Alarm review | Core parameters | Historic values

Alarm details

Purpose of alarm

Cause of alarm

Consequence if missed

Operator response

Table of consequences

Health	Environmental	Financial
Loss of life	>50bbls release	>$5MM
DAFWC	<50bbls release	$500K to $5MM
First aid case	1 tonne spillage	<$500K
Unlikely to cause injury	Negligible	none

Time to event: min. - Operator response time: min. = Urgency: min.

Reference to P&ID

Hazard and operability

Reference parameters

Priority determination matrix

Immediate 0 - 3 min	Prompt 3 - 10 min	Soon 10 - 30 min	No action
Emergency	Emergency	High	No alarm
High	High	Low	No alarm
Low	Low	Low	No alarm
No alarm	No alarm	No alarm	No alarm

Determined priority

Selected priority

Comment

Run the Video !_ Operator Response & Determining alarm priority

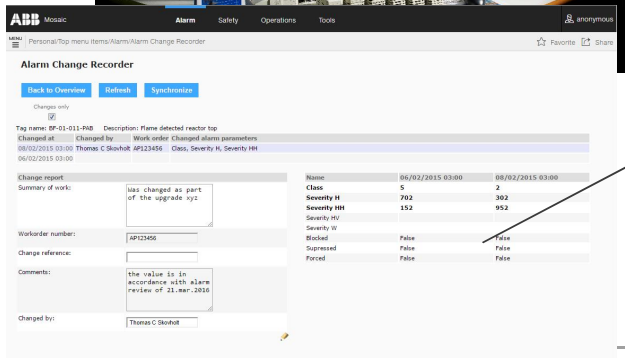
Save | Cancel | Copy...

Last saved:

Risk Management Tools

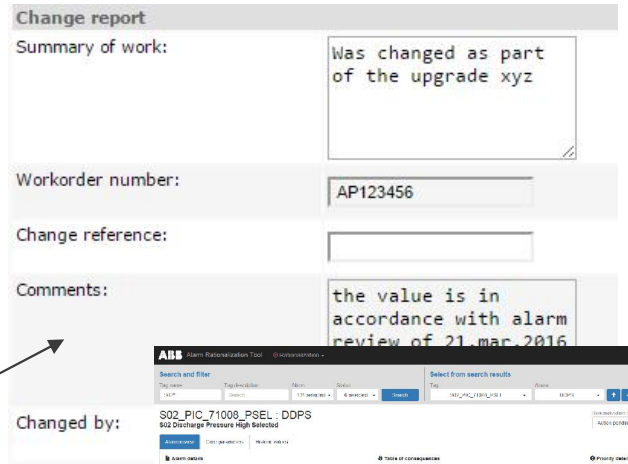
Alarm Management - AlarmInsight

1.Monitor Alarm Attribute changes in the DCS (using ACR)

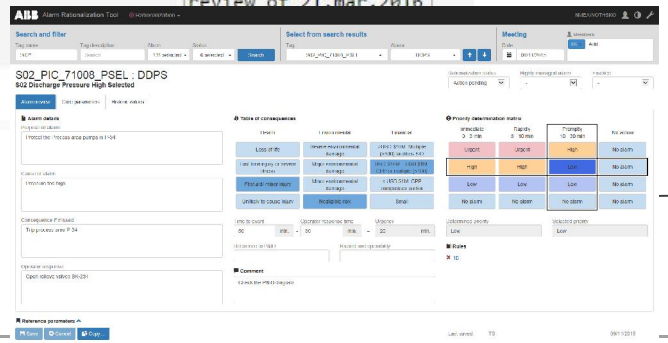


Alarm Change Recorder (ACR)

2. Approve changes in ACR and compare with design values in ART



ACR



ART

3. Look for alarms not present in ART, or with missing Alarm Helper texts. Add to “To-do” list in ART.

ART Excel file

ABB Alarm Rationalization Tool | Rationalization | NMEA\NODAROM

Search and filter

Tag name: Search | Tag description: Search | Alarm: 3 selected | Status: 5 selected | Search

Select from search results

Tag: F02_LALL_51004 | Alarm: LL

Meeting

Date: 04/11/2015

Members: KH | Add

F02_LALL_51004 : LL

Inlet Header Boot No.1 LL Edit

Rationalization status: New | Highly managed alarm: - | Enabled: -

Rule: Assign a rule

Alarm review | Core parameters | Historic values

Alarm details

Purpose of alarm

To notify the operator that the inlet header boot No1 level is LL

Cause of alarm

Boot drain has failed to hold the boot level within the control set-points.
Drain valve has failed to close in time.
Drain valve is passing.

Consequence if missed

Gas blow-by to produced water header on to the pond to atmosphere

Operator response

Notify plant operator to investigate, possibly manually shutting boot drain valve.

Table of consequences

Health	Environmental	Financial
Loss of life	>50bbls release	>$5MM
DAFWC	<50bbls release	$500K to $5MM
First aid case	1 tonne spillage	<$500K
Unlikely to cause injury	Negligible	none

Time to event: 60 min. - Operator response time: 45 min. = Urgency: 15 min.

Reference to P&ID

Hazard and operability

Reference parameters

Priority determination matrix

Immediate 0 - 3 min	Prompt 3 - 10 min	Soon 10 - 30 min	No action
Emergency	Emergency	High	No alarm
High	High	Low	No alarm
Low	Low	Low	No alarm
No alarm	No alarm	No alarm	No alarm

Determined priority: Low

Selected priority: High

Comment

Save | Cancel | Copy...

Last saved: KH 04/11/2015

Run the Video! _ Time saving features

Risk Management Tools

Alarm Management

Gas processing, Egypt

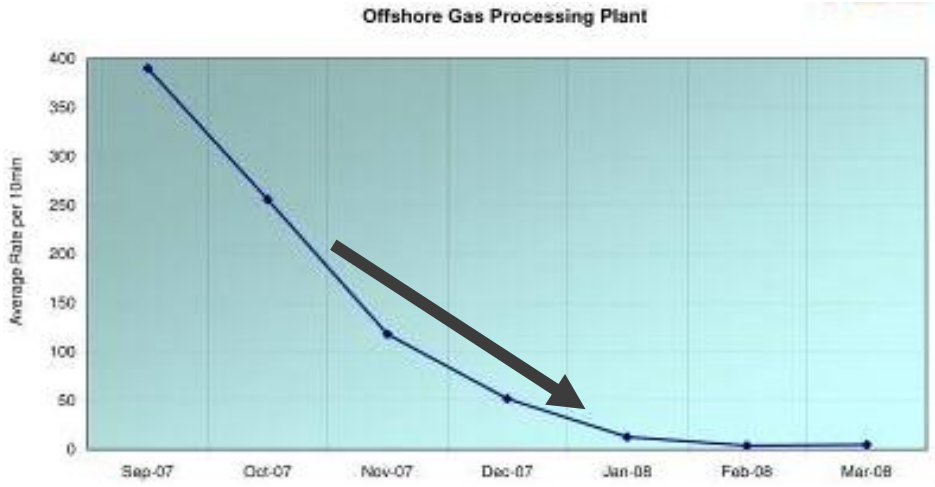


Figure 1. Alarm rate reduction over time

Problem

- Too many alarms / safety issue
- Numerous plant shutdowns led to lost production

Solution

- ABB lead alarm diagnosis, alarm rationalization and implementation of new design

Benefits

- Alarm rates reduced
  - 400 → 8 alarms/10 min
- Improved plant uptime
  - From 25 → 6 shutdowns/yr
- Higher production per year
  - Estimated USD 2M/yr

Risk Management

Risk Culture vs Safety Culture

"An 'At-Risk' system is an unsafe system"

AJ Smith

ABB