EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Distributed Control System Life Cycle Management

Guidelines for Planning and Managing the Life Cycle of Distributed Control Systems

2013 TECHNICAL REPORT

Distributed Control System Life Cycle Management

Guidelines for Planning and Managing the Life Cycle of Distributed Control Systems

3002001123

Final Report, December 2013

EPRI Project Manager
M. Little

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATION, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

OptiControls Inc.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2013 Electric Power Research Institute, Inc. All rights reserved.

ACKNOWLEDGMENTS

The following organization, under contract to the Electric Power Research Institute (EPRI), prepared this report:

OptiControls Inc.
League City, Texas 77573

Principal Investigator
J. Smuts

This report describes research sponsored by EPRI.

EPRI would like to acknowledge the contributions of the following organizations and individuals:

ABB, Power Generation
Wickliffe, Ohio
Mark Bitto and Ralph Porfilio

Arkansas Electric Cooperative Corporation
Little Rock, Arkansas
Michael Massery

Emerson Process Management Power & Water Solutions
Pittsburgh, Pennsylvania
Richard Stafford

General Electric Company
Salem, Virginia
John Plenge, John Emery, and
Thomas Finucane

Invensys Operations Management
Foxboro, Massachusetts
Rick DeVoe and Phil Knobel

Southern Company
Charlotte, North Carolina
James Goosby

Tennessee Valley Authority
Knoxville, Tennessee
Josh Brewer

This publication is a corporate document that should be cited in the literature in the following manner:

Distributed Control System Life Cycle Management: Guidelines for Planning and Managing the Life Cycle of Distributed Control Systems. EPRI, Palo Alto, CA: 2013. 3002001123.

ABSTRACT

Power producers are often not concerned with the life cycle of a control system until they receive a notification from the manufacturer that the system is no longer supported. This situation results in a reactive effort to gain information, develop a plan, obtain funding, and execute an upgrade project. Effectively managing the life cycle of a control system requires a proactive approach, including gaining information about the installed system and its expected life span and the available end-of-life options, drafting a plan that outlines an optimal strategy and the associated timing, obtaining the approval and funding for the plan, and, finally, executing the plan.

Considering several strategies for managing the life cycle of a distributed control system, the optimal strategy will balance the cost and the risk. The cost includes the installation and lifelong maintenance of hardware and software for the control system, programming tools, and human-machine interfaces. The risk includes plant trips caused by hardware failures and possible extended outages because of the unavailability of replacement parts.

This report covers factors that affect the life of a control system and outlines five different strategies for managing a control system's life cycle. It lists the advantages and disadvantages of each strategy and provides guidelines for determining the most suitable strategy or combination of strategies, given the business environment and the state of the control equipment for a particular plant or group of plants. The report provides methods for determining cost and predicting risk that can be used to make informed, cost-reducing decisions, and it covers life cycle management guidance provided by several control system manufacturers.

The report also covers the steps that a power producer can take to develop a life cycle management plan for its control systems. It describes the information needed to determine the best path forward and helps establish the required timing for planning, funding, and executing upgrade projects.

Because several of the life cycle management options include extending the working life of currently installed control systems, the report examines the North American Electric Reliability Corporation Critical Infrastructure Protection standards for cyber security in the context of bringing legacy control systems and supporting computer equipment into compliance with these standards.

Keywords

Control system modernization
Control system upgrade
Cost-benefit analysis
Distributed control system (DCS) life cycle management
Legacy control system

ABBREVIATIONS AND ACRONYMS

BES	bulk electric system
CIP	Critical Infrastructure Protection
CPU	central processing unit
DCS	distributed control system
DOS	disk operating system
ESP	electronic security perimeter
FERC	Federal Energy Regulatory Commission
FTP	File Transfer Protocol
HMI	human-machine interface (computerized operator interface)
IEC	International Electrotechnical Commission
I/O	input/output
IRR	internal rate of return
ISA	industry standard architecture
IT	information technology
NERC	North American Electric Reliability Corporation
NPV	net present value
O&M	operation and maintenance
OEM	original equipment manufacturer
OLE	Object Linking and Embedding
OPC	OLE for Process Control
PCI	peripheral component interconnect
PLC	programmable logic controller
PSP	physical security perimeter
TCO	total cost of ownership
TCP/IP	Transfer Control Protocol over Internet Protocol
USB	Universal Serial Bus
VM	virtual machine

CONTENTS

***1* THE DISTRIBUTED CONTROL SYSTEM LIFE CYCLE 1-1**

Technology Life Cycle 1-1

Product Life Cycle 1-2

Factors Influencing the Control System Life Cycle 1-3

Equipment Reliability 1-3

Obsolescence 1-4

Cost of Maintenance 1-5

Technological Advances 1-7

Business Opportunities 1-7

Connectivity 1-7

System Expansions 1-8

Cyber Security 1-8

Programming Tools 1-8

Workforce Turnover 1-8

Control Room Consolidation 1-9

Environmental Regulation Compliance 1-9

Standardization 1-9

Usable Plant Life 1-9

Life Cycle Management Challenges 1-10

***2* DCS LIFE CYCLE MANAGEMENT 2-1**

DCS Upgrade Options 2-1

Rip and Replace 2-1

Partial Upgrades 2-2

Human-Machine Interface 2-3

Controllers 2-4

Controller Network Gateway 2-5

I/O Modules 2-6

I/O Gateway 2-7
Wiring Terminations 2-8
Upgrade Versus Migration 2-8
Migration Tools 2-9
Function Block Converters 2-9
Code Translators 2-9
Reverse-Engineering Tools 2-9
Migrating to New Features 2-9
DCS Life Cycle Management Strategies 2-10
Aggressive 2-10
OEM-Directed 2-11
Fixed Cost 2-11
Cost-Justified 2-12
Run to Fail 2-13
Comparison of Strategies 2-13
Strategies for Extending HMI and Workstation Life Cycles 2-14
Replacing the System 2-15
Repairing the System 2-15
Using Virtualization 2-16

***3* OEM VIEWS ON LIFE CYCLE MANAGEMENT 3-1**
ABB Group 3-1
Evolution Without Obsolescence 3-1
Legacy System Life Cycle and Support 3-2
Migration to Symphony Plus 3-2
Symphony Plus Life Cycle 3-3
Fleet-Wide Life Cycle Management 3-3
Emerson 3-3
Legacy System Life Span 3-3
Legacy System Support 3-3
Migration to Ovation 3-3
Ovation Life Cycle 3-4
Fleet-Wide Life Cycle Management 3-4
General Electric 3-4
HMI Life Cycle 3-4

Legacy Control System Support 3-5
Control System Migration 3-5
Mark IV to Mark VIe 3-5
Mark V to Mark VIe 3-6
Mark VI to Mark VIe 3-6
New System Life Cycle 3-6
Forced Upgrades 3-6
Fleet-Wide Strategy 3-7
Invensys 3-7
Legacy System Support 3-7
I/A Series System Life Cycle 3-8
Migration from Legacy Systems 3-9
Migration from Old I/A Systems 3-9
OEM/Technology Selection 3-9
Evaluation Criteria 3-10
Comparison Matrix and Evaluation 3-11
Other Factors 3-13
Product Life Cycle 3-13
Service Offering/Reputation 3-13
Migration Tools 3-13
Company Standard 3-13
Cost 3-13

***4* COST-AND-BENEFIT ANALYSIS 4-1**
Total Cost of Ownership 4-1
Application of the TCO to Dissimilar Options 4-2
TCO Analysis Timeframe 4-3
Net Present Value and Internal Rate of Return 4-3
Example Calculation 4-3
Determining the Cost 4-6
O&M Cost of a Control System 4-6
Control System Reliability and Cost of Failures 4-6
Terminology 4-7
Reliability Prediction Methodology 4-7
Reliability Prediction Procedures and Tools 4-7

Accuracy of Reliability Predictions....4-8
Plant/Fleet Statistics....4-9
Reliability over Time....4-10
Predicting Future Failure Rates....4-11
Projected Maintenance Cost....4-12
Cost of a Unit Trip....4-13
Probability of Failures Causing Unit Trips....4-13
Trip Risk Assessment....4-13
Total Cost of a Unit Trip and Downtime....4-15
Cost of Downtime....4-16
Cost of Startup and Cycle....4-16
Justifying Upgrades Based on Unit Trips....4-17
Cost of an Upgrade....4-17
Benefits of an Upgrade....4-18
Benefit of Reduced Costs....4-18
Release of Spare Parts....4-18
Improved Thermal Performance....4-18
Environmental Compliance....4-18
Reduced Operator Error....4-19
Improved Monitoring and Diagnostics....4-19
OEM Versus User Perspective....4-19
Cost-Benefit Analysis....4-19

5 **THE DCS LIFE CYCLE PLAN....5-1**
Components of the Plan....5-1
Life Cycle Management Objectives....5-1
Business Objectives for the Unit....5-2
Control System Audit....5-2
OEM Support and Obsolescence....5-3
Choosing the Optimal Strategy....5-4
Project Plan....5-4
Parts Relocation Strategy....5-4
Business Case....5-5

6 NERC CIP COMPLIANCE WITH LEGACY CONTROL SYSTEMS 6-1
Control System Cyber Security 6-1
The Cyber-Threat Spectrum 6-1
Organized Crime 6-1
Insiders 6-2
Targeted Attacks 6-2
Distribution Mechanisms 6-2
Importance of Cyber Security in the Power Industry 6-2
The NERC CIP Standards 6-3
CIP-002: Critical Cyber Asset Identification 6-4
Version 4 6-4
Version 5 6-4
Impact on Legacy Control Systems 6-5
CIP-003: Security Management Controls 6-5
Version 4 6-5
Version 5 6-6
Impact on Legacy Control Systems 6-6
CIP-004: Personnel and Training 6-6
Version 4 6-6
Version 5 6-7
Impact on Legacy Control Systems 6-7
Access Revocation 6-7
CIP-005: Electronic Security Perimeters 6-7
Version 4 6-7
Version 5 6-8
Impact on Legacy Control Systems 6-8
CIP-006: Physical Security of Critical Cyber Assets 6-8
Version 4 6-8
Version 5 6-8
Impact on Legacy Control Systems 6-9
CIP-007: Systems Security Management 6-9
Version 4 6-9
Version 5 6-10
Impact on Legacy Control Systems 6-11

Disabling Unnecessary Logical Ports 6-11
Disabling Unnecessary Physical Ports 6-11
Disabling Unnecessary Drivers 6-11
Security Patch Management 6-11
Malicious Code Prevention 6-12
System Access Control 6-12
Security Event Monitoring 6-12
Other Requirements 6-12
CIP-008: Incident Reporting and Response Planning 6-13
Version 4 6-13
Version 5 6-13
Impact on Legacy Control Systems 6-13
CIP-009: Recovery Plans for Critical Cyber Assets 6-13
Version 4 6-13
Version 5 6-13
Impact on Legacy Control Systems 6-13
CIP-010-1: Configuration Change Management and Vulnerability Assessments 6-14
Impact on Legacy Control Systems 6-14
CIP-011-1: Information Protection 6-15
Impact on Legacy Control Systems 6-15
Summary 6-15

7 **CONCLUSIONS 7-1**

8 **REFERENCES 8-1**

LIST OF FIGURES

Figure 1-1 Phases and sales volumes over a product's life cycle....1-2
Figure 1-2 Bathtub curve depicting failure rate over time....1-3
Figure 1-3 Typical DCS component life cycle in years....1-4
Figure 1-4 Approximate age of installed control systems....1-4
Figure 1-5 Expected cost and availability of replacement parts over time....1-6
Figure 1-6 A flood of used parts stabilizing price and availability for many years....1-6
Figure 2-1 Connection points between DCS subsystems....2-3
Figure 2-2 Installing a new HMI onto an existing control system....2-4
Figure 2-3 Two options for connecting new controllers to existing I/O....2-5
Figure 2-4 Connecting new controllers to an existing control system through a controller network gateway....2-6
Figure 2-5 Upgrading I/O while keeping existing wire terminations....2-6
Figure 2-6 Options for upgrading controllers and I/O while keeping existing wire terminations....2-7
Figure 2-7 Using an I/O gateway to add more I/O to a legacy control system....2-8
Figure 4-1 Bathtub curve depicting failure rate over time....4-10
Figure 4-2 Predicting future failure rates....4-12
Figure 5-1 Example of a component life cycle map indicating support available and obsolescence....5-3

LIST OF TABLES

Table 2-1 Cost and risk of DCS life cycle strategies 2-13
Table 3-1 Product life cycle phases, as defined by Invensys 3-8
Table 3-2 Sample comparison matrix 3-12
Table 4-1 NPV over time of maintaining versus upgrading a control system 4-4
Table 4-2 IRR of a control system upgrade over maintaining the current system 4-5
Table 4-3 Assessing the trip risk associated with control system failures 4-14
Table 4-4 Median hot- and warm-start costs of various types of units 4-16
Table 4-5 IRR of upgrading the DCS and reaping benefits versus maintaining the old system 4-20

1
THE DISTRIBUTED CONTROL SYSTEM LIFE CYCLE

The life cycle of a control system can be viewed from three different perspectives that build on each other to finally govern the overall life cycle of a distributed control system (DCS). First, the technology being used in control systems has life cycles shaped by advances in networking, central processing unit (CPU), communications, and software. Second, as commercial products, control systems have their own life cycles that are influenced by technology, market trends, and competitiveness. Finally, from an end-user's perspective, the control systems in use have a limited life span influenced by failure rates, original equipment manufacturer (OEM) support, and technological trends.

Technology Life Cycle

Technology life cycle refers to the stages a certain technology goes through over time. It begins with research and development. Some refer to a new or emerging technology as *bleeding edge* [1]. The technology shows high potential but has not demonstrated its value or robustness. Examples of this include the early implementations of microprocessors, OLE for process control (OPC), Ethernet, and Windows human-machine interfaces (HMIs). There are usually a few, if any, competitors offering the same emerging technology. In general, the power industry takes a more conservative approach than adopting bleeding-edge technology.

As a technology progresses, it becomes known as *leading edge*. It has proven its viability in the marketplace but is still new enough that it may be difficult to find knowledgeable personnel to implement or support it. Competitive offerings begin to emerge in the marketplace. If the technology addresses a burning issue in power plants, for example, it lowers emissions, early adopters within the power industry may begin testing and implementing the technology.

When a particular technology is widely adopted as the right solution, it becomes known as *state of the art*. The technology is offered by most competitors, and skills for its implementation and maintenance are abundantly available. If the technology applies, it would be adopted by the power industry. In the case of process control technology, implementing new control systems is seldom pulled by new technology and rather pushed by obsolescence.

As the technology ages, it is referred to as *dated*. It is still useful and sometimes implemented, but a replacement leading edge technology is making inroads into the marketplace and begins taking its place.

At some point, technology becomes obsolete. It has been superseded by other state-of-the-art technology. Obsolete technology loses OEM support, it may become significantly more expensive to maintain over time, and the number of skilled people available to support it decreases.

When buying a control system, one becomes tied to its technologies. It is important to understand where these technologies are in their respective life cycles. This is particularly

important in modern control systems incorporating multicore CPUs, networking, embedded historians, analytics, alarm management, equipment diagnostics, sequential automation, and advanced control technologies. Upgrading to a new control system, based on dated technology, could significantly shorten its useful life.

Product Life Cycle

In the field of product marketing, a *product life cycle* is used to map the commercial life span of a product in four stages: introduction, growth, maturity, and decline [2]. The cycle directly relates to their sales volumes and profitability (Figure 1-1). Control systems follow the same cycle.

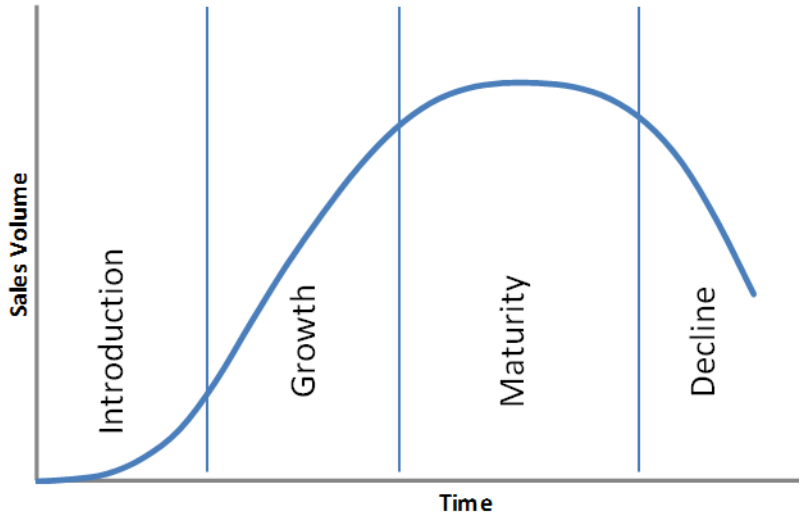


Figure 1-1
Phases and sales volumes over a product's life cycle

The remaining time to obsolescence becomes shorter as a product moves through this life cycle. Interviews with OEMs revealed that they will typically stop marketing a system at the end of its maturity phase, stop production during the decline phase, and stop sales at the end of the decline phase when the stock has run out. Most OEMs continue to repair failed components or replace them with used parts, but some do this for a few years only.

Technical product support follows a similar trend in which the OEMs initially provide full technical support and field services, but these offerings decline later in the product's active life cycle and are typically terminated, at some point. However, some OEMs indicated that they continue providing support for legacy systems.

Toward the end of a control system's product life cycle, a niche market opens up for third-party vendors to pick up the maintenance and support of the obsolete system. These companies would typically repair failed equipment and/or buy decommissioned hardware from end users who have replaced their obsolete control systems. In this way, the third-party vendors have a supply of spare parts to continue supporting obsolete systems for many years after OEM has ended its support. A search on www.google.com for various types of DCS and replacement parts revealed dozens of vendors who provide parts, repairs, and site support services for legacy control systems.

It is foreseeable that over time, the number of installed legacy systems will inevitably dwindle to the point where their support no longer provides a feasible level of business. At that time, the third-party vendors will also drop their support for these systems. Users of a control system in this stage of its life will likely find it very difficult and expensive to get replacement parts, and personnel skilled to work on these systems will be hard to find. Based on an overall life cycle of two to three decades, it is believed that this end of support will spread slowly from one vendor to the next, possibly over a decade from its first signs.

Factors Influencing the Control System Life Cycle

Late in the life of a DCS, many factors come into play and make it difficult to continue maintaining the current control system. Users are then forced to explore alternatives such as upgrading or replacing their control systems. Where applicable, these factors can be used in a business case to justify the expenditure of a control system upgrade or migration. Many of them will be covered in more detail in the section on cost and benefit analysis.

Equipment Reliability

The failure rate of electronic equipment changes over time. Initially, the failure rate is relatively high, but if equipment is properly "burned in" by manufacturers, few end users will experience this initial high failure rate. During burn-in, weak components fail, and the failure rate of the remaining equipment drops significantly. After burn-in, failures occur randomly but infrequently, and the failure rate stays low for many years (the duration depends on component stress level and service conditions such as temperature). Eventually, the failure rate increases as the equipment ages and moves through the wear-out phase. Over time, the failure rate takes on the shape of a bathtub (Figure 1-2) and is commonly referred to as a *bathtub curve*.

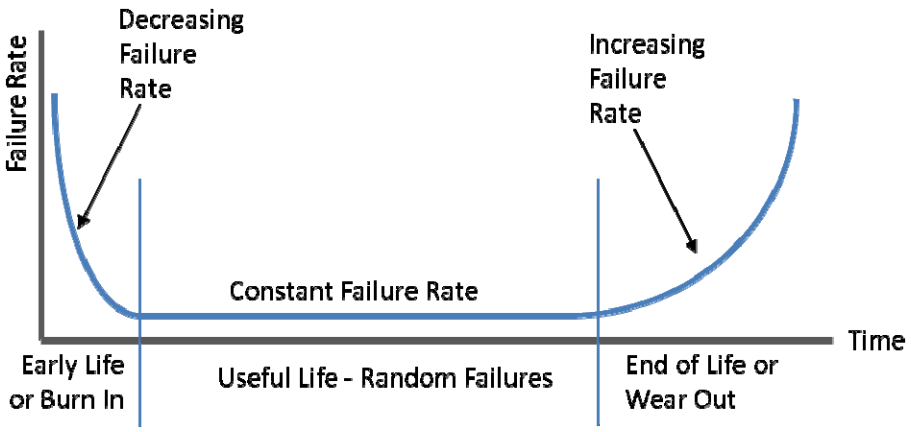


Figure 1-2
Bathtub curve depicting failure rate over time

Continuing the use of control system hardware into the wear-out phase elevates the risk of unit trips and unplanned downtime.

Obsolescence

The ARC Advisory Group estimated that the installed base of legacy process automation systems (across all industries) reaching the end of their useful life is equivalent to over $65 billion in replacement cost [3].

Figure 1-3 shows the typical life span in years of various DCS components, as given by ARC. However, obsolescence does not happen on a specific date and rather is a gradual process that starts with the OEM discontinuing support. Spare parts then become harder to procure and more expensive to repair. At some point, spares become too expensive or too hard to find, and maintaining the control system becomes difficult, and the system must be replaced or upgraded.

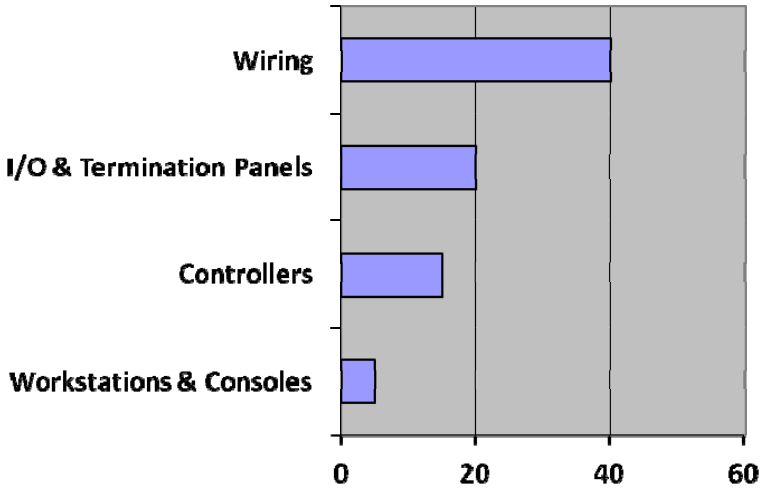


Figure 1-3
Typical DCS component life cycle in years [3]

In a survey done by ARC (across all industries), more than 85% of the respondents said that they have used control systems beyond the manufacturer's stated obsolescence date [3]. Another ARC survey indicated that roughly one third of installed control systems were younger than 10 years, roughly half were between 11 and 20 years old, and the remainder were older than 20 years (Figure 1-4). According to the same survey, only 1.5% of installed control systems were older than 30 years.

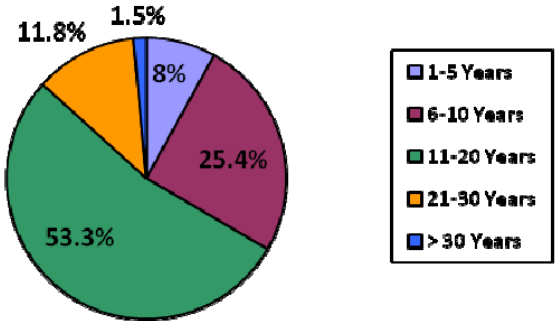


Figure 1-4
Approximate age of installed control systems [3]

In a group discussion on the LinkedIn website about the useful life of programmable logic controllers (PLCs) [4], comments were made that control system hardware will last easily 15 to 20 years and that, normally, end of life can be considered in the 20- to 25-year range. Several examples were given of long lives for DCSs and PLCs, as follows:

- General Electric Series 6 PLC still running after 25 years
- ABB NETWORK 90 controllers still running after 30 years
- Siemens (Moore/Texas Instruments) TI 565 and 505 controllers still running after 30 years
- SAIA Burgess PLCs (originally Landis & Gyr) still running after 30 years

Although some contributors described harsh conditions in which PLCs were operating fault-free over many years, it was generally recommended that control systems be housed in climate-controlled environments (temperature and humidity controlled, free of dust and vibration) and powered from a clean source (no voltage spikes or supply interruptions).

The group discussion also revealed a general perception that older systems were more robust and lasted longer than modern systems. An example was given of the input/output (I/O) on new systems that failed under stress conditions that the older I/O easily handled. The reasoning was given that newer systems are designed with much less engineering tolerance and manufactured with lower quality processes than older systems to bring down cost.

Programming tools seem to be affected by obsolescence to a greater extent than the control systems. Legacy programming software (especially for PLCs) is often a disk operating system (DOS) program. The last windows operating system that fully supported running DOS programs was Windows 98. It is impossible to run Windows 98 on modern computer hardware, so, if the programming computer fails, it has to be replaced with one of the same age (which is likely close to the end of its life, too). The same applies to legacy HMI software that runs on commercial, off-the-shelf computers in contrast to the older systems that had hardened operating consoles.

Cost of Maintenance

Toward the end of a control system's life, the OEM ceases the manufacture of replacement parts, after which their inventory is depleted over time and OEM sales for new parts of the product come to an end. Although replacement parts may still be available for many years from third-party vendors who deal in obsolete control system equipment, the price of these parts increases as they become less available (Figure 1-5). Replacement of failed control system modules then becomes more costly, and the overall maintenance cost is further inflated by the increased failure rate of these modules.

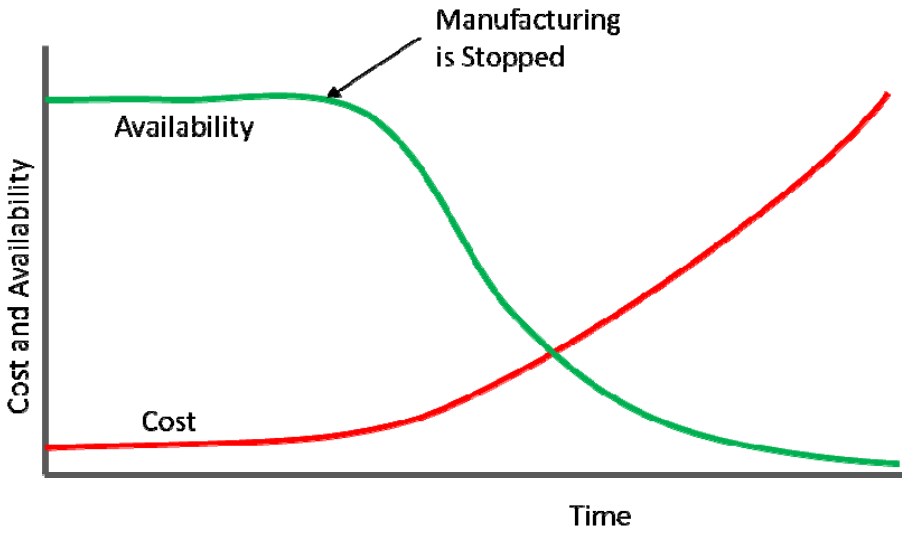


Figure 1-5
Expected cost and availability of replacement parts over time

Simple economics tells us that price will increase when availability decreases. However, the availability of control system spare parts does not necessarily decrease linearly over the remaining life of a control system. Initially, when the production of new spare parts is stopped, the price increases because of the reduction in supply. However, over the ensuing years, more spare parts become available from decommissioned (upgraded or replaced) control systems. Also, because the number of legacy systems in service reduces over time, the demand for spare parts may even decrease. These factors could have a stabilizing effect on price (Figure 1-6) and may even cause prices to decrease.

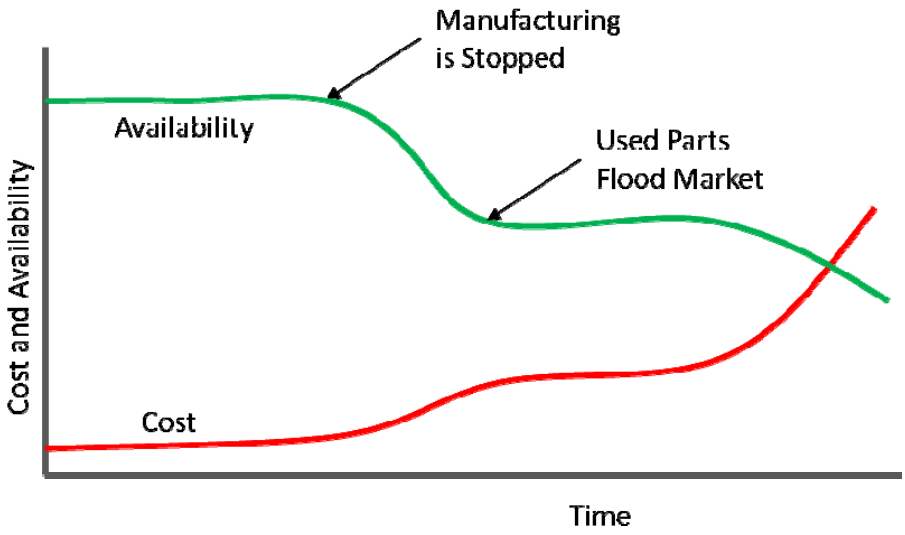


Figure 1-6
A flood of used parts stabilizing price and availability for many years

Two cases in point: (1) A company located in Long Beach, California, specializing in Bailey NETWORK 90 and INFI 90 DCSs offers unused surplus and refurbished used DCS components at 15% to 20% of the original cost of new components. (2) An Allen-Bradley PLC 5/80 with Ethernet interface that sold for $7500 in early 2000 can now be found on eBay listed for about $2000.

However, there may still be a few parts with much higher failure rates, causing shortages and sharp increases in price. The price of replacement parts may also increase if fewer systems are decommissioned than their parts are consumed, therefore, depleting the pool of spare parts over time.

Technological Advances

The latest offerings of all control system vendors include technologies and applications that were not available or in widespread use two decades ago. These include the following:

- New control algorithms, such as model-based steam temperature control
- Sequential automation for automatic startup and shutdown of equipment
- Combustion optimization
- Alarm management
- Operator effectiveness tools, such as embedded procedures
- High-performance HMI
- Support for asset management systems
- Fieldbus, HART, and multivariable sensors
- Open-standard connectivity to other systems, such as OPC

During interviews with control system OEMs, vendors said that technological advances available in their new control systems are a key driver for many users to upgrade their legacy systems.

Business Opportunities

Changes in the market may open up desirable business opportunities that cannot be harvested because the installed control system is not capable of meeting the demands. One example would be a power plant that was built for base loading and now has to do load following to be economically viable or to increase profits. A legacy control system may not have the control strategies in place that allows active load following, and its capacity or capability may not support these types of controls.

Connectivity

Old control technology typically had proprietary networks and was difficult to connect with other systems, such as process historians and combustion optimization systems. Some old control systems did not support remote I/O, and most did not support the Fieldbus standard(s). New control systems support open-standard communications, such as OPC, HART, and Foundation Fieldbus.

System Expansions

A legacy control system may have no spare capacity for adding new controls, such as environmental controls. This may be caused by a combination of factors, including hardware (for example, I/O count or rack space), firmware (for example, maximum control blocks used), or processing-power.

Cyber Security

The North American Electric Reliability Corporation (NERC) has developed Critical Infrastructure Protection (CIP) standards with specific requirements to be met by power plants and other responsible entities. The NERC CIP compliance program helps protect the power generation and transmission systems in North America.

Power plants are currently required to comply with Version 3 of the NERC CIP standards. Version 4 is due to become effective in April 2014. Version 5, which includes additional requirements, has been approved by the NERC board of trustees and, at this time, is awaiting final approval by the Federal Energy Regulatory Commission (FERC).

DCSs, HMIs, engineering stations, and other control-system-related computer equipment have to comply with the NERC CIP standards. Power plants with legacy DCS and outdated computer systems might find it increasingly difficult and/or laborious to comply with certain NERC CIP requirements. This could become a driving force for upgrading these systems if their modern replacements can be brought into compliance with less effort or cost. A comprehensive discussion of this matter is presented in Section 6: NERC CIP Compliance with Legacy Control Systems.

Programming Tools

Software and hardware used for programming a legacy control system may be running on proprietary or obsolete operating systems with no OEM support. If the programming hardware fails, a virtual equivalent of it is required because the old software will likely be incompatible with new hardware.

For example, old operating systems do not come with drivers for new hardware, and new hardware rarely has drivers supporting decade-old software. Software may require floppy disks for installation, which are no longer available or supported on most new computer systems. Hardware keys for programming the software are typically plugged into parallel ports that have to be specifically added to new computers, if they are supported.

Although a DCS upgrade can likely not be justified based solely on outdated programming tools, new versions may provide substantial improvements in programming and faultfinding that should be added to the upgrade's justification.

Workforce Turnover

Thousands of years of experience and knowledge are lost from industrial plants annually, and much of this knowledge is never captured in any meaningful way in the plant [3]. This massive loss of experience manifests itself in the need to contract experienced workers out of retirement to assist with plant startups and training. The loss of expertise from the field of process automation leads to a global scarcity of people able to program, troubleshoot, and maintain legacy control systems.

As control systems age and are replaced with new-generation systems, training on the legacy systems become increasingly difficult to find. Users often have to know DOS or Unix commands and special keystrokes to use legacy programming software, and younger technicians simply do not like working on old, cumbersome systems.

This trend could leave a legacy control system virtually orphaned from an on-site support perspective. One way around this would be to establish a service agreement with a third-party vendor that still provides field support for the control system, but this will likely be more costly than the in-house solution. Another option for a fleet owner would be to centralize DCS support services. Loss of in-house expertise could also cause additional downtime after a unit trip if an off-site field-support engineer/technician needs to drive across town or fly across the state to assist with troubleshooting.

Control Room Consolidation

Manpower can be reduced by consolidating separate control rooms into one, so that operators from different units can help with startups and emergency situations at other units, reducing the need for additional staff. Control room consolidation relies heavily on new HMI technologies that likely require a DCS upgrade.

Environmental Regulation Compliance

An old DCS may be incapable of performing more robust control strategies required for reducing emissions to levels required by ever-increasing regulatory standards. For example, controlling fuel and air flow to individual burners may be required for reducing NOx levels, but an old control system might not have the capacity to run the additional controls.

Strategically upgrading control systems and implementing advanced combustion controls on selected units in a fleet may allow fleet managers to offset high emissions on other units.

Standardization

If power plants change ownership and become part of a large fleet, their control systems may be of a different type and incompatible with the existing fleet. This complicates spares holding, engineering support, training, and vendor relations. If nonstandard control systems are mature or obsolete, the latter provides additional motivation to replace them with new, standardized systems.

Usable Plant Life

Finally, the DCS life cycle might be influenced by the future of the plant. If the plant is scheduled to be decommissioned in the foreseeable future, performing any type of DCS upgrade makes little business sense. If the future of the plant is uncertain, DCS upgrades are also not advisable. Control system upgrades might only be considered if the plant has a potential life of a decade or longer.

Life Cycle Management Challenges

Several challenges encumber the planning of DCS life cycle and replacements, as follows:

- **Timing**. Many DCS vendors repair and replace failed cards long after the production of new cards has ended. Even in cases in which a DCS is no longer supported by the OEM, third parties continue providing this service. Unless the end of production is used as a signal (and this might be premature), there is no clear line marking the time when a DCS becomes obsolete.
- **Cost justification**. Even if the cost of spare parts increases after the OEM has stopped production, continuing to maintain the legacy system remains a cost-effective option.
- **Choosing the right option**. Several upgrade options exist. These range from doing nothing to complete replacements. Each increment becomes more expensive but has distinct benefits.
- **Life cycle mismatches**. Modern computer systems and software have life cycles that are much shorter than those of the DCS. It is often difficult keeping all systems compatible and, at the same time, out of obsolescence.
- **Creating the plan**. Life cycle management can be a daunting task if an engineer suddenly gets tasked with it. A newcomer may not know what upgrade options exist, what information is needed to make a decision, and what constitutes a DCS life cycle management plan.

The investigation and findings documented in this report aim to address these challenges and other issues related to managing the life cycle of a control system.

2
DCS LIFE CYCLE MANAGEMENT

The term *DCS life cycle management* normally refers to decisions made and strategies followed at the end of a DCS's life to either extend its life or upgrade the DCS to a new system. Ideally, end-of-life strategies should be considered when specifying a new control system, but because a control system's life spans several decades, decisions made at the beginning may no longer be relevant at the end. For most of a DCS's life, life cycle strategies take a backseat to other priorities.

After decades of operation requiring only minimal maintenance, issues such as decreased reliability, increased cost and scarceness of spare parts, and lack of OEM support draw attention back to the DCS and managing its life cycle (which, at that time, means making end-of-life decisions). Although several options may be available, if plant and corporate management bases decisions mostly on cost, it is difficult to justify any other strategy.

In contrast to DCS hardware with an average life span of 20 years, computer systems such as those used for operator interfaces, programming tools, and process data historians often have much shorter life cycles, typically lasting less than a decade. Computer hardware is much less reliable than DCS hardware, consequently requiring more frequent replacements. On the other hand, computer systems cost orders of magnitude less than control systems, making end-of-life decisions easier than those for DCSs. Options for extending the life cycle of these systems are covered at the end of Section 2.

DCS Upgrade Options

Before exploring the various DCS life cycle management options, this report will explore various options for replacing and upgrading control systems when they do come to the end of their lives. Different control system OEMs offer varying degrees of flexibility for modernizing control systems, and the availability of options sometimes depends on the version of the installed DCS. Users should consult their DCS vendor to establish which of the following options discussed is available to them.

Rip and Replace

Also called *bulldoze replacement*, in this option, the entire DCS is replaced with new equipment. This includes I/O, racks, and HMI. This is the most severe of all DCS upgrade options and may be followed when a plant changes to a completely new type of DCS from a different manufacturer. (It will be discussed later that vendors typically have adapters to other vendor's wiring terminations, which can greatly reduce project scope and cost.) Rarely is the rip-and-replace approach necessary when upgrading a DCS to a newer version from the same manufacturer.

To reduce downtime during a rip-and-replace project, the new control system is built in its entirety and configured while the plant continues to run with the old DCS. These activities are normally done at the OEM's facilities. Old control strategies and custom code are translated (if possible) or reverse engineered and reconfigured in the new controllers. Old operator graphics are translated, replicated, or redesigned (preferably) in the new HMI. The factory acceptance test is performed, and the new system is taken to the site and installed. Where necessary, new instrumentation is installed and wired to the new system, the plant is shut down, and all of the wiring is connected to the new I/O. The wiring out to the field devices is loop checked all the way back to the control system and to the HMI. Instrumentation and Controls staff are trained on the new control system, and operators are trained on the new HMI. The plant is then started up with the new DCS and HMI.

The rip-and-replace option is the most costly option, including the highest cost for hardware, manpower, and downtime. It is the most disruptive to operations and carries the most project risk. According to one DCS vendor, such a project could require 1800 man-days of OEM and customer time and cost four million dollars, not counting loss of revenue during downtime. One power company that contributed to this research claimed that they typically expect to pay six to eight million dollars for a DCS rip-and-replace project. The advantage of the rip-and-replace approach is that the entire control system and HMI are new and that all of the subsystems are on the same version level and are compatible with each other. It provides a fresh, new start, and all of the components are at the beginning of their life cycles.

Partial Upgrades

In contrast to the rip-and-replace option, most control systems do not have to be upgraded as one monolithic system. It makes economic sense to upgrade only the subsystems that offer the best return on investment or the greatest reduction in risk of failure or obsolescence. Looking at a control system as a modular instead of a monolithic system reveals several possibilities for partial upgrades.

The modular control system consists of a stack of subsystems consisting of different layers containing the HMI, controllers, I/O modules, field-wire terminations, and field devices. These subsystems are serially connected through well-defined connection points (Figure 2-1). A control system can potentially be migrated to a newer system in a stepwise approach by upgrading subsystems between these connection points [5].

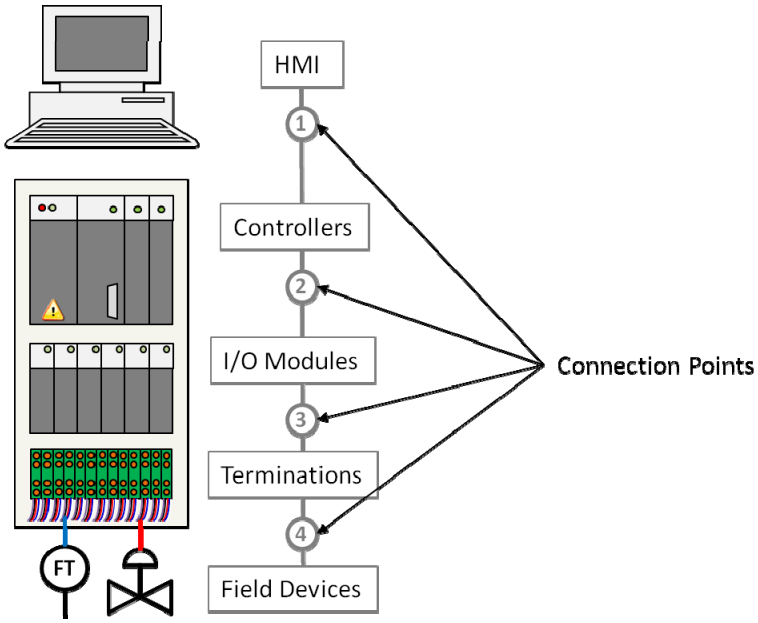


Figure 2-1
Connection points between DCS subsystems

To determine the optimal scope of a partial upgrade, all of the subsystems should be assessed in terms of cost, risk, and benefit of upgrading versus the status quo of maintaining the existing equipment. Subsystems can then be strategically selected for cost-beneficial upgrading, if the OEM offers that possibility. Note that there are large differences in partial-upgrade flexibility offered by different OEMs, and some parts have to be replaced in sets.

Human-Machine Interface

The HMI is at the highest level in the stack. HMIs have the shortest life cycle, and their technology changes the fastest, making them ideal candidates for a targeted upgrade while leaving the remainder of the control system in place (Figure 2-2). The HMI connects to controllers through a network that is typically also used for communications between controllers. The feasibility of upgrading only the HMI depends on the new HMI using the same communication protocol as the existing controllers and, if not, whether a communications interface is available to connect the HMI to the existing network. If the new HMI cannot be made to communicate with legacy controllers, both components have to be upgraded at the same time.

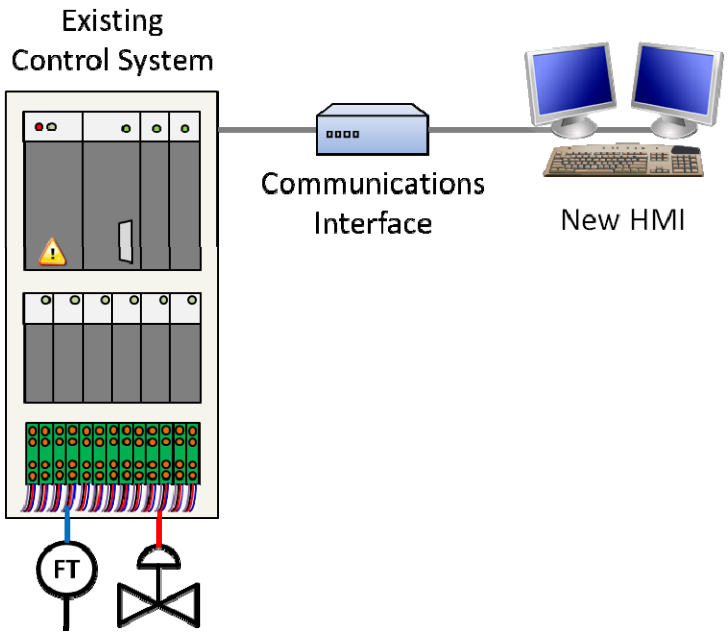


Figure 2-2
Installing a new HMI onto an existing control system

Graphics translation tools can greatly assist with migrating operator graphics from old systems to new ones, if such tools are available for the particular type of upgrade. However, to capitalize on the full potential of new HMI features and technologies, the operator graphics will likely have to be redeveloped. In this case, HMI redesign should be based on task analysis and not simply copying piping and instrumentation diagrams or copying the old graphic screens. An HMI philosophy using best practices and abnormal situation management guidelines for HMI design will be needed for consistency and to ensure that best practices are followed. Operators must be involved in the task-analysis and design processes, but care should be taken not to incorporate operator-driven features that do not comply with the HMI philosophy.

Controllers

It may be desirable in certain cases to upgrade controllers and take advantage of new technologies, but it is recommended to leave the existing I/O in place. Except for the addition of remote I/O and acceptance of the Fieldbus standards, there have been only minor advancements in I/O technology, leaving little to be gained from upgrading I/O modules. The ARC survey [3] also indicated a longer life span for I/O than controllers. To this effect, some DCS vendors allow existing I/O to remain in place while upgrading the upper layers of the control system.

To replace the controllers while leaving the old I/O in place, the connection between the two has to be considered. This connection could run directly through the backplane or through a network cable. On older control systems, both connection methods would likely be using a proprietary protocol. The feasibility of upgrading a controller while leaving its I/O in place depends on whether the OEM has changed the communication protocol and, if so, whether a communication interface is available to connect the two subsystems. If not, controllers and I/O have to be upgraded together.

For cases in which a new controller can be connected to existing I/O, some vendors provide form-fit controller modules that can replace the legacy controller in the same rack, whereas others provide cables and I/O interfaces to connect new controllers to the legacy I/O (Figure 2-3).

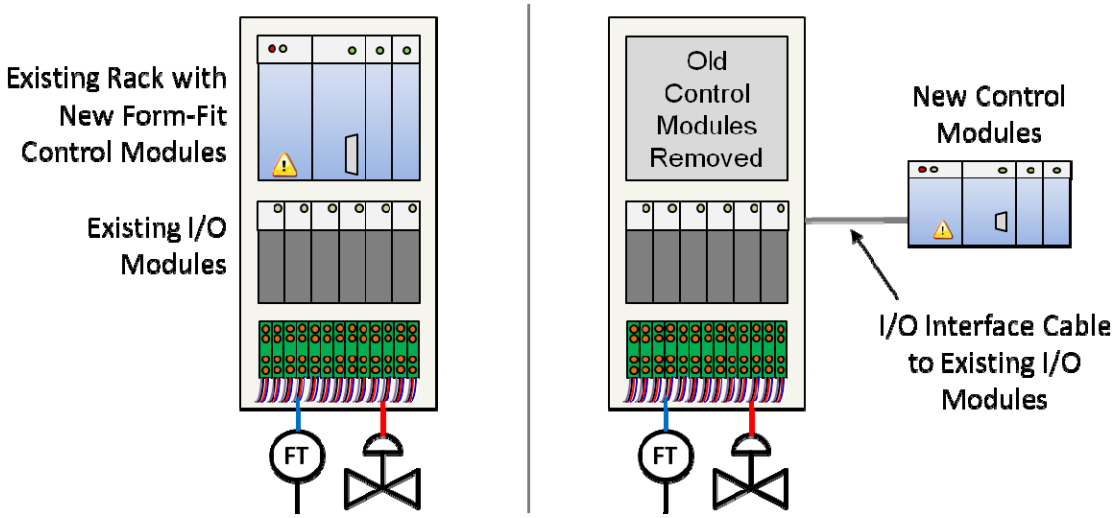


Figure 2-3
Two options for connecting new controllers to existing I/O

Much of the effort in upgrading controllers can go into migrating the control strategies and custom code from the legacy controller into the format used by the new controller. In some cases, conversion tools are available to help with this migration. Some OEMs state that their new controllers can faultlessly execute old code and old control strategies. The configuration is simply exported from the old configuration tool, imported into the new one, and exported to the new controller. Other vendors have indicated that manual intervention is required during their upgrades.

Controller Network Gateway

Controller network gateways provide peer-to-peer communication between legacy controllers and new controllers (Figure 2-4). This can be used to control new equipment (expansions) if the legacy control system cannot be expanded. Gateways provide protocol translation and throughput normalization (for example, converting fractional integers to floating point numbers). Gateways and their configuration can be costly, but this option would likely still be less expensive than replacing the legacy control system.

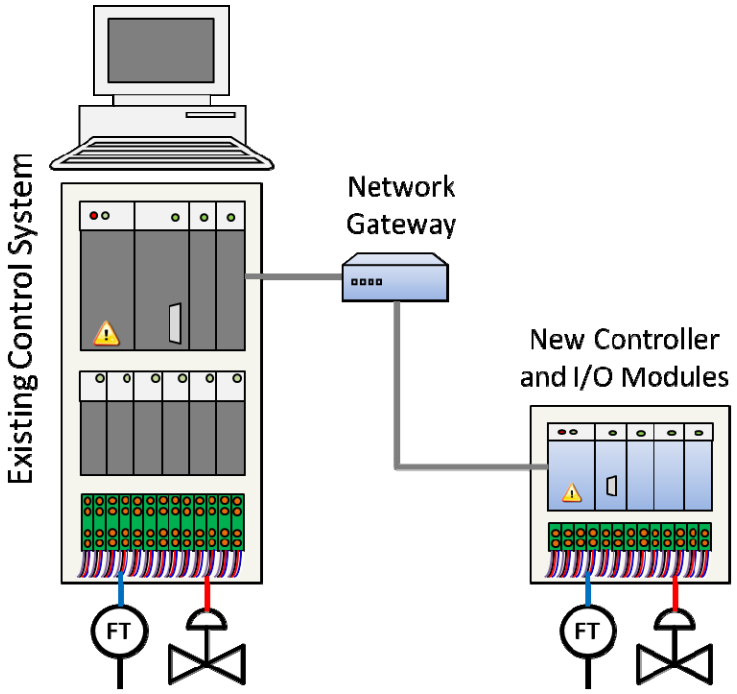


Figure 2-4
Connecting new controllers to an existing control system through a controller network gateway

I/O Modules

The next level down the control system stack contains the I/O modules, which convert the signals between the electrical formats used in the field and digital formats used in the DCS. The field wiring's termination blocks connect to the I/O either directly or through wiring harnesses. If the I/O has to be replaced while keeping the legacy wiring terminations in place (which is the recommended practice), I/O-connect kits consisting of ribbon cables or wiring harnesses can be used to connect legacy wiring connectors to new I/O modules (Figure 2-5).

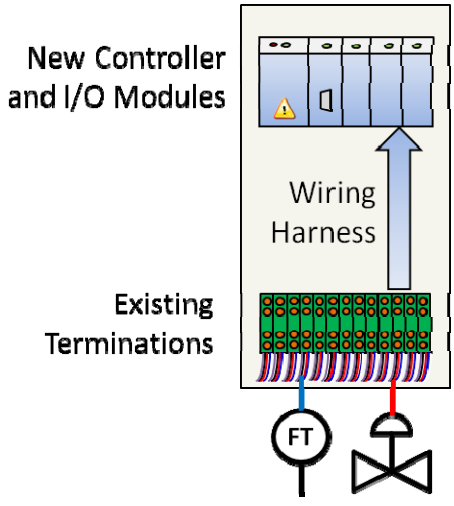


Figure 2-5
Upgrading I/O while keeping existing wire terminations

These I/O-connect kits preserve the existing I/O terminations and field wiring, which can significantly reduce overall project costs and the length of the outage required for the upgrade. Some upgrade solutions allow the I/O modules to be replaced with new form-fit modules and, in this way, reuse the existing rack and wiring terminations. This can be done in conjunction with installing form-fit control modules or with an interface cable to new control modules (Figure 2-6).

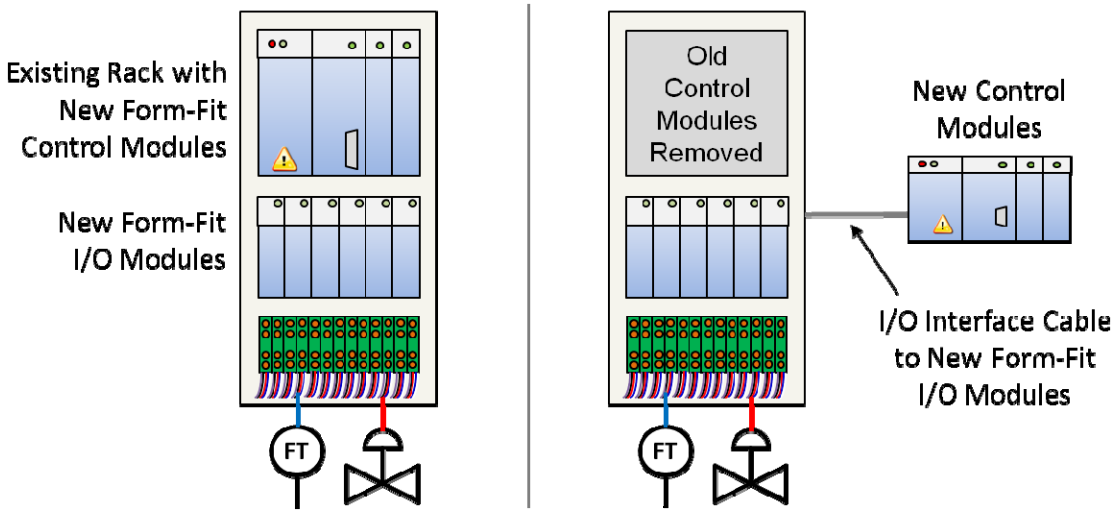


Figure 2-6
Options for upgrading controllers and I/O while keeping existing wire terminations

I/O Gateway

If additional I/O has to be added to an existing control system, and no rack space is available for doing so, a gateway or specialized I/O module can be used. An I/O gateway allows new I/O modules to be connected to legacy controllers (Figure 2-7).

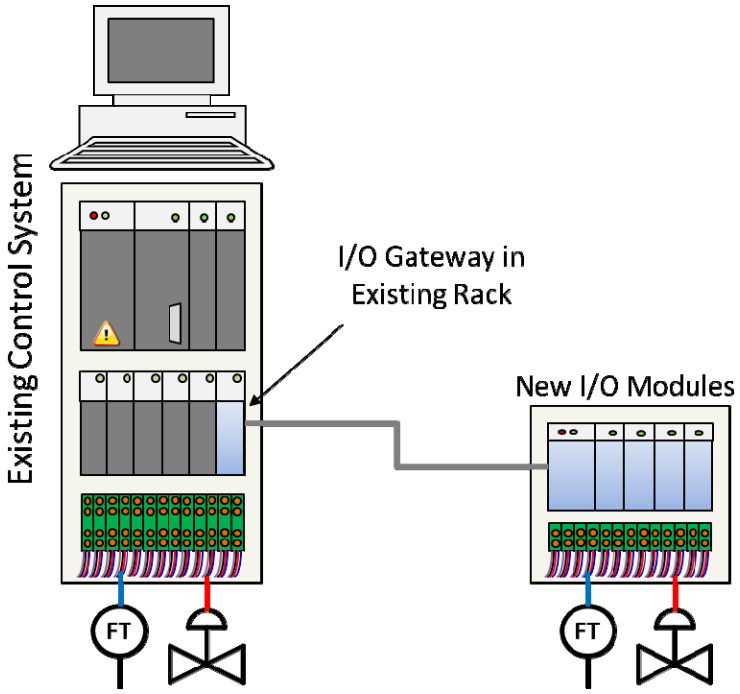


Figure 2-7
Using an I/O gateway to add more I/O to a legacy control system

Wiring Terminations

At the bottom of the stack, field wiring is individually connected to screw terminals in termination blocks. Partial DCS upgrades attempt (at minimum) to keep these wire terminations in place because reconnecting field wiring requires retesting each instrument loop. Reconnecting and retesting wiring are large efforts and can add substantial cost to a control system upgrade. An estimated 75% reduction in installation labor can be achieved by reusing the existing I/O connections and using adapters or interface cables to connect it to the I/O modules of the new control system [6].

Most vendors offer I/O connections to legacy terminals, and some vendors offer cable connections to other vendors' legacy equipment [7]. All four of the DCS vendors interviewed for this project have solutions for upgrading the control system without having to reconnect the field wiring.

Upgrade Versus Migration

Although the terms *upgrade* and *migration* are often used interchangeably, in that context, migration is normally associated with a smoother transition than an upgrade. The practical difference is that a migration reuses the configuration information (sometimes called *intellectual property/assets*) from the legacy system in the new system.

The difference between an upgrade and a migration can be illustrated with an analogy to computers. Upgrading a computer normally means all software have to be reinstalled, all printer and other drivers have to be reinstalled, and all of the personalization has to be redone. Instead of upgrading, if one could migrate to a new computer, all of the software, drivers, and other configurations will be automatically moved from the old machine to the new one.

A DCS migration actually consists of two tasks: (1) upgrading the DCS and (2) migrating all of the I/O configuration, control strategies, alarm configuration, and custom code to the new system. A control system migration will attempt to reuse as much as possible of the old control system's configuration to minimize the amount of reconfiguration required on the new system.

Migration Tools

Using tools to automate the migration can make a substantial difference to the time and cost of a project. Without these tools, substantial manpower would be required to manually reverse-engineer the code, control strategies, and operator graphics, and then to reprogram the new system accordingly.

Function Block Converters

Software tools have been created for converting control and logic functions from one system to the next [6]. Because basic function blocks are reasonably standard in functionality, these tools can save an enormous amount of time if they are available for the migration being planned.

Code Translators

Software tools have become available for migrating scripts and code from the older system to a new system. These tools work reasonably well for migrating from one version of a control system to the next but has been said to correctly convert only a maximum of 80% of code between different brands of the DCS [6]. This can result in an enormous effort trying to find the 20% or more of code that was not correctly converted. A complete rewrite of the code could be more effective. Rewriting the code also gives the opportunity for eliminating dead code, fixing workarounds, and properly documenting the new code.

Reverse-Engineering Tools

Software tools are also available to help with documenting and reverse-engineering control system configurations. These tools extract the actual configuration resident in the control system and therefore guarantee the as-built status. This type of reverse engineering is extremely useful because it gives a complete list of all of the functions that have to be migrated. It can be used as a checklist to ensure that all functions planned for migration have indeed been implemented correctly in the new system. The new system can be reverse-engineered in the same way for a side-by-side comparison.

Migrating to New Features

Existing controls should not be copied as-is to a new system without first analyzing the new system and understanding the improvements presented by it. This is especially true with HMI migrations in which new HMI systems provide vast improvements over systems of a decade old only.

Older DCS graphic displays may not have had a built-in shape library or prebuilt faceplates. This functionality would have been provided originally by custom-building the objects, often using inefficient code by modern standards. These custom-built objects can severely hamper performance of a modern HMI if the code is simply copied into the new system. There also may

have been a lack of uniformity when different people working on the graphics created separate objects for the same function. Reusing old code will carry the same inconsistencies into the new HMI as they were present in the replaced systems. There is also likely no support for the original objects because the programmers might have retired or moved on to different jobs.

In older control systems, temperature and pressure compensation on flow measurements might have had to be programmed, whereas, in newer systems, function blocks exist for this purpose. In cases such as this, the new technology should be used in lieu of the old, complex, and inefficient methods.

If conversion tools are used for automatic conversion, these tools should automatically upgrade to the new functionality, or those parts of the conversion where engineering is required to activate the new functionality should be flagged. The need for manual intervention should be carefully analyzed during the upgrade planning phase so that time and resources can be allocated to the project for doing the redesigning or reprogramming that may be required.

DCS Life Cycle Management Strategies

Several strategies, ranging in cost and risk, are available for managing the end of a DCS's life. Although these strategies are discussed individually over the next few sections, following a combination of two or more strategies on multiple units or plants is often most effective. An organization may also initially adopt a certain strategy and change it over time when they gain more experience [8]. The choice of strategy or strategies rests on many factors, including system age, OEM support, failure rates, cost of spare parts, and cost of upgrades. In some cases, the choice is obvious, but, in many cases, it is less clear. Guidance on the selection of the most appropriate life cycle management strategy or strategies is provided in Section 5: The DCS Life Cycle Plan.

Aggressive

When following an aggressive strategy for life cycle management, a system is updated or upgraded when a new version becomes available. This strategy would be expensive and disruptive to apply to DCS and computer hardware, but it is often followed for software and operating systems as part of a configuration management strategy.

Most software vendors offer support plans under which new versions of software are made available at no additional cost. Software upgrades should be done judiciously and with due diligence. Compatibility with computer hardware, other software applications, and the control system should be checked before upgrading software.

Packaged releases of patches and security updates for Microsoft operating systems and software programs are made available monthly by Microsoft. These packages normally contain security updates and malicious software removal tools, but, at times, new versions of Internet Explorer and service packs for the operating system and other installed software are included, too. NERC CIP standards require the installation of security patches in a timely fashion. However, updates should not be installed automatically. Information Technology (IT) personnel and control system administrators obtain clearance from the control system OEM before installing software updates.

OEM-Directed

The OEM-directed life cycle management strategy relies on OEM recommendations to guide frequency and scope of upgrades. This strategy eliminates the risk of obsolescence, because control systems are upgraded before OEMs stop production of new parts or terminate support for a particular control system.

The OEMs who were interviewed for this project all said that their approach is to work with power plants and fleets to identify critical units and to propose a DCS upgrade plan that would maximize the return on investment. To construct this plan, OEM field service engineers first audit the installed control system and produce an accurate record of all of its installed components. The inventory of components is compared to the projected life cycle of each component, and a plan for upgrades before obsolescence is drafted. The plan is then adjusted according to the power company's business objectives and strategies for each unit so that units that hardly ever run and units slated for decommissioning are not upgraded.

The OEM-directed strategy would be suitable for power producers that prefer stable, long-term plans and seek to lower the risk of DCS equipment failures and obsolescence. Capital expenditure for control system upgrades can be planned out for a few years into the future, and capital can be made available annually to fund the upgrade projects.

The OEM-directed strategy would also be the preferred plan for companies that buy control system parts and support services from only the OEM or its authorized resellers. This may be to ensure that all parts are covered by a warranty and/or to ensure high quality and reliable repairs when necessary.

The OEM-directed strategy is not the most cost-effective strategy. This report will later show how difficult it is to justify DCS upgrades, based on economics alone. Rarely does an upgrade pay for itself in a reasonable time frame. If a power company focuses only on minimizing operating costs and improving its bottom line, the OEM-directed plan would not be suitable. However, if the culture of a power company is to improve plant reliability and operability and minimize the risk of failures, obsolescence, and human error, the OEM-directed strategy goes a long way to support such a culture.

The OEM's audit and upgrade plan provide a good starting point that can be modified and refined (if necessary) using a combination of the following strategies described to develop a solid DCS life cycle management plan that supports the culture and fiscal objectives of the company.

Fixed Cost

As the name indicates, the fixed-cost strategy makes available a certain amount of money for upgrading DCS technology. The fixed-cost strategy could be based on the OEM-directed upgrade plan, but a lesser amount of money is allocated, such as a certain percentage of the plan's cost (for example, 25%) or a fixed annual amount (for example, $10 million). Units are prioritized for receiving upgrades so that risk and impact of unit trips and obsolescence are minimized.

Older systems that are no longer supported by the OEM can be maintained using the strategies presented in the next section.

Cost-Justified

The cost-justified strategy aims to minimize control-system related expenditure over a finite time frame, for example, three to five years. This strategy would be preferred by plants and companies that want to minimize cost and/or require that any capital expenditure produce a return on investment in the short term (within a few years only).

Whether to upgrade or maintain the current control system is decided by analyzing the cost of each of these two options over a relatively short time period, typically three to five years, and picking the option with the lowest cost. This generally results in no upgrades being done, unless serious reliability issues drive the cost of maintaining the old system higher than the cost of an upgrade or migration.

In lieu of an upgrade, the existing control system is maintained with replacement parts or repairs provided by the OEM until the latter stops its support for the product. Then parts and repairs are obtained from third-party specialist companies or on the open market. Multinational online marketplace, eBay Inc., does an estimated $100 million annually in control system parts [3].

An upgrade is done only when replacement parts and repairs become unavailable or their failure rate and cost escalate high enough to justify the upgrade. Partial, targeted upgrades are preferred over sweeping upgrades, and control system parts freed up during an upgrade become spare parts for other systems.

Because this strategy poses the risk of running out of spare parts or developing reliability issues, it should be reevaluated periodically (one to three years) to ensure its validity as a feasible strategy. Spare parts obtained from third-party vendors and repair shops that are intended to be used as stock should be thoroughly tested before placed into stock. It should be realized that repaired parts are not new, meaning that this strategy will not keep the DCS evergreen, and failure rates are bound to increase, eventually.

A special concern arises with Windows-based programming tools. Personal computers have a much shorter life than DCSs. This may create problems long before the reliability of the DCS is of any concern. Personal computer hardware can possibly be replaced with similar hardware obtained from eBay, but the replacement hardware is just as old as the failed hardware, and its failure may be imminent. One solution could be to run DOS and old versions of Windows in virtual machines (VMs), using VMware. However, the host machine may have to be fitted with floppy disk drives for loading the software, parallel ports for attaching hardware keys, and serial ports for communicating with the control system.

Run to Fail

Finally, the DCS life cycle might be influenced by the future of the plant. If the plant is scheduled to be decommissioned, performing any type of DCS upgrade will make no sense. If a control system component fails, several options exist, as follows:

- If the failed component is on a noncritical system, it could be left in place.
- The component can be replaced by using one from a noncritical system.
- The component can be replaced by using one from the stock of spare parts.
  - Depending on stock levels and the expected life of the plant, it might not even be necessary to purchase a replacement part to keep in stock.
  - If a replacement part is required for stock, a return policy can be negotiated with the vendor that will allow returning the spare part, if unused.

Comparison of Strategies

Each of the strategies has advantages and disadvantages. Some of these pros and cons are subjective and may cause disagreement and extensive debating. A clear company policy such as insistence on using OEM-supported equipment or minimizing short-term expenditure will go a long way in helping the decision on the appropriate strategy. The pros and cons of the five strategies are presented in Table 2-1.

Table 2-1
Cost and risk of DCS life cycle strategies

Strategy	Pros	Cons
Aggressive	• Longevity • Periodic gains from new technology • Perpetual OEM support • Relatively constant operation and maintenance cost • Retirement of experienced workforce not a problem • Migrations usually offered	• Highest cost of ownership • System validation required more frequently • Plant as possible test site for new technology • Training required almost continuously
OEM driven	• Lower total cost of ownership than aggressive strategy • Long-term planning possible • Periodic gains from new technology • Perpetual OEM support • Retirement of experienced workforce not a problem • Migrations usually offered	• High engineering cost if migration not possible • Capital expenditure possibly required • Frequent training required

Table 2-1 (continued)
Cost and risk of DCS life cycle strategies

Strategy	Pros	Cons
Fixed cost	• Lower total cost of ownership than OEM-driven strategy • Owner's decision how much to spend	• High engineering cost if migration not possible • May lose OEM support on some systems
Cost justified	• Substantially lower cost than options listed previously • Minimal capital expenditure required, and infrequently • Minimum training required • Minimum re-engineering required	• Multiple systems to support • No OEM support for old system • Retiring of experienced workforce issue on old system • Cost of parts to possibly increase with time • Infrequent gains from new technology • Risk of no parts available
Run to fail	• Capital expenditure not required • Lowest total cost of ownership • Training not required • Engineering not required	• No OEM support • System possibly failing prematurely • Risk of no parts available • No gains from new technology • Retiring of experienced workforce

Strategies for Extending HMI and Workstation Life Cycles

In contrast to DCS hardware with an average life span of 20 years, computer systems used for operator interfaces, programming tools, and process data historians often have much shorter life cycles, typically lasting less than a decade. Computer hardware is much less reliable than DCS hardware, consequently requiring more frequent replacements. It is foreseeable that computer hardware could need replacements three or more times during the life span of a DCS.

When computer hardware is replaced after several years of service, the new hardware is likely not supported by the original operating system because of advances in technology and the lack of backward compatibility (new hardware ships with the latest operating system, therefore, there is no need for maintaining backward compatibility). This necessitates using a new operating system.

However, the rapid advances in operating system technology create incompatibilities with old software applications. For example, the last operating system that fully supported DOS applications was Windows 98, for which Microsoft ended its support in 2006. Windows applications that store configuration data in the Program Files folder no longer function in operating systems after Windows XP, for which Microsoft is ending support in 2014.

As a result, the HMI and engineering software may have to be upgraded to be compatible with the new operating system running on the new hardware. This upgrade may be very expensive compared to the cost of the replacement hardware forcing the upgrade. To make matters worse, the latest version of software would be designed for the latest model of DCS and may be incompatible with the old DCS. This creates a dire situation unless an alternative solution can be found.

Assuming that the computer hardware is failing, and it is premature for replacing the DCS, and upgrading the HMI and/or engineering software is not possible or is undesirable, three possible alternatives exist, as follows:

1. The failed system can be replaced with a compatible one.
2. The failed system can be repaired.
3. VMs can be used for backward compatibility.

Replacing the System

The simplest approach, in theory, is to simply replace a failed computer with an identical or equivalent computer. Replacement computers and servers can be sourced from the following various places:

- Trading/auctioning websites such as eBay
- Specialty companies that can be found through Internet searches (for example, “used computer OR server”)
- Dell’s auction website maintained for Dell computers with large numbers of certain types of older systems
- IT department’s old business computers put in storage for replacing

It is important to note that the replacement computer or server does not have to be identical to the failed one; it just needs to be able to run the same operating system and software as the failed one.

The downside of replacing failed systems with equivalent systems is that the replacement system is not new and, on average, will have a shorter remaining life than the time to failure of the system it replaces. Hard drives of all computers should be backed up regularly as a best practice and as a requirement for cyber security, and these backups may be needed more frequently as systems age.

Repairing the System

Computer systems consist of a few basic components: motherboard, memory, hard disk drive, power supply, and the external video card. If one of these components in a computer fails, only the failed component has to be replaced. The same resources listed in the previous section can be used as sources for computer spare parts. Another route may be to send the computer to a repair shop. Numerous repair shops can be found through Internet searches.

Similar to replacing entire computers with equivalent ones, when computers are repaired with used parts, their life cycle is not reset to zero, and the mean time to failure is expected to decrease as the system ages.

Using Virtualization

Virtualization separates the operating system from the hardware through the use of a VM. A VM is a software-based emulation of computer hardware that provides a complete system platform for the operating system and execution of other applications. A VM can be configured to emulate the computer architecture and functions of a real world computer where the real hardware is not available, for example, due to obsolescence. It is also possible to have multiple instances of VMs running on a single system for more efficient use of computing resources.

Virtualization provides the ability to run obsolete operating systems and software on virtual hardware that is emulated on a modern computer or server. The entire configuration of the VM resides in a file that can be moved to another computer, if needed.

Virtualization technology has two subsets: a Type 1 (or native) hypervisor runs directly on the hardware and does not require a base operating system, whereas a Type 2 (or hosted) hypervisor runs on an operating system. A hypervisor or virtual machine monitor is a piece of computer software, firmware, or hardware that creates and runs VMs.

Practically, a VM will be created and used, as follows:

1. Acquire new hardware, complete with the operating system (if a hosted hypervisor is used), keyboard, mouse, and video display.
2. Load the virtual machine monitor software onto the physical machine.
3. Configure a VM to meet the system specifications of the obsolete operating system and software.
4. Start the VM, and load the obsolete operating system and software.
5. Run the software as if it were running on a real machine.

One shortfall of virtualization is that the new physical machine might not have the correct slots for plugging in old hardware, for example, a new machine will have peripheral component interconnect (PCI) slots; whereas, an old communication card may have an industry standard architecture (ISA) connector. A PCI-to-ISA bridge could be used to facilitate the old device's connectivity. However, the device must be supported by the host system. The setup will require the use of a native hypervisor, and either the virtual machine monitor or DCS OEM must support virtualization of the physical device through an appropriate driver for the device. It is not clear on how many proprietary devices (if any) are supported in this way.

If proprietary devices are supported by the virtual machine monitor, or if the obsolete system uses a standard serial-port or Ethernet for its communications, virtualization can provide a relatively simple and practical means of running obsolete operating systems and software on modern hardware.

3
OEM VIEWS ON LIFE CYCLE MANAGEMENT

The following write-ups originate from phone interviews conducted with product and/or marketing managers at control system OEMs and supplemented with information posted on their websites.

ABB Group

In 1989, Bailey Controls merged with Italy's Elsag Group to form Elsag Bailey Process Automation. Elsag Bailey, in turn, was merged with ABB in 1998.

Bailey Controls introduced the NETWORK 90 DCS in 1980, after which the system was continuously enhanced with new features. In 1988, the enhanced system was renamed INFI 90 and then renamed INFI 90 OPEN in 1994 [9]. The control system was merged with other product lines under the family name Symphony.[1] The Bailey line of controllers and I/O was collectively referred to as Harmony.

ABB first developed a migration path from Symphony to their 800xA system and later reinvested in further developing the Symphony platform. A new version of this platform was released as Symphony Plus[2] in 2010.

Evolution Without Obsolescence

ABB established an evolution-without-obsolescence policy for the Bailey/Symphony line of products. This policy dictates that no product will be removed from active sale until a compatible, equivalent, or superior product is available. This allows incremental, planned steps for adding new technologies or upgrading technologies in existing systems while maintaining the remainder of installed assets.

The ABB system evolution consists of a four-point strategy [10], as follows:

- Each new development step is a natural progression of the current system offering. All versions and models of system components are compatible with each other, enabling new features to be seamlessly added into existing applications, with minimal impact.
- A comprehensive audit on an installed system can be done, after which areas of greatest risk and potential are identified and targeted for upgrade. Guided by the customer's business goals, a long-term upgrade plan is drawn up. The plan is periodically reviewed and updated, to incorporate changing needs and solutions.

[1] Symphony is a registered trademark of ABB.
[2] Symphony Plus is a registered trademark of ABB.

- With this proactive approach to hardware and software upgrades, the evolution process can help customers implement new technologies and avoid obsolescence with stepwise, incremental upgrades.
- Upgrade tools and other translation resources are available to migrate control blocks, code, point configurations, and graphics to the new system with minimum effort. This service is performed by ABB's trained system engineers.

New controllers can run the code from old controllers. Upgrading to a new controller simply involves importing the code into the new programming environment, called *conductor*, and then loading it into a new controller. Form-fit controllers can slide into the existing racks to replace old or failed controllers. Similarly, form-fit and backward-compatible I/O and communications modules are available to replace legacy components. DIN-rail (DIN is the German Institute for Standardization) modules are also available for new systems and/or expansions.

Translation tools are available for HMI graphics, and, from ABB's experience, roughly 95% of graphics can be converted problem-free. Symphony Plus HMI, called *operations*, can be connected to the legacy INFI 90 network, or a new communications module can be installed to improve network performance.

Legacy System Life Cycle and Support

ABB continues to support a large installed base of the NETWORK 90 and INFI 90 systems with field services, parts repair, and parts replacement. Selected components are still being manufactured as new.

Guided by the evolution policy, new Symphony Plus parts are backward-compatible, allowing failed components to be replaced with new components as part of an upgrade strategy. Form-fit replacement parts are available for controllers, I/O, and communications modules.

When a component fails, a customer has the option of replacing it with a repaired part of the same version or with a compatible equivalent of the latest version.

Migration to Symphony Plus

ABB's evolution program supports a stepwise approach in which components or process areas can be upgraded individually, as required, while leaving the rest of the system undisturbed. These upgrades can be done during normal maintenance outages, or, in some cases, with the plant on-line.

Alternatively, a more extensive upgrade can be performed in which major components such as controllers, HMI, and power supplies are replaced during a normal maintenance outage, while leaving the original I/O in place.

With these two options, ABB helps users use the DCS assets to their full life cycle potential by replacing only what is deemed necessary. It also alleviates the need for a large capital investment and major outage associated with a full-scale rip-and-replace approach. ABB's evolution approach costs 70–80% less than rip-and-replace alternatives [11].

Symphony Plus Life Cycle

In step with ABB's evolution policy, the Symphony Plus platform will not be made obsolete in a way that requires a complete system upgrade. ABB plans to continue offering new technologies in backward-compatible modules that can replace old parts with minimal impact when the need arises.

Fleet-Wide Life Cycle Management

ABB field engineers have tools to audit installed systems and compile a list of installed hardware and software to identify areas of greatest risk and potential. ABB then works with customers to draw up a long-term upgrade plan that takes into account the customer's business goals. The plan is periodically reviewed and updated to incorporate changing needs and solutions. Parts released from upgraded systems can be used as replacement parts to maintain the remaining legacy control systems.

Emerson

The Emerson Electric Company acquired Westinghouse Process Control, Inc., in 1998, a division of CBS Corporation. Previously known as *Westinghouse Process Control*, the acquired business became Emerson Process Management Power & Water Solutions, Inc.

The WDPF[3] system was a Westinghouse product released in 1982. Although it still accounts for a portion of Emerson's installed base of control systems in power and water plants in North America, the majority of the company's installed base comprises Emerson's newer Ovation[4] expert control system.

Legacy System Life Span

The usable life span of the WDPF system seems to depend mostly on environmental factors. Although exposure to excessive heat, humidity, and coal dust may affect a system's life span, some systems maintained in a climate-controlled environment have operated in excess of 30 years.

Legacy System Support

Emerson provides support for the WDPF system, including spare parts, phone support, and field service. Although a few parts are still being manufactured as new, most of the replacement parts available today are refurbished used parts. However, legacy support has become more expensive due to the availability of the older parts.

Migration to Ovation

Emerson offers a WDPF-to-Ovation Migration program as a cost-effective alternative to a complete system replacement [12]. Users are able to retain their existing WDPF cabinetry, Q-line I/O subsystem and its associated wiring, control logic, and process graphics. This saves the cost of replacement I/O hardware, field labor, and wiring checkout time; it also saves the expense and risk of redeveloping control schemes and eliminates the need for training operators on new graphics.

[3] WDPF is a trademark of Emerson Process Management.
[4] Ovation is a trademark of Emerson Process Management.

To begin the migration process, Emerson performs a hardware and software inventory of the existing WDPF system. Using this information, Emerson develops a hardware layout, software map, and migration plan to guide the process. The existing control logic, process graphics, and databases are converted off-line to their Ovation equivalent. New workstations and network devices are prepositioned at the plant and configured before cutover to the new system. Finally, during a suitable shutdown, the WDPF data processing units are replaced with Ovation controllers, completing the migration.

Emerson also offers a migration from the WDPF Q-line I/O to the new Ovation I/O. The existing edge connector and terminations are reused, which saves field labor and checkout time.

Ovation Life Cycle

By incorporating commercial, off-the-shelf technology throughout the system, Ovation provides an adaptable platform that allows a plant to continually modify and expand the system to meet new needs. In other words, the Ovation system can evolve incrementally as technology progresses or when required by plant expansions. Ovation is known to eliminate system obsolescence by allowing users to stay current with new developments in communications, processing, and advanced applications. Users would access new technologies, features, and improvements by simply replacing a module in the control system or HMI and/or upgrading their software level.

Fleet-Wide Life Cycle Management

Emerson works with owners of single units as well as large fleets to determine the best approach to managing the life cycle of the installed control systems. Peaking units running only a few hours per month or units that might be decommissioned in the foreseeable future may not be targeted for control system upgrades. Emerson would rather ensure that the owner has the spare parts needed to maintain the control system. Units with a substantial life expectancy and a legacy control system would be considered for an upgrade in order to benefit from newer technologies that can enhance security, improve efficiency, and enable or streamline compliance with new regulations.

General Electric

The General Electric Company is a provider of turbine control systems, DCS, and HMI systems. It manufactures all control system hardware, firmware, and software, except for the HMI hardware and operating system. Its latest control system is Mark[5] VIe, which was released in 2004 and became its mainstream product in 2006. General Electric differentiates between HMI and control system equipment for the purpose of life cycle planning.

HMI Life Cycle

In General Electric's viewpoint, the life cycle of HMI computer equipment and software is in the order of three to five years, but it acknowledges that customers often upgrade between five and seven years only. In some cases, users wait until they are forced to upgrade due to operating system obsolescence and/or cyber security requirements. General Electric reported that a dwindling number of customers still have systems that run on DOS and Windows NT.

[5] Mark is a trademark of the General Electric Company.

General Electric prefers to bundle the HMI and operating system software with compatible computer hardware to provide a fully tested and OEM-supported system.

General Electric has stated that it does not force users to upgrade but recommends hardware and software upgrades in the following cases:

- Before the support for hardware and/or operating system is ended by the respective OEMs, General Electric recommends upgrading the computer system to its latest supported hardware, operating system, and HMI that is compatible with the control system hardware.
- When old computer hardware is incapable of effectively running new HMI software, General Electric recommends doing a hardware upgrade if the customer wants to upgrade HMI software.
- When a customer upgrades the control system and has not upgraded the computer system within the prior two years, General Electric recommends upgrading the computer hardware, HMI software, and, if applicable, the operating system.

Legacy Control System Support

General Electric's life cycle support program provides spare parts support, field service, and upgrades to extend the life of control systems. General Electric informs customers when product enhancements are available and notifies customers of last-time-to-buy opportunities in advance of parts and services no longer being offered for sale.

General Electric typically produces complete new systems for a period of 10 years after first release. During this time, General Electric fully supports these systems with newly manufactured replacement parts and card repair services. After 10 years, General Electric does not produce full systems but still supports the existing systems with field support, newly manufactured spare parts, and card repairs for 10 more years. Twenty years after the initial release of a system, the production of new hardware is ended, but card repairs and replacements with refurbished cards as well as field services still continue. During this period, General Electric strives to support systems as much as possible, but no guarantees are made that card repairs or replacement parts will remain available.

Control System Migration

Mark IV to Mark VIe

To upgrade the Mark IV system to Mark VIe, General Electric provides prefabricated bases with Mark VIe electronics that are installed in the existing Mark IV cabinets and connected to the existing terminal boards with plug-in wire harnesses [13]. Board racks with hardwired backplanes are replaced with smart I/O modules with local distributed processors to interface with turbine devices. Field terminations are retained to lower cost and minimize installation time.

The operator interface on the cabinet door is replaced with a modern HMI in the same location. Remote operator panels and smart remotes are replaced with HMIs and historians. The Mark IV's serial communications to plant monitoring systems are replicated, but modern protocols such as OPC are also available.

Generator excitation upgrades are also available with the front-end digital, which replaces just the control portion of the exciter without affecting the power bridges.

Mark V to Mark VIe

General Electric provides a migration solution from a legacy Mark V control system to the Mark VIe through a simple exchange of the electronic modules [14]. The new Mark VIe I/O cards are ribbon-cabled out to the existing termination cards, requiring no change to wiring, panel terminations, or panel size.

Before the I/O replacement, General Electric uses automation tools to translate existing application software, while maintaining I/O scaling, alarms, and point names. On site, the I/O cards are replaced, and the new I/O is connected through an Ethernet switch to the Mark VIe CPU. The I/O replacement and installation of the Mark VIe modules can be completed in 36 to 48 hours of plant downtime.

Mark VI to Mark VIe

Normal Mark VI control system production ended in 2009. However, a full suite of spare parts is still in production to support Mark VI control systems in the field, and upgrades to Mark VIe are not yet necessary.

New System Life Cycle

General Electric's latest control platform (Mark VIe) was designed with an almost infinite life span in mind. Its architecture is based on Ethernet, which allows various control system hardware components to be upgraded independently, based on their individual life cycles. For example, a control processor may be based on microprocessor technology that becomes obsolete in 10 years. At that time, the obsolete control processor can simply be replaced with the latest one, without having to change out other hardware components. With the Ethernet-based architecture, General Electric claims that they have architecturally immunized themselves against obsolescence as well as they can.

Forced Upgrades

When questioned about upgrades during an interview, General Electric admitted that they are aware of a perception among customers that General Electric forces upgrades onto customers. General Electric stated that only in isolated cases would the company require an upgrade, and that it would normally only recommend a course of action that they believe would be beneficial to a customer, based on the current situation. There may be occasions where obsolescence dictates a certain path, but General Electric claims that it tries to accommodate customers as far as possible. Most often, a customer is given the choice to either continue operating with the installed system or upgrade it.

General Electric gave the following three examples of situations that would typically require an upgrade:

- When a legacy control system's electronic cards cannot be repaired anymore because electronic components on it are no longer in production and the customer wants to obtain support from General Electric
- When a legacy operating system must be replaced with a new one (for example, for compliance with a cyber-security policy) and the HMI software is incompatible with the new operating system
- When a legacy control system is being upgraded and the HMI software is incompatible with the new control system

Fleet-Wide Strategy

General Electric works with fleet owners to determine the version of all control hardware and software and the criticality for each unit/turbine in the fleet. General Electric then makes life cycle recommendations that cover the entire fleet. For example, turbines close to retirement are not recommended for upgrade, if possible, whereas critical units with old control systems that will likely benefit from the latest technologies may be recommended for phased upgrades over the span of a few years. Other control systems may be placed on General Electric's multiyear support plan.

Invensys

Invensys Systems, Inc., provides the Foxboro control systems and Triconex safety shutdown systems, among other products. The Foxboro line of control systems includes the analog SPEC 200, DEC-based SPECTRUM, and distributed-architecture I/A Series systems.

Legacy System Support

Invensys still manufactures and sells parts for the SPEC 200 system, mainly to the nuclear power industry. Many units of the SPECTRUM line of control systems, originally launched around 1980, are still in operation. Refurbished parts and card repairs for the SPECTRUM are provided by third-party vendors.

Invensys defines five phases in its product life cycles, each phase having a different level of support, as shown in Table 3-1. The various parts of a control system all have their own, individual life cycle phase assignment. Invensys notifies registered customers of any changes in the phase of a product through a semiannual phase change report.

Table 3-1
Product life cycle phases, as defined by Invensys [15]

Phase	Description
Preferred	Products in this phase are the most recent products available in their functional area. Products are actively being produced, promoted, enhanced, and sold. The length of time that a product remains in this phase varies. Many products move to the available phase, whereas others may move directly to the mature phase.
Available	Products in this phase are no longer the preferred product offering. Products are available for sale and are being produced but generally are no longer being enhanced. Typically, these products are sold for expansions not for new installations. This designation also serves as early notice that the product will be withdrawn from sale. The length of time a product remains in this phase varies.
Mature	Parts are still repaired and refurbished parts are available, but new parts are no longer being manufactured. The product is withdrawn from sale, and no more enhancements are provided. Before the product is withdrawn, Invensys ensures that a clearly defined support program is in place. The length of time that a product remains in this phase varies, based on product type—the more difficult it is to replace the product with a new one, the longer the duration. • I/O products are supported in the mature phase for 10 years. • Control and network communications products are supported in this phase for five years. • Workstations in this phase are supported for three years. • Software in this phase is supported for two years.
Lifetime	Products are supported on a best-efforts basis for as long as Invensys can provide quality repair or replacement. When Invensys can no longer repair or replace a given product, the product moves to the obsolete phase.
Obsolete	Parts have become obsolete and are no longer available from Invensys. Invensys strives to provide at least one year's notice before a product becomes obsolete.

I/A Series System Life Cycle

Since its release in 1989, Invensys has infused new technologies into their I/A Series DCS platform as backward compatible features, which do not require a full DCS upgrade. Marketed as continuously current, the I/A platform allows lifetime support and never forces a complete system upgrade. The I/A system is modular, which allows partial upgrades. The system can be installed in pieces, with a *piece* being defined as the amount of work required to disassemble an existing system, to do any needed wiring modifications, and to replace it with the new system, that can fit into a maintenance outage.

To help users better manage the life cycle of their installed systems, Invensys field service engineers use a software tool that interrogates the installed system and produces an inventory of all hardware with version numbers. This is mapped onto the life cycle timeline, indicating the phase that each component is in and when support for it will likely end. A report is then produced to help users plan out their system life cycle and timing of upgrades.

Migration from Legacy Systems

Invensys provides a legacy system migration approach that retains the existing field wiring, DCS cabinets, and power supplies. This significantly reduces migration costs and shortens the duration of a switchover. The scope of migrations is normally scaled to comfortably fit within the timeline of a maintenance outage so that no downtime is attributed to the migration. This is achieved through I/A Series Plugged In DCS integrators, which consist of I/A 200 Series Fieldbus Module circuitry on form-factor boards that fit into the legacy infrastructure.

Invensys provides this migration path not only for legacy Foxboro systems, but also for Emerson (Westinghouse) WDPF and (Fisher) Provox, Honeywell TDC 2000 and TDC 3000, and ABB (Bailey). This migration approach integrates the I/A Series system at the I/O level, avoiding any use of proprietary elements. As a result, gateway performance "bottlenecks" are eliminated, and multivendor software licensing is not required.

Migration from Old I/A Systems

The continuously current concept simplifies migration from the I/A 100 Series to the 200 Series.

Control schemes in the I/A Series are built by arranging precompiled control blocks. These are backward-compatible. Control processor upgrades are simplified by exporting the parameters that characterize the various blocks into a text file, which is then converted and imported into the new configuration software. Any additional features added to a block since the old version are then reviewed and configured.

The original message structure in old Fieldbus communications is still used, but this is now wrapped in a transfer control protocol over Internet protocol (TCP/IP) stream. During migration, the I/A 100 Series I/O cards are routed to a communication conversion module which then networks to the I/A 200 Series control processor using TCP/IP. Approximately 50% of the installed base still runs on the I/A 100 Series I/O with updated control processors and HMIs.

Conversion tools are used to convert old display manager graphics into the new graphics format, which further simplifies migration.

OEM/Technology Selection

Control system migrations are typically done within the same brand of control system, but complete upgrades (HMI, controllers, and I/O) provide an opportunity for changing brands to a system that more closely meets the user's needs. There is also the option of changing to an OEM that is more aligned with the power company's business objectives and/or technology requirements. Even when a control system migration is planned, it might be wise to consider alternatives as a matter of due diligence. Several OEMs and third parties provide hardware to facilitate partial upgrades and software and work processes to migrate control system and HMI configurations. Both scenarios require an evaluation of OEMs and their product offerings and then selecting the most suitable OEM or product.

The evaluation of OEMs and their offerings can be a substantial task in itself, and it is advisable to select a small number of systems (two to four) to evaluate. Possibilities include the newest iteration of the existing DCS, its closest competitor, the market leader, and systems having specific desirable features, such as built-in model-based control.

Evaluation Criteria

It is difficult for humans to do an objective comparison between different offerings because they tend to be emotionally tied to systems with which they are familiar. A more objective comparison can be obtained by using a comparison matrix with all of the requirements of interest (which could be hundreds) [16].

Technical criteria to consider may include the following:

- Specific requirements for basic control functions
- Advanced functions such as steam tables, model-based control, and efficiency calculations
- Sequential automation functions for automatic startup and shutdown of equipment
- Engineering station features for programming and faultfinding
- Controller execution rate and network speed
- System footprint and power consumption
- Number of servers required
- Software technology such as Structured Query Language Server versus Oracle
- Interfaces such as OPC and Open Database Connectivity
- HMI features and flexibility
- Call-up time for certain complex graphics
- Availability of alarm-management, asset management, and process historian
- Ability to preserve existing assets that still offer value (Be cautious of a snowball effect in which replacing one part of a system requires widespread replacement of perfectly good components.)
- Upgrade and migration complexity
- Tools for database, control strategy, and graphics conversion
- Process downtime requirements
- Ability to run new and old systems (for example, HMI) in parallel during upgrade
- New system learning curve for engineers and operators

In addition to the technical requirements, there may be nontechnical requirements and other considerations about the OEM, such as the following:

- Clear product roadmap for the next 10 years
- Systematic migration plan for the future
- Personnel competency
- Availability of local support
- Training solutions offered

- Size of installed base in power generation
- Historical profitability of company
- History of (and possible for future) acquisition and mergers
- Warranties and service contracts

These requirements and criteria can be categorized by type, and related items can be grouped together to simplify research and evaluation.

Comparison Matrix and Evaluation

The list of criteria should be placed in a spreadsheet for ease of processing. Each criterion should be assigned a weight that reflects its importance to the plant and/or perceived cost/effort during the migration. Too much resolution will make weight assignment difficult. A system with weight-values of one, two, and three, with one being the least important and three the most, is likely sufficient.

During the evaluation, each competing offering should be assigned a score for each of the criteria. A scoring system between 0 and 3 can be used: 0 for not meeting the criterion at all, 1 for meeting it poorly, 2 for average, and 3 for well. The individual scores are multiplied by the weighting factors and then summed up for each offering to obtain a total weighted score for the offering. The higher the score is, the better suited the offering would be.

A small extract from a comparison matrix with technical criteria is shown as a sample in Table 3-2.

Table 3-2
Sample comparison matrix

Criteria	Weight	Vendor A	Vendor B	Vendor C
Hardware				
Form-fit I/O or connectors	3	3	0	1
Footprint	1	2	3	2
Power consumption	1	3	2	3
Configuration Software				
IEC 61131-3 compatible	3	3	3	0
Display real-time values	3	1	3	3
Ease of point configuration	2	3	3	2
Advanced Control				
Model-predictive controller	2	0	3	0
OEM				
Installed base	3	2	3	2
Profitability	2	1	2	3
Totals				
		40	48	33

IEC = International Electrotechnical Commission

Gathering information to rank each control system can be challenging because end users often do not have detailed technical information on a variety of vendors. Corporate engineering groups, engineering firms, or independent system integrators can assimilate the information on behalf of the power company. If OEMs are asked to complete their part of the matrix, they might misinterpret a criterion or even stretch the truth. Detailed explanations or supporting information should be requested from OEMs and reviewed afterward.

Although this process is still subjective in terms of prioritization of criteria and applying rankings to offerings, it generally reduces debate, documents the decision-making process, helps a plant determine priorities, and sheds light on the relative standing of different OEMs and their product offerings.

A diverse team of qualified and experienced automation professionals, operators, and possibly process engineers should be involved in evaluating OEMs and selecting technology. It may be prudent to visit power plants where the technology is being used and obtain their inputs on the system's capabilities, upgrade effort, and ease of maintenance.

Other Factors

Although the comparison matrix provides a reasonably unbiased and thorough technical evaluation, there are other factors to consider when making a decision about the most suitable control system. These factors may outrank the technical evaluation, and a plant might have to settle for the technical second or third choice.

Product Life Cycle

Technology and product life cycles should be taken into consideration when purchasing a control system. Unless there is a specific reason to do so, it is important not to be a test site for new technology, because unforeseen problems are likely to come up and may cause schedule and cost overruns. On the other hand, it is also important not to select control systems that are anywhere near obsolescence. Obtain OEM commitment for the number of years that the control system will still be supported with technical services and parts repair or replacement.

Service Offering/Reputation

The contrast between vendors with respect to service can be stark. Because service is a critical factor in a successful migration, it could be the single most important vendor evaluation item [7]. It is very important to consult with other companies that have done similar upgrades to determine whether the OEM is likely to deliver services at the level required.

Migration Tools

Migration tools and their effectiveness play an important role in how much effort will be required for the upgrade. Manpower required for migrating control logic and custom code from one system to another can carry substantial costs and could be the deciding factor for selecting one type of DCS over another.

Company Standard

The company may have a preferred type of control system, or there may simply be more of one kind of DCS installed at its plants. If the cost and technical capabilities of a competing control system indicate only a slight advantage, it might be beneficial to stay with the company standard.

Cost

Cost can certainly trump any technical evaluation. The total cost of ownership (TCO) should be considered and not just the cost of the DCS hardware. The cost of configuration, commissioning, training, spare parts, and so forth, should be considered when determining the total cost.

4
COST-AND-BENEFIT ANALYSIS

Justifying control system upgrade projects can be challenging. Any system being replaced must provide a superior business value, which means lower life cycle cost, and increased functionality to take advantage of new opportunities or technologies. Without a way to accurately measure return on investment, it is difficult to justify investment in new control technology when compared to other types of capital projects. Capital expenditure is even more constrained under the current economic pressures, requiring an even stronger rationale for making investments.

Using only obsolescence to justify a DCS upgrade is not easy, except if company policy dictates otherwise. Obsolescence may be a viable reason for an upgrade if there is a substantial risk of control equipment failures repeatedly shutting down units or causing extended outages. However, management may not be convinced that a system is about to begin failing and adding substantial cost if it has no recorded history of incidents.

Other possible drivers for control system upgrades include limitations of the legacy system preventing the plant from taking advantage of advanced controls or the inability to cost-effectively support open networks, plant asset management applications, and production management solutions. The shortcomings in cyber security on older systems may be another critical concern. Old technology can hinder improvements in process performance and operator effectiveness. Having an old or outdated system installed can actually increase the number of preventable unit trips if operators lack the visibility into plant conditions that would otherwise help prevent abnormal situations.

A viable business case for a control system upgrade should be based on a clear, multifaceted cost justification that takes into account all of the costs over time associated with keeping the current system and compares that to the cost of and additional benefits provided by the new system over the same timeframe.

Total Cost of Ownership

The TCO considers the cost of a system over its lifetime. A TCO analysis provides the information needed to make informed decisions about available alternatives to obtain the most economic solution from inception to decommissioning. Procurement strategies focused on the lowest initial cost are more likely to lead to higher long-term costs. For example, the lower initial capital costs may come with higher engineering and maintenance costs in the long run.

The TCO of upgrading a control system consists of the following costs:

- New hardware, including I/O terminations and I/O modules, control processors, network interface modules, power supplies, cabinets and racks, network switches, routers and cabling, servers, engineering stations, HMI stations, operating panels or desks, liquid-crystal displays, and printers
- Software, including operating systems and software for engineering, HMI, alarm management, asset management, and keeping the process history
- Labor for the analysis of the existing system and the subsequent engineering, configuration, programming, and migration of control logic and operator graphics
- Labor during commissioning (Also consider product maturity; new technologies being rolled out by the OEM may cause unforeseen problems, project overruns, and startup delays.)
- Training of operations, maintenance, and engineering personnel on the new system
- Spare parts for stockholding

The TCO of both new and old control systems consists of the following costs:

- Ongoing maintenance, troubleshooting, and re-engineering
- Replacement of failed cards, upgrading of computer hardware and software
- OEM technical support programs, site services, warranties, and service contracts for hardware and software
- Startup costs and penalties resulting from unit trips directly caused by control system failures
- Loss of revenue due to control-system-related downtime

In addition to its TCO, the remaining life span (time before expected obsolescence) of a control system should also be considered. Buying old technology may have a lower initial price, but the mature system will become obsolete sooner and therefore might increase the cost of the control system over the remaining life of a power plant.

Application of the TCO to Dissimilar Options

TCO is typically used when comparing similar options, such as in the question, “Should we purchase a new DCS from Vendor A or from Vendor B?” assuming that the decision to purchase a new system has been made. TCO works well in this case because the cost of both systems is compared using the same basis—from inception to the end of their lives. Vendor A may offer a solution with a lower initial price tag, but it may be more costly to maintain. The decision is made by calculating the TCO for both scenarios.

A TCO analysis must be cautiously applied to comparing dissimilar options, such as in the question, “Should we upgrade our DCS or stay with the status quo?” The total life cycle cost of the legacy system cannot be included in the analysis, because most of it may be sunk costs that took place in the past. Only future costs projected over the same time period for both systems can be used in the TCO analysis. In the analysis, there should be some allowance given for tax advantages gained from the depreciation in value of a new system.

TCO Analysis Timeframe

TCO is frequently used by OEMs and systems integrators [17] to help justify control system upgrades. It encourages plant owners to set aside their short-term obsession with the prohibitively high replacement cost of a DCS in lieu of a long-term view that totals up all of the costs associated with a DCS over the lifetime of the system, typically 20 years [18], and compares that with the cost of maintaining the existing system.

However, including long-term future costs may be frowned upon by management, who usually wants to see a return on investment over a much shorter time period, typically three to five years. If there is no payback over this timeframe, the capital can be spent on other projects that have a higher rate of return. Cost justifications for DCS upgrades should therefore be done over the time period that management expects to see a return on investment.

If, however, the culture of the company is deemed efficient and cost-effective over the long term to keep up with new technologies or reduce the stress on the workforce, management will probably have more lenience over the payback period. In this case, DCS upgrades would be much easier to justify because it uses the longer timeframe to offset the large initial layout of capital.

Net Present Value and Internal Rate of Return

From an accounting perspective, it is incorrect to simply add up all of the costs and returns over the life span of an investment to obtain a final number. There is a large difference between spending money early or late in a timeframe. Accountants refer to this as the *time-value of money*. Net present value (NPV) and internal rate of return (IRR) are two methods developed for analyzing investments over long periods of time.

NPV calculations take into account that money can be invested to grow over time. One hundred dollars invested at a compounded interest rate of 5% per year will grow to $168 over 10 years. By working backward, $168 withdrawn in 2023 then would have an NPV of $100 in 2013. Future costs and benefits are lower in current NPV. When analyzing investments and returns over a period of time, NPV should be used instead of the simple arithmetic sum of the values. The Excel function *NPV(rate, values)* can be used for calculating NPV.

The IRR represents the effective growth rate of an investment to support a number of withdrawals over a period of time. If $100 is invested on January 1 and $20 is withdrawn on December 31 of each year for 10 years, the growth rate of the investment must be 15% to support the withdrawals. In other words, the IRR is 15%. In terms of a control system upgrade, the cost of the project is the investment (negative number), and the benefits each year are the withdrawals (positive numbers). The Excel function *IRR(values)* can be used for calculating IRR.

Example Calculation

The example provided considers the cost of two scenarios over several timeframes. Scenario 1 is a legacy DCS that results in a cost of $100,000 per year in maintenance, unit trips, and so forth. This cost escalates by $2500 each successive year. In Scenario 2, the same DCS is upgraded in the first year at a cost of $1,500,000 after which the running cost of the control system drops to a mere $10,000 per year. The upgrade occurs during the first year so that only half of the savings ($90,000/2=$45,000) is realized in this year. Ninety percent of the cost of the DCS is depreciated

over five years, earning an estimated 40% reduction in taxes ($1,500,000/5*0.4*0.9 = $108,000 per year). Because the DCS goes into service in the middle of the first year, only half of the tax break can be taken in this year (that is, $54,000) and the remainder in the sixth year. The maintenance cost in Scenario 2 remains constant for the first 10 years and then escalates by $2000 per year. The costs associated with the two scenarios are shown in Table 4-1.

Table 4-1
NPV over time of maintaining versus upgrading a control system

End of Year	Maintain	Upgrade
Start		$ (1,500,000)
1	$ (100,000)	$ (1,000)
2	$ (102,500)	$ 98,000
3	$ (105,000)	$ 98,000
4	$ (107,500)	$ 98,000
5	$ (110,000)	$ 98,000
6	$ (112,500)	$ 44,000
7	$ (115,000)	$ (10,000)
8	$ (117,500)	$ (10,000)
9	$ (120,000)	$ (10,000)
10	$ (122,500)	$ (10,000)
11	$ (125,000)	$ (12,000)
12	$ (127,500)	$ (14,000)
13	$ (130,000)	$ (16,000)
14	$ (132,500)	$ (18,000)
15	$ (135,000)	$ (20,000)
16	$ (137,500)	$ (22,000)
17	$ (140,000)	$ (24,000)
18	$ (142,500)	$ (26,000)
19	$ (145,000)	$ (28,000)
20	$ (147,500)	$ (30,000)

	NPV		Difference
5 yr	$ (453,540)	$ (1,114,283)	$ 660,743
10 yr	$ (851,304)	$ (1,108,213)	$ 256,910
15 yr	$ (1,196,186)	$ (1,148,221)	$ (47,964)
20 yr	$ (1,492,442)	$ (1,199,403)	$ (293,039)

When the NPV of the two scenarios is compared over various timeframes, it is evident that maintaining the legacy DCS is the best course of action for minimizing cost over 5 and 10 years. Even at 15 years, upgrading the system shows only a marginal benefit. Because the current economic philosophy leans toward short-term benefits, it is unlikely that the control system upgrade project will be approved, unless other substantial benefits can be included in the cost justification.

If the IRR of the upgrade over maintaining the existing DCS is considered (Table 4-2), a similar picture develops, except now the result is expressed in terms of the growth rate of the initial investment. The IRR over 5 and 10 years shows no growth, and at 15 years it shows a slight growth (but still not a very good investment). Only the 20-year analysis shows reasonable growth. The perceived profitability of an upgrade strongly depends on the timeframe that management considers for the return on investment.

Table 4-2
IRR of a control system upgrade over maintaining the current system

End of Year	Maintain	Upgrade	Difference
Start		$ (1,500,000)	$ (1,500,000)
1	$ (100,000)	$ (1,000)	$ 99,000
2	$ (102,500)	$ 98,000	$ 200,500
3	$ (105,000)	$ 98,000	$ 203,000
4	$ (107,500)	$ 98,000	$ 205,500
5	$ (110,000)	$ 98,000	$ 208,000
6	$ (112,500)	$ 44,000	$ 156,500
7	$ (115,000)	$ (10,000)	$ 105,000
8	$ (117,500)	$ (10,000)	$ 107,500
9	$ (120,000)	$ (10,000)	$ 110,000
10	$ (122,500)	$ (10,000)	$ 112,500
11	$ (125,000)	$ (12,000)	$ 113,000
12	$ (127,500)	$ (14,000)	$ 113,500
13	$ (130,000)	$ (16,000)	$ 114,000
14	$ (132,500)	$ (18,000)	$ 114,500
15	$ (135,000)	$ (20,000)	$ 115,000
16	$ (137,500)	$ (22,000)	$ 115,500
17	$ (140,000)	$ (24,000)	$ 116,000
18	$ (142,500)	$ (26,000)	$ 116,500
19	$ (145,000)	$ (28,000)	$ 117,000
20	$ (147,500)	$ (30,000)	$ 117,500

IRR of Upgrade over Maintain	
5 yr	–14%
10 yr	0%
15 yr	5%
20 yr	7%

Determining the Cost

To do a cost comparison between upgrading a control system and maintaining the existing one, three sets of information are needed, as follows:

- Operation and maintenance (O&M) costs associated with the old system (no upgrade) over the timeframe of interest
- Cost of unit trips and downtime caused directly by the old control system, if applicable
- Cost of the control-system upgrade
- O&M costs associated with the new system over the timeframe of interest

O&M Cost of a Control System

For cost comparison purposes, the O&M cost must be considered for both the old and new control systems. This cost needs to be determined independently for the new and old systems by calculating or estimating the following costs for each year over the period of the analysis:

- **Ongoing maintenance, troubleshooting, and re-engineering**. This is the annual labor and engineering cost of plant personnel or contractors for keeping the system running. The costs can be obtained from the plant's financial department. A careful allocation of the percentage of time actually spent on these activities versus others should be made. If no or only minor savings in labor are expected from the new system, this analysis can be skipped and a note made to this effect in the business case document.
- **Replacement of failed control system hardware**. This is the annual cost for replacing or repairing failed control-system equipment. If a high rate of failure is driving the upgrade, one would expect to see a reduction in failure rate as a result of modernizing a control system. Projecting future failure rates and replacement costs is covered in the next section.
- **Upgrading of computer hardware and software**. This cost could be higher on the new system than the old one. Modern HMIs use more computers, and the hardware does not last as long. Typical life of modern computer hardware used in industrial environments is around seven years. Software also needs to be upgraded, and the seven-year interval can be used for this, too. Cost of replacement computer hardware and software can be obtained from the OEMs.
- **OEM support programs, warranties and service contracts, including hardware, software, and site services**. If the old system is still covered by a support program, it may likely be higher than a similar coverage on the new system. These costs are normally charged annually and can be obtained from the OEM and/or third-party support provider.

Control System Reliability and Cost of Failures

Reliability of control equipment such as electronic cards, power supplies, and wiring terminations is important from two perspectives: failures can cause unit trips with costly consequences, and failures require repair or replacement of the failed equipment (which become more difficult and expensive over time).

Depending on a module's failure rate and life cycle stage, failures may pose an immediate or long-term threat to the viability of a unit. Accurate predictions of how often components will fail is essential for determining adequate levels of spare-parts and for proper maintenance and life cycle planning. For example, in the European Defense Sector, the risk of obsolescence of missile spare parts is strategically mitigated by producing and storing quantities of stock to cover 20 years of consumption, based on reliability studies [19]. Although accurately predicting the reliability of electronic components may be possible through the use of strictly enforced procedures, reliability prediction in general can be a significant challenge.

Terminology

Various terms are used to describe equipment reliability, as follows:

- **Failure rate**. The frequency of failures over a period of time. This is the inverse of the mean time between failures.
- **Mean time between failures**. The sum of the mean time to failure and the mean time to repair. However, if the mean time to repair is short compared to the mean time to failure, the mean time between failures and the mean time to failure are virtually equivalent. This is the case if the failed component is simply replaced with a working one.
- **Mean time between trips**. The equivalent of mean time between failures but for power generating units instead of electronic devices.
- **Mean time to failure**. The statistical mean value for the duration of time that an electronic device operates error-free before it fails.
- **Mean time to repair**. The statistical mean value for the duration of time that it takes to repair an electronic device.
- **Trip rate**. The number of unit trips caused over a period of time.

Reliability Prediction Methodology

Manufacturers of electronic equipment can predict the theoretic mean time to failure of the equipment by following established reliability prediction procedures. These procedures typically view electronic systems as hierarchical assemblies. Systems are constructed from modules that, in turn, are constructed from devices. The base failure rates of devices are obtained from published tables, charts, and equations. These failure rates are then multiplied by influencing factors such as manufacturing quality, operating environment (that is, temperature, humidity, dust, vibration), electronic stress level, and thermal cycles. The failure rates of all of the devices comprising a module are then statistically aggregated to obtain the predicted failure rate for the module. Failure rates of modules are similarly aggregated to obtain the predicted failure rate for the system.

Reliability Prediction Procedures and Tools

A few methods have been developed for predicting the failure rate of systems based on sophisticated reliability models. These documented methods provide procedures for predicting failure rates of electronic equipment, based on the typical failure rates of the constituent discrete components, adjusted for manufacturing quality, burn-in, electrical stress, and operating environment.

The United States Department of Defense, with the assistance of the military departments, federal agencies, and industry, has developed the Military Handbook for Reliability Prediction of Electronic Equipment [20]. This handbook has been revised several times to improve prediction methods and also to include new technologies.

Telcordia, now part of Ericsson, has developed prediction procedures for electronic equipment that they make available commercially in a document referred to as *SR-332*, *Reliability Prediction Procedure for Electronic Equipment* [21]. Telcordia also provides an Excel spreadsheet software tool that automates the reliability prediction procedures in SR-332.

The International Electrotechnical Commission (IEC) has developed a universal model for the reliability prediction of electronic components, circuit boards, and equipment [22]. The technical report, which references 32 other IEC reports and two non-IEC documents, can be used as an aid for maximizing equipment reliability by examining the effects of various influencing factors.

Item Software provides a suite of prediction and analytic modules in one integrated environment, called ITEM ToolKit [23]. This commercially available software uses globally recognized standards and methodologies (including the three mentioned previously) to analyze the reliability of components and systems.

These procedures and tools are very comprehensive and extremely detailed, requiring enormous amounts of information to be of any use. It will require a substantial amount of time from end-users to understand the tools and gather the information needed to apply them. For example, the circuit board in a power supply module might have 75 discrete components on it, consisting of a variety of resistors, capacitors, inductors, thyristors, and integrated circuits. Each component type can have individual elements with different configurations, manufacturing processes, and materials, which all play a role in their failure rate. Each component is also subjected to a certain level of electrical stress, which would be known probably to the circuit designer only. Unless all of this information is available for each component, the overall reliability cannot be predicted or will be based on best guesses.

These tools would be more valuable to manufacturers for analyzing failure rates and achieving a good balance between the life expectancy of DCS components and their cost. Weak links can easily be identified and corrected at the design stage by using a different type of component or reducing the electrical stress on it. Also, what-if scenarios can be run inexpensively without having to manufacture electronic modules.

Accuracy of Reliability Predictions

Although it is generally believed that reliability assessment methods should be used by manufacturers to aid in product design and development, the integrity and auditability of the reliability prediction methods have been found to be questionable; in that the models do not predict field failures, cannot be used for comparative purposes, and present misleading trends and relations [24].

Manufacturers could potentially use reliability prediction tools to predict the failure rate of electronic modules, but several practical aspects make accurate prediction of failure rates in the field difficult, if not impossible. The tools described in the previous section provide an initial, theoretic estimate only, which could be adjusted based on actual failure-rate data obtained from field-installed systems. However, and especially for older DCSs, many failed cards/modules are

not returned to the manufacturer but are scrapped or sent to third-party repair shops for repair or exchange. For the cards that are returned to the OEMs, the manufacturers likely know very little about the actual cause of the failure, which may have been human error such as short circuits, water ingress, and incorrect connections. (Several conversations on web-based discussion boards indicate human error as the primary cause of control system card failures.) For cards that failed of natural causes, manufacturers do not know much about the systems' operating environments, for example, temperature, humidity, dust, vibration, and cleanliness of the power supply.

These factors make it virtually impossible for OEMs to adjust the original reliability estimates obtained from the reliability-prediction tools. Also, because the original failure rate estimates were likely inaccurate [24], useful estimates of actual reliability seem unattainable to manufacturers of industrial control system equipment.

Plant/Fleet Statistics

Because accurate reliability predictions are not available from manufacturers, power companies would be well served by keeping and using their own statistics. A computerized maintenance management system should be able to provide statistical data on DCS component failures, provided that the appropriate records are kept by the maintenance technicians. In the absence of accurate maintenance records, purchasing records of control system parts can be queried to obtain counts of replacements consumed over time. The total number of installed components is also required, and an audit of all installed components may be required to obtain this information.

The accuracy of the analysis will be better with a larger installed base, so the analysis should be done fleet-wide, if the control systems are of approximately the same age and operate under roughly the same conditions. Clearly, the failure rates for different components (for example, controllers, communications modules, power supplies, and each type of I/O module) should be determined by type to obtain a type-specific failure rate. If failure rates vary greatly between different sites (for example, higher failure rates at coal-fired plants compared to gas-fired), or if the control systems are many years apart in age, site-specific failure rates should be determined.

The failure rate for each type of component can be determined by using Equation 4-1.

$$\lambda = \frac{n_{failed}}{n_{installed} \times t} \qquad \textbf{Eq. 4-1}$$

Where:

λ = failure rate in failures per hour
n_{failed} = number of component failures counted during the assessment period
$n_{installed}$ = number of components installed in the plant/fleet
t = hours spanned by the assessment

The failure rate (λ) can be converted to a measure of reliability and expressed in terms of mean time between failures, as shown in Equation 4-2.

$$MTBF = \frac{1}{\lambda} \qquad \textbf{Eq. 4-2}$$

Where:

$MTBF$ = mean time between failures in hours
λ = failure rate per hour

If a reliability assessment is done periodically (such as annually), the failure rate of critical components can be trended over time. An upswing in the trend would indicate that the type of component is nearing the end of its life (as explained in the next section). A plan should then be established to replace these components when it becomes economically justifiable.

Reliability over Time

The reliability of electronic components does not remain constant. Much has been written about the *bathtub* curve (Figure 4-1) for illustrating life cycles of various entities, from mammals to electronic equipment. These entities have relatively high mortality/failure rates early in their life cycle, followed by a period of low and almost constant failures, and, finally, an increased failure rate [25]. The failure rate of control system hardware is believed to follow the same trend.

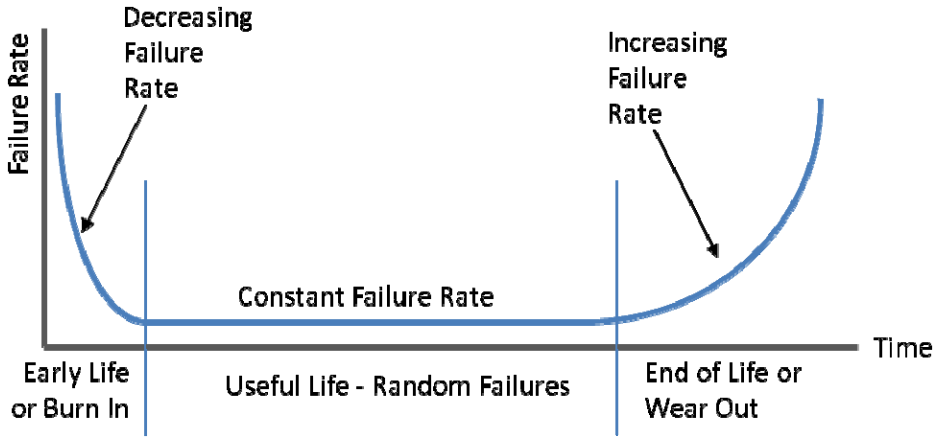


Figure 4-1
Bathtub curve depicting failure rate over time

The failure rates of control system hardware components over the life cycle of a DCS can be roughly described, as follows:

- Early in the life of electronic components, the failure rate is relatively high, typically two to three times higher than later in their life [22]. However, manufacturers of control system equipment improve component reliability by burning-in electronic equipment and testing them before shipping. Burn-in is done by running the components at elevated temperatures for a few dozen hours [25]. This causes the early-life failures to occur very rapidly, which results in fewer failures later when the control-system is in service.

- After the relatively high rate of early-life failures, components stabilize, and, with the early-life failures removed from the pool, the reliability of the remaining components is higher (that is, their failure rate is lower). Over the next 15 to 30 years, only random failures occur, and failure rates of control system hardware remain reasonably constant. The precise duration of this period is unknown for most control systems, but it would be reasonable to assume that this low failure rate will not continue indefinitely. It is, however, difficult to justify replacing control system components based on failure rates that have not yet increased.
- Eventually, the failure rate of electronic equipment increases due to wear-out [26]. The percentage of failures caused by wear-out remains low for most of a component's life, but, during the wear-out phase, it becomes the dominant cause of failure. This phase has not occurred for many DCSs, which makes it difficult to cost-justify control system replacements based on reliability improvements.

Because the failure rate of DCS hardware seems to remain low for decades, it can create a false sense of security. To proactively detect the onset of the wear-out phase, reliability assessments should be done annually and the failure rate of electronic modules (for example, controllers, I/O, communications modules, and power supplies) trended over time. An upswing in the trend would indicate that the module type is entering the wear-out phase and nearing the end of its life.

Because the period of constant (low) failure rate is many decades long for most DCS hardware, the OEM is likely not manufacturing new parts for this model of DCS by the time the wear-out phase of a component's life cycle begins. Although replacement parts may still be available for many years, these are not new parts but simply repaired versions of failed parts, which are now all in the wear-out phase of their life cycle. The rate of failure can be expected to increase exponentially over time [26].

The key point is to not assume that DCS component failure rates will remain low indefinitely. Failure-rate data from the field should be used to analyze failure rate trends and detect exponential upswings indicating the onset of the wear-out phase.

Because hardware failures can be costly because of replacement costs and, in some instances, unit trips, a high rate of failure can play an important role in cost-justifying a partial or full control system replacement. However, it will be wrong to assume that the new hardware will have no failures and that all of the failure-related costs will be saved by upgrading the system. Random failures will continue in the new system, likely at the same rate as in the replaced system before its wear-out phase.

Predicting Future Failure Rates

Cost justifications are normally done by comparing the cost of alternatives over a period of time. If the return on investment needs to be realized over five years for a project to obtain funding, this would be the period to consider for the cost comparison. It is therefore necessary to predict future costs, to which the future rate of hardware failures might add a large contribution.

The most practical and probably most accurate way to predict future failures is to look at historical trends of failure rates (per component) and extrapolate these trends into the future. If the failure rate of a control system component is relatively constant, the average failure rate over the last few years can be used as the future failure rate. If, however, the failure rate is on the

upswing, the increasing gradient of the curve needs to be extrapolated, too. This could be challenging because the historical trends may be erratic. Excel has a *trend line* feature that can be used to fit a linear or exponential curve to the data. This curve can be extended (by Excel) to obtain a forecast, as shown in Figure 4-2.

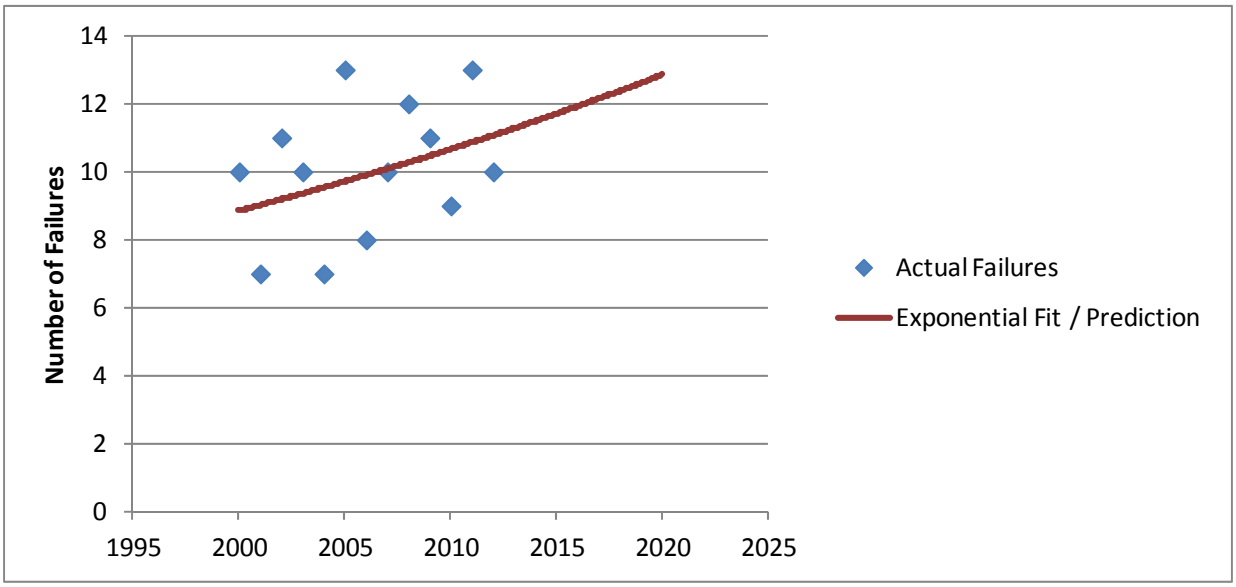


Figure 4-2
Predicting future failure rates

Projected Maintenance Cost

It is widely believed that the cost of spare parts and the frequency of failure will increase, but virtually no guidance exists for determining to what extent that these increases will take place. The assumption of escalating spare-part prices is based on having a constant demand for spare parts that is drawing on a shrinking supply. The economics become inverted when control systems are decommissioned at a higher rate than the spare parts they release are consumed. For example, INFI 90 parts can currently be obtained at substantially lower prices than the original purchase price for new parts.

Estimates of future spare-part prices should be based on market trends. Third-party vendors dealing in obsolete control system parts would be a good resource for these data. The projected price of electronic modules can then be multiplied by the projected annual failure rate to estimate the annual maintenance cost associated with replacing failed control system components.

Interviews with end users and OEMs revealed that, in general, aging control systems have not yet shown a significant increase in failure rates. However, there are cases in which the failure rate of certain components increases significantly, perhaps due to the design or manufacturing issues or environmental conditions. One power company described how it has a certain type of I/O module at one of its plants that now fails at the elevated rate of one card every one to two weeks. They were able to cost-justify replacing those modules with a different type, based on the projected cost of maintenance. However, the failure rate on the remaining DCS was low, which made it impossible for the company to justify upgrading anything else.

It is also important to realize that many control system failures are caused by external factors such as short circuits, power spikes, and human error. These failures will likely continue at the same rate with a new system. An honest cost justification will take these random failures into account and also add them to the cost of a new system.

Cost of a Unit Trip

Probability of Failures Causing Unit Trips

Some of the cost of using an old control system will lie in the number of trips that it causes over time. However, most component failures in power plant control systems are unlikely to cause unit trips. Power plant DCSs are normally designed with redundant power supplies, controllers, networks, and communications modules. I/O modules are usually not redundant, but redundant field instruments are used for critical variables. For instance, main steam pressure would be measured with three different transmitters residing on three different process taps and wired to three different input modules. The health status for each signal is read, and a median select of the healthy signals is used for the control signal. This provides a very robust and fault-tolerant signal. For breaker control, redundant trip outputs are sourced from different I/O modules.

However, not all control systems are built this way, and nonredundant components, including controllers, power supplies, and I/O modules, can cause unit shutdowns upon failure. To determine the risk of a unit trip as a result of a control system failure, an audit of all installed components should be done, and an accurate assessment should be made of which individual electronic module failures can cause unit trips.

Thermocouple input cards may process several signals used for indication purposes only. If single-channel failures occur, not all will cause a unit shutdown. Several measurements may be redundant and provide inputs to a two-out-of-three voting system. In these cases, single failures also should not cause unit trips. Many digital input cards process signals used to indicate open or closed valve positions, which also will not cause unit trips upon failure. Failure of nonredundant analog input signals used for control should cause the controller to shed to manual control (if it has been configured correctly), giving the operator the chance to manually control the unit based on other indications. Failures in the balance of plant control systems will not necessarily cause unit trips.

The probability that the failure of any module of a specific type will cause a unit trip could therefore be substantially less than 1.0, and with redundancy it is negligible. By performing an audit of installed modules and considering their failure rates and redundancy, the expected rate of unit trips caused by control system failures can be predicted.

Trip Risk Assessment

To predict the number of trips that control system failures might cause, it is necessary to know what modules are installed, how frequently they fail, and the probability that a failure will result in a unit trip. The installed count of modules and their failure rate (mean time to failure) can be obtained from annual audits.

The trip probability of a particular type of module can be determined by dividing the number of modules that will cause a trip if they fail by the total number of installed modules of that type. If single-channel failure is the main failure mode of multichannel cards, the number of channels that can cause a unit trip is divided by the total number of channels.

When this information has been obtained, the mean time between trips can be calculated, as shown in Equation 4-3.

$$MTBT = \frac{MTTF}{Installed\ Count \times Trip\ Probability} \qquad \textbf{Eq. 4-3}$$

Where:

MTBT = mean time in hours between unit trips caused by a specific control system failure

MTTF = mean time to failure of the specific control system component

Installed count = number of the specific components installed

Trip probability = probability that a single failure will cause a unit trip

The number of trips per year attributed to a particular type of control system failure can then be predicted, using Equation 4-4.

$$Trips\ per\ Year = \frac{24 \times 365}{MTBT} \qquad \textbf{Eq. 4-4}$$

This analysis should be done for each component of the control system prone to failure that can cause unit trips upon failure. The *trips per year* contributions of the component types can then be added together to obtain the statistical total number of trips per year that will be caused by control system failures (Table 4-3).

Table 4-3
Assessing the trip risk associated with control system failures

Module	Installed Count	MTTF (hr)	Trip Probability	MTBT (hr)	Trips per Year
Controller	14	500,000	0.0 (redundant)	44,643	0.00
Power supply	21	100,000	0.65	7,326	1.20
Analog output	13	200,000	0.6	25,641	0.34
Digital output 24 V	11	200,000	0.25	72,727	0.12
Digital output relay	28	150,000	0.15	35,714	0.25
Analog input	23	400,000	0.3	57,971	0.15
TC input	12	300,000	0.2	125,000	0.07

Table 4-3 (continued)
Assessing the trip risk associated with control system failures

Module	Installed Count	MTTF (hr)	Trip Probability	MTBT (hr)	Trips per Year
Digital input 24 V	21	250,000	0.1	119,048	0.07
Digital input 120 V	46	200,000	0.1	43,478	0.20
Network interface	20	900,000	0.0 (redundant)	—	0.00
Total trips per year					2.40

MTBT, mean time between trips; MTTF, mean time to failure.

This analysis could be useful for more than determining the total number of trips; it may also reveal that one particular type of control system component will likely cause a disproportionally high number of unit trips, compared to others. For example, Table 4-3 shows that power supply failures alone will cause almost half of all control-system related unit trips. If redundant power supplies can be installed, this alone may buy a few years before the entire control system has to be replaced. Cost savings in doing targeted replacements or upgrades could have a substantial benefit-to-cost ratio.

Total Cost of a Unit Trip and Downtime

When the number is known of unit trips that a control system is likely to cause, the financial impact of those trips should be calculated to help build the case for replacing or upgrading the DCS. As can be imagined, significant costs are incurred during the startup of a unit after it has tripped. However, many of these costs are often overlooked, resulting in a much lower estimate for the cost of a cycle in unit operation [27]. The cost of a unit trip and consequent startup includes the following:

- Downtime (loss of profit)
- Startup fuel
- Auxiliary power usage
- Environmental penalties and/or taxes on CO_2 and other emissions while consuming fuel but not producing power
- Heat rate losses during operation at loads lower than full load
- Additional chemicals consumed for water and flue gas conditioning
- Overtime payment for additional staff required during startup
- Long-term loss of boiler/heat recovery steam generator component life
- Increased equipment maintenance costs due to cycling
- Increased forced outage costs due to cycling
- Penalties imposed on the failure to generate contracted load
- Incremental cost of replacement power

Cost of Downtime

In a competitive power market, the downtime after a unit trip causes a loss of revenue, but some of the loss is offset by savings in fuel. The 2012 average wholesale price of electricity varied between $22/MWh and $47/MWh, depending on the trading point [28], with a mean value of $35/MWh. The cost of coal was around $20/MWh based on 2011 prices [29]. (Interestingly, the cost of fuel for a gas-fired, combined cycle plant was around $40/MWh in 2011.)

Based on these numbers, a 500-MW unit will lose 500 × $(35–20) = $7500 of operating margin per hour of forced outage. Assuming that a control system failure can be repaired and the unit restarted in about four hours, the total loss of operating margin would be $30,000 per trip.

Cost of Startup and Cycle

The subsequent startup will consume fuel, and the entire cycle will reduce the unit's life and raise the O&M costs. Intertek APTECH has done cost-of-cycling studies on hundreds of units and quantified (in 2011 U.S. dollars) the increase in capital and O&M costs (including fuel costs) of power plants due to increased cycling [27]. The median cycling costs for different unit types in North America are summarized in Table 4-4.

Table 4-4
Median hot- and warm-start costs of various types of units [27]

Unit Type	Cost of a Cycle in US$/MW Capacity	
	Hot Start	Warm Start
Small coal-fired subcritical steam (35−299 MW)	94	157
Large coal-fired subcritical steam (300−900 MW)	59	65
Large coal-fired supercritical steam (500−1300 MW)	54	64
Gas-fired combined cycle (CT-ST and HRSG)	35	55
Gas-fired simple cycle large frame CT (General Electric 7/9, N11, V94.3A, 501, and similar models)	32	126
Gas-fired simple cycle aero-derivative CT (LM 6000, 5000, 2500, and similar models)	19	24
Gas-fired steam (50−700 MW)	36	58

CT, combustion turbine; HRSG, heat recovery steam generator; ST, steam turbine.

From Table 4-4, the startup cost of a hot start after a trip of a 500-MW subcritical unit, would have a median cost of $59/MW × 500 MW = $29,500, or roughly $30,000.

Then, by adding the loss of revenue and the startup cost, the total cost of a trip on a 500-MW unit is approximately $60,000.

Justifying Upgrades Based on Unit Trips

Interviews with power companies revealed that justification of upgrades based on control-system-caused unit trips is difficult, unless the hardware failure rates are extremely high, which typically they are not.

Considering that a DCS replacement could cost in the order of six million dollars (using the average of estimates provided by an OEM [11] and one of the power companies that contributed to this research), more than 15 trips must be prevented per year to show a 5% return over the first five years, assuming the same savings in maintenance and tax breaks described earlier.

The burden of cost justification becomes lighter if a DCS migration costing $1,500,000 is done instead of a full upgrade. In this case, it would require the elimination of four control-system-related trips per year to show a 5% return over the first five years, again assuming the same two scenarios described earlier.

Although the cost of unit trips is substantial, justifying the cost of a control system migration based on reducing unit trips alone would require the elimination of several unit trips per year. Also, justifying the cost of a control system replacement could require the elimination of two unit trips per month. If control-system-related unit trips are rare, plant management would likely rather invest capital in other areas.

Cost of an Upgrade

The first step in determining the cost of an upgrade would be to decide on the scope of the upgrade. This requires careful analysis of the installed control system and the upgrade options available for it (for example, replacing the HMI only, replacing HMI and controllers, and replacing everything except the wiring terminals). The OEM can provide ball-park cost estimates for each type of upgrade. The cost estimate for a control system upgrade should include the following costs:

- New hardware, including I/O terminations and I/O modules, control processors, power supplies, cabinets and racks, network switches, routers and cabling, servers, engineering stations, HMI stations, operating panels or desks, liquid crystal displays, and printers
- Software, including operating systems and software for engineering, HMI, alarm management, asset management, and keeping process history
- Labor for the analysis of the existing system and the subsequent engineering, reprogramming, and/or migration of control logic and operator graphics
- Labor during commissioning (Also consider product maturity; new technologies being rolled out by the OEM may cause unforeseen problems, project overruns, and startup delays.)
- Training of operations, maintenance, and engineering personnel on the new system
- Spare parts for stockholding

Benefits of an Upgrade

A strong business case for a control system upgrade would likely have to include more than just a comparison of the costs of the old system versus the new one. Benefits derived from new features may carry significant weight in some cases. The following sections illustrate several benefits derived from upgrading a control system that could strengthen a business case.

Benefit of Reduced Costs

Several benefits arise from a new system reducing the O&M costs over those of the old system. These include reduced maintenance and labor costs and improved reliability. Although cost savings technically are benefits, these have already been covered previously under the discussion about the cost of ownership.

Release of Spare Parts

When the control system of one unit is upgraded, the parts coming from the now upgraded DCS can be used for maintaining legacy control systems on other units. This will result in cost savings because fewer parts will need to be purchased or repaired. However, credit cannot be taken for all of the spare parts at once. Credit can be taken for only the parts that will actually be consumed. The value of releasing parts from the upgraded DCS to other units can be no higher than the fair market value of these spare parts that would be consumed or repairs that would be needed over the period of the analysis, based on the projected failure rate.

For example, if 21 analog input cards with a market value of $2500 per card become available, and these cards are projected to be consumed at a rate of three cards per year on other units, the benefit is $7500 per year over seven years. But if failed analog input cards can be repaired for $950 per card, the benefit is only $2850 per year for seven years. Note that there are also tax ramifications for carrying large amounts of inventory.

This analysis needs to be done for each type of regularly consumed electronic module that is released by the upgrade.

Improved Thermal Performance

Some of the OEMs interviewed for this project claimed that they now have control algorithms that can help improve the performance of units and/or decrease the heat rate. If improved heat rate is one of the expected outcomes of the upgrade, the resultant fuel cost savings should be added to the dollar value of expected benefits. The OEM should be able to estimate the improvement based on its experience with similar units. This is an area that needs to carefully scrutinized because a minute claim of improvement in heat rate could alter the return on investment by many years.

Environmental Compliance

Some OEMs also claimed that they have advanced combustion control algorithms that could improve emissions. This can reduce penalties on the target unit, or the improvement can offset emissions on another unit in a fleet with the same reduction in penalties. If reduced emissions are one of the expected outcomes of an upgrade project, these potential cost savings should be added to the dollar value of expected benefits. The OEM should be able to estimate the improvement, based on its experience with similar units.

Reduced Operator Error

HMIs have seen vast technological improvement over the past two to three decades. New HMIs improve an operator's situational awareness of the plant, has improved navigation, can support automatic procedures, and also provide online documentation. It is hard to quantify the dollar value of these improvements, but if operator error is a significant cause of plant trips, trip reports can be reviewed, and a reduction in unit trips based on HMI improvements can be estimated. If this benefit will play a large role in the overall cost justification, this analysis should be done very comprehensively so that it can stand up to questioning.

Improved Monitoring and Diagnostics

Similar to HMI technology discussed previously, equipment monitoring technology has made great strides over the last few decades. If the control system upgrade is required to enable the use of some of these technologies or to bring the information and early warnings that it provides to the control room, this would have a certain benefit to the long-term health of the unit. For example, control valve health monitoring software can flag control valve or damper problems before they cause damage to the unit. Records of past problems can be reviewed to estimate the possible benefits of these features.

OEM Versus User Perspective

During interviews with OEMs, they were asked the reasons that power plants would upgrade their control systems if support and parts were available from third-party vendors. Their replies were centered on benefits that can be obtained from new control systems because of new features that they have. These included advanced combustion control, environmental controls, automation, and data communications. However, when power plants were asked whether they could cost-justify upgrades with the additional features in new systems, they said the added value was simply not high enough.

Cost-Benefit Analysis

When the projected O&M costs of the old and new systems, trip costs of the old system, and cost of the upgrade to the new system are known over a time period of interest (management-specified maximum payback period), the final cost-benefit analysis can be done. One way would be to simply subtract the benefits of the new system from its costs and run the two-column (maintain versus upgrade) analysis similar to what was shown before.

For more clarity in the business cases, an additional column with the expected annual benefits can be added. An IRR should then be run on cost of the upgrade and new system (negative numbers) plus the value of the benefits (positive numbers) minus the cost of the old system (negative numbers), as shown in Table 4-5.

Compared to Table 4-2, the following table shows that after benefits were included in the IRR calculation, the upgrade project showed a reasonable return in 10 years, as opposed to 20 years without it.

Table 4-5
IRR of upgrading the DCS and reaping benefits versus maintaining the old system

End of Year	Maintain (M)	Upgrade (U)	Benefits (B) of Upgrade	U+B−M
Start		$ (1,500,000)		$ (1,500,000)
1	$ (100,000)	$ (1,000)	$ 25,000	$ 124,000
2	$ (102,500)	$ 98,000	$ 50,000	$ 250,500
3	$ (105,000)	$ 98,000	$ 50,000	$ 253,000
4	$ (107,500)	$ 98,000	$ 50,000	$ 255,500
5	$ (110,000)	$ 98,000	$ 50,000	$ 258,000
6	$ (112,500)	$ 44,000	$ 50,000	$ 206,500
7	$ (115,000)	$ (10,000)	$ 50,000	$ 155,000
8	$ (117,500)	$ (10,000)	$ 50,000	$ 157,500
9	$ (120,000)	$ (10,000)	$ 50,000	$ 160,000
10	$ (122,500)	$ (10,000)	$ 50,000	$ 162,500

IRR	
5 yr	−8%
10 yr	6%

5
THE DCS LIFE CYCLE PLAN

The control system life cycle management plan provides structure to an otherwise *ad hoc* process of managing control system obsolescence and upgrades. The plan, in essence, specifies what should be done with an aging control system and when it should be done. The plan is influenced by the company culture, age and business objectives of the DCS, availability of support and spare parts, and the upgrade options available for the control system. It is prudent to consider all of the units in a plant or fleet in the plan, because the direction taken with one unit's control system may influence the fate of another (for example, spare parts freed up from upgrading one control system may be used to extend the life of several others). Timing is also very important with a large fleet because DCSs are not generally considered major component equipment, and an unplanned requirement of DCS replacement across a fleet could amount to hundreds of millions of capital in a short period of time.

Components of the Plan

The DCS life cycle plan should consist of the following:

- Life cycle management objectives of the company
- List of all units and their operating/business objectives
- Audit of all installed control systems and their components
- A map of when OEM support for each component will end
- The strategy of what will be done after OEM support has ended
- A project plan indicating when certain systems will be upgraded
- A reallocation strategy for parts released from upgraded systems
- The business case for control system upgrades

Life Cycle Management Objectives

Because cost justification is likely to be difficult, the overarching direction for the DCS life cycle plan would be guided by management's attitude toward minimizing costs in the short-term and running plants without warranties and OEM support.

A TCO analysis may show that upgrading a DCS produces a substantial return on investment over 20 years, but, if the window is shortened to 5 years, the same upgrade may likely show a loss. If management approves only projects with payback periods of less than 5 years, this upgrade may not be justifiable. However, if management believes in, or can be convinced of, the value of OEM support for control systems and the perils of obsolescence, upgrade projects may be approved on this basis alone.

The objectives of the life cycle management program should be defined up front and approved by management before spending too much time on defining details of the strategy. Examples of these objectives could be any or several of the following:

- To ensure reliable control system operation covered by OEM warranties and support plans.
- To minimize cost while ensuring adequate spare parts for continued reliable operation.
- To capitalize on new opportunities as quickly as they can be supported by control system technology. These include reducing equipment failures through improved monitoring, reducing operator error, and improving heat rate on all units of 500 MW and above.
- To ensure long-term cost minimization over the next 20 years.
- To balance the cost of upgrades with the risk of obsolescence, taking into account all units in the fleet.

Business Objectives for the Unit

In addition to the overall objectives for control system life cycle management, control system life cycle plans are affected by the life span and business objectives for each unit. There is likely no business case for upgrading control systems in units slated for shutdown or peaking units running only a few hours per year. New control systems will have usable life cycles of 15 to 25 years, and, if the remaining life of the unit itself is much shorter than this, justification of an upgrade becomes more difficult.

Also, a unit might have been designed for base loading, but, because of shifts in the makeup of generators on the grid, it may now be better to run it in load-following mode or even a twice-a-day peak-load cycler. The unit may now require a control system with advanced control and automation features.

The business objectives for each unit should be determined and clearly defined in the control system life cycle plan. This includes the expected life of the unit and the anticipated mode of operation. Units can also be assigned a rank, indicating its value or contribution to the business of the power company.

Control System Audit

To help define an accurate and optimal life cycle plan for control systems, it is necessary to understand what is installed and when it will become obsolete. This begins with an audit of the installed control systems at each unit as well as the spare parts in stock. The audit should include at least the following:

- Plant name and unit number, or spare parts store location
- Functional group of components (I/O, controller, communications, HMI)
- Manufacturer
- Model number
- Quantity installed

Some OEMs have tools that interrogate the control system across the network and produce an inventory of everything that is installed. Most control system vendors offer auditing services that may use a tool or do it manually. For the spare parts inventory, a listing can be obtained from the inventory/maintenance management software.

OEM Support and Obsolescence

As soon as an inventory of all control system components is available, the product life cycle for each component should be assessed. Many OEMs have different product life cycles for different components of a control system. The generic example is the difference in life cycle length of control system hardware compared to HMIs. Some vendors have separate life cycles mapped for each card or device in the control system.

Control system vendors should be able to provide power producers with a timetable of when product production will be stopped and when support will be ended. This is best indicated on a map of all products' life cycle timelines.

There are numerous third-party companies repairing and replacing parts no longer supported by the OEMs. (Several third-party companies even repair and replace parts that are still in production.) There will certainly continue to be third-party support for components losing OEM support in the future. Depending on the power company's view on using third-party components and support, these may provide a viable alternative after an OEM has dropped support for a product. If so, third-party support should be added to the life cycle map, and the product life cycle should be extended based on the third-party vendor's estimate for how long a product will be supported by it (Figure 5-1).

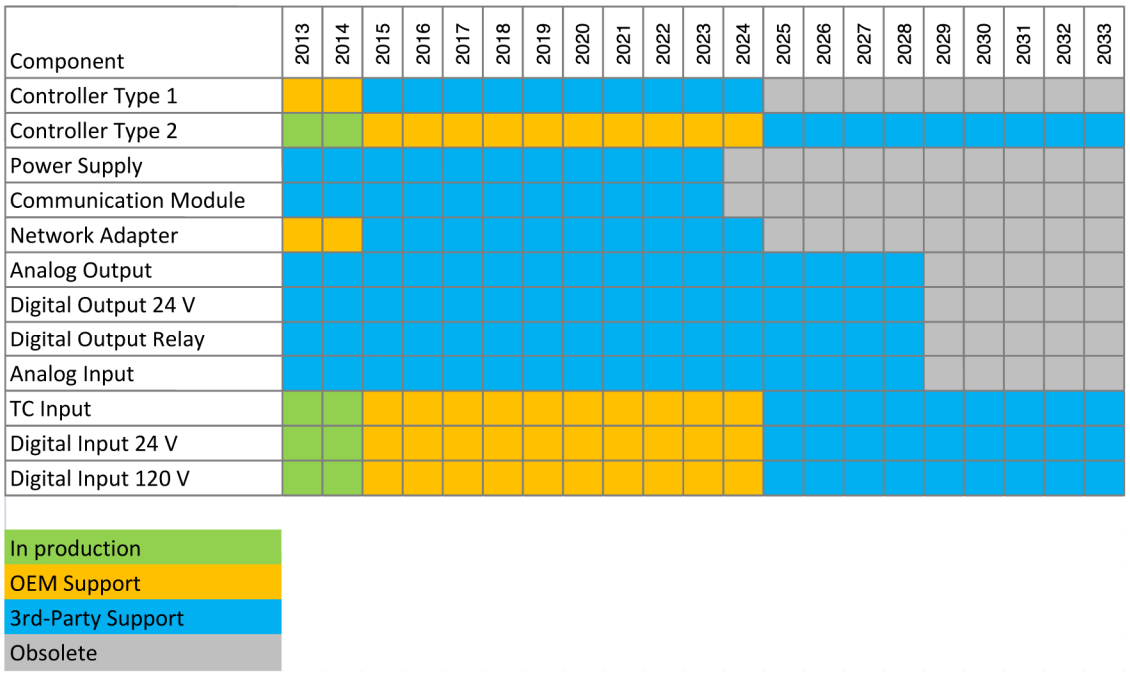


Figure 5-1
Example of a component life cycle map indicating support available and obsolescence

Choosing the Optimal Strategy

Several strategies for upgrading control systems and managing life cycles were described earlier. These included several types of upgrades and several life cycle management strategies. The choice of life cycle management strategy may likely be different for different units, depending on each unit's business objectives. When the control systems on high-ranking units are upgraded, the parts that become available can be used to support lower-ranking units.

If the OEM-directed strategy is used, the OEMs all offer life cycle planning services. Their approach is to work with power plants and fleets to identify critical units and propose a DCS upgrade plan that would maximize the return on investment and minimize reliability and obsolescence issues.

Some units could rank high in business importance and have control systems that are obsolete or that are about to become obsolete. If the company culture is to not run high-ranking units with unsupported equipment, these units will have to be upgraded before their control systems become obsolete. The upgrades may be full or partial, depending on the scope of obsolescence. Control system upgrades can be scheduled in the order of the unit's importance in the business of the company. High-ranking units with significant reliability problems can be moved up in the schedule to address those problems first. If the company allocates a certain amount of money to upgrades, the schedule can be constructed to fit within the budget.

If the company culture is to minimize cost, third-party support becomes a viable option. Some units may have to be upgraded because of severe reliability issues, but these may be certain parts only, such as power supplies or digital output cards. The remainder of the control systems will go onto third-party support, until parts are no longer available or become so expensive that upgrades can be cost justified. In either case, top-ranking units should be upgraded first, and the parts that become available can be used to support lower-ranking units.

For units slated for decommissioning, the best strategy might be to do no upgrades. It should be ensured that these units have enough spare parts.

Project Plan

As soon as upgrade and/or maintenance strategies have been developed for each unit, a project plan can be drawn up showing where each upgrade will be taking place. If possible, the upgrades should be coordinated with planned outages of suitable lengths. The annual budget and resource requirements should be listed in the project plan document. Project managers should be assigned, and the OEM(s) should be brought into the loop so that they can also begin their own planning for the upgrades.

Parts Relocation Strategy

A relocation strategy should be developed for parts released from upgraded units. The inventory of spare parts for upgraded units should also be reviewed, and parts no longer used should be placed in the pool of available parts. Depending on the power company's strategy on spare parts management, these may be taken to a central warehouse or they could be assigned to other units in the order of unit rank.

Business Case

Before management would make funds available for control system upgrades, a business case needs to be developed. That document should include the previously approved life cycle management objectives and a summary of the unit objectives and rankings, audit results, and product life cycle map. Cost justifications should be included, and all assumptions should be stated and motivated. Finally, the project plan with annual budget and resource requirements should also be included.

6
NERC CIP COMPLIANCE WITH LEGACY CONTROL SYSTEMS

Control System Cyber Security

Cyber security is at the forefront of every IT manager's concerns, but maintaining the security on process control networks has its own unique challenges, as follows:

- On business networks, the security of data always comes first (above integrity and availability), but, on control networks, integrity and availability have traditionally outranked security.
- Because of the relatively small number of installations of industrial software (compared to, for example, Internet Explorer), it typically contains many undetected vulnerabilities [30]. Even if vulnerabilities are discovered and patches are made available, most plants are unable to apply them in a timely manner because of safety and reliability testing requirements.
- The vulnerability of older process control-related systems is also compounded by the use of plain-text communications protocols now running over serial-to-Ethernet adapters. An attacker with access to a process control network can simply send plain-text commands to any such device on the network, and the device will carry out the commands.
- Old computer systems, used as HMIs or for system maintenance, may run old operating systems no longer supported by Microsoft and antivirus vendors, so the systems are not kept resistant to new threats. The old software is required for compatibility with old process control equipment and cannot simply be upgraded to solve the problem.

The Cyber-Threat Spectrum

To better understand the methods used to protect computer equipment used for process control, it is advisable to first understand the types of cyber threats and their distribution methods.

Organized Crime

Professional virus and malware authors produce products that steal credit card or banking information and/or harness compromised machines to send spam or carry out denial-of-service attacks. The products spread automatically to as many machines as possible. Usually, antivirus software producers soon identify these products and produce and distribute protections for them to their subscribers. This is predominantly a threat for machines with access to the Internet, but, without proper security measures in place, infections can spread very quickly throughout all computer systems at a plant or in an organization. When this has happened, infections can be difficult to remove.

Insiders

Disgruntled employees or contractors with sufficient access privileges to the control system network can easily interfere with control system software and communications. With sufficient change-tracking and auditing, it is difficult for individuals to cause damage without being detected and prosecuted. However, as demonstrated by the shooting attack at the Fort Hood military base on November 5, 2009, detection and prosecution is not a deterrent for members of a terrorist group.

Targeted Attacks

Whether the objective is espionage (theft of information) or sabotage, targeted attacks are probably the most serious and difficult-to-detect cyber threat. Mostly done by organizations with tremendous resources, these attacks target a specific company or industry and have a very specific objective. Such attacks have repeatedly demonstrated the ability to bypass conventional IT defenses. Prime examples include China gaining U.S. weapons secrets form secured computer systems [31], the destruction of thousands of Iranian uranium gas centrifuges with the Stuxnet virus [32], and the Shamoon attack that erased tens of thousands of hard drives in Middle-Eastern petrochemical firms [33]. The preferred method of attack is low-volume malware, operated by interactive, manual remote control [30].

Distribution Mechanisms

Malicious software normally infects a system in one of three ways [34], as follows:

- Using file transfer mechanisms such as file shares and file transfer protocol (FTP)
- Exploiting vulnerabilities in network-facing software and operating systems that allow code to be injected into the system
- The automatic copying of files from portable media such as universal serial bus (USB) sticks, compact disks, digital video disks, and cell phones to the system

Importance of Cyber Security in the Power Industry

Although a successful cyber attack against an industrial plant could result in grave losses, the damage will normally be contained at the plant site, with little or no consequence to the general population. However, a large-scale cyber attack launched successfully against several power plants may destabilize the power grid to such an extent that a widespread blackout may occur.

It is understandable that the NERC takes cyber security very seriously, recommending and enforcing compliance to CIP standards. The remainder of this section provides a high-level overview of the cyber security requirements stated in the NERC CIP Version 4 and 5 and elaborates on meeting these requirements with legacy control systems and HMIs.

The reader should note that this section is not a comprehensive coverage of NERC CIP or cyber security in general and is advised to consult other sources for a broader understanding of these topics. This section explores the NERC CIP standards with the objective of determining whether there are any requirements that cannot be met with legacy control systems or their associated computer equipment, which would therefore require a complete or partial control-system upgrade to achieve compliance.

The NERC CIP Standards

The NERC develops and enforces reliability standards [35], monitors the bulk electric system (BES) in North America, and educates industry personnel. One of NERC's key areas of focus is cyber security. As part of this program, the NERC has developed CIP standards that detail specific compliance requirements to be met by power plants and other responsible entities.

The NERC CIP standards include provisions for identifying critical cyber assets (CIP-002), developing security management controls (CIP-003), implementing training (CIP-004), identifying and implementing perimeter security (CIP-005), implementing a physical security program for the protection of critical cyber assets (CIP-006), protecting assets and information within the perimeter (CIP-007), conducting incident reporting and response planning (CIP-008), and crafting and implementing recovery plans (CIP-009). The NERC CIP Version 5 has two additional standards for configuration change management and vulnerability assessments (CIP-010) and information protection (CIP-011).

Among other responsible entities, power plants are currently required to comply with Version 3 of the NERC CIP standards. Version 4, which has additional requirements for identifying critical assets and critical cyber assets, is due to become effective in April 2014.

Version 5 is a significant rewrite of prior versions. It includes certain wholesale changes in the program and is seen as a more mature set of standards. It has been approved by the NERC board of trustees and was submitted to FERC for regulatory approval in January 2013. The NERC requested that the FERC retire Version 4 and use Version 5 to replace Version 3. The FERC has agreed within their notice of proposed rulemaking and public commission statements that this approach is reasonable, and they are working toward that end [36].

DCSs and associated computer systems must comply with the NERC CIP standards for plants with a total generation capacity of 1500 MW or more. Power plants might find it increasingly difficult to comply with certain NERC CIP requirements because of limited access- and change-control features provided by legacy DCSs and attached computer systems. This could become the driving force behind upgrading these systems with ones that support the NERC CIP compliance.

What follows is a high-level overview of the NERC CIP standards, and, where applicable, discussions of specific issues in meeting their requirements with obsolete or otherwise unsupported legacy control systems, software, and operating systems. For the purpose of this report, these standards are viewed from the perspective of applying them to process control systems, including DCSs and PLCs, their engineering stations and programming tools, and their associated HMIs and process data historians.

NERC CIP-001 covers sabotage reporting and does not form part of the Cyber Security Standards covered in NERC CIP-002 through 011. Therefore, the discussion begins with NERC CIP-002.

CIP-002: Critical Cyber Asset Identification

Version 4

A responsible entity is required to identify all of its critical assets through a risk-based assessment methodology and maintain a list of these assets. The list of critical assets must then be used to define a list of associated critical cyber assets that are essential to the operation of the critical assets. The entity must update these lists as necessary, review them at least annually, and senior management must approve them annually.

Under CIP-002-4, a computing system or device qualifies as a cyber asset if it uses a routable protocol to communicate within a control center or to communicate outside of an electronic security perimeter (ESP), or a device that is accessible through dial-up. The only cyber assets that must be considered are those shared cyber assets that could, within 15 minutes, adversely impact the reliable operation of a unit classified as a critical asset.

Applicable to this report is the Critical Asset Criterion 1.1: Generating units at a single plant of which the plant has a net real power aggregate rating of 1500 MW or more are classified as critical assets. However, Criterion 1.3 allows the planning coordinator or transmission planner to designate other generation facilities as critical assets as necessary to avoid adverse reliability impacts.

Version 5

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying critical assets and critical cyber assets to identifying BES cyber systems.

The standard provides criteria for responsible entities to categorize their BES cyber systems based on the impact of their associated facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the BES.

The standard requires that responsible entities identify all high-, medium-, and low-impact BES cyber systems according to a classification system. These identifications need to be updated and approved by senior management at least once every 15 calendar months.

Applicable to this report is the Impact Rating Criterion 2.1 that would classify BES cyber systems associated with generating units at a single plant of which the plant has a net real power aggregate rating of 1500 MW or more as a medium impact rating. In addition, Criterion 2.6 allows the planning coordinator or transmission planner to assign other generation facilities with medium impact ratings as necessary to avoid adverse reliability impacts. Other generation resources will have a low impact rating.

BES cyber systems have associated cyber assets, which, if compromised, pose a threat to the BES cyber system by virtue of: (a) their location within the ESP (protected cyber assets) or (b) the security control function that they perform (electronic access control or monitoring systems and physical access control systems). These cyber assets include the following:

- Electronic access control or monitoring systems such as electronic access points, intermediate devices, authentication servers, security event monitoring systems, and intrusion detection systems
- Physical access control systems such as authentication servers, card systems, and badge control systems
- Protected cyber assets, which are devices within the ESP, such as file servers, FTP servers, time servers, local area network switches, networked printers, digital fault recorders, and emission monitoring systems

Impact on Legacy Control Systems

According to Version 4, control systems and HMIs at plants producing more than 1500 MW are classified as critical cyber assets. According to Version 5, control systems and HMIs are classified as BES cyber systems, and related systems are classified as associated cyber assets. Both are assigned a medium impact rating at plants producing more than 1500 MW and a low impact rating at other plants.

The implementation of CIP-002 Version 4 or 5 should not be affected by a cyber asset that is obsolete or no longer supported by the OEM.

CIP-003: Security Management Controls

Version 4

This standard requires that responsible entities have at least minimum security management controls in place to protect critical cyber assets. It requires that the responsible entity document and implement a cyber security policy that represents management's commitment and ability to secure its critical cyber assets. This policy must address CIP-002-4 to CIP-009-4, must be readily available to personnel working with cyber assets, and must be reviewed and approved annually. It requires identification of a responsible manager and reporting of exceptions.

The CIP-003-4 standard also requires identification, classification, protection, and change-control of critical cyber asset information and access control to this information. The critical cyber asset information to be protected includes operational procedures, lists as required in CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain critical cyber assets, equipment layouts of critical cyber assets, disaster recovery plans, incident response plans, and security configuration information. Although not specifically mentioned, control system and HMI configuration would also be included.

Version 5

This standard specifies consistent and sustainable security management controls that establish responsibility and accountability to protect BES cyber systems against compromise that could lead to incorrect operation or instability in the BES.

It requires for all high- and medium-impact BES cyber systems that the responsible entity establish documented cyber security policies that collectively address the following:

1.1 Personnel and training (CIP-004)

1.2 ESPs (CIP-005), including interactive remote access

1.3 Physical security of BES cyber systems (CIP-006)

1.4 System security management (CIP-007)

1.5 Incident reporting and response planning (CIP-008)

1.6 Recovery plans for BES cyber systems (CIP-009)

1.7 Configuration change management and vulnerability assessments (CIP-010)

1.8 Information protection (CIP-011)

1.9 Declaring and responding to CIP exceptional circumstances

It also requires documented cyber security policies for all high- and medium-impact BES cyber systems that address the following:

2.1 Cyber security awareness

2.2 Physical security controls

2.3 Electronic access controls for external routable protocol connections and dial-up connectivity

2.4 Incident response to a cyber security incident

These policies must be reviewed and approved at least every 15 months. A senior CIP manager must be identified by name, and delegation of authority must be documented.

Impact on Legacy Control Systems

The implementation of NERC CIP-003 Version 4 or 5 should not be affected because a cyber asset is obsolete or no longer supported by the OEM.

CIP-004: Personnel and Training

Version 4

This NERC CIP standard requires that personnel having authorized unescorted physical access to critical cyber assets, including contractors and vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

This standard also requires that the responsible entity maintain list(s) of personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets. These lists must be kept up to date, and the responsible entity must revoke access of personnel terminated or who no longer require access.

Version 5

This standard is designed to minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing high- and medium-impact BES cyber systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES cyber systems.

The standard also requires an authorization process for electronic and physical access to high- and medium-impact BES cyber systems or their information, and a process for revocation of such authorization and access upon termination or when no longer needed.

The standard calls for changing of shared passwords after personnel have been terminated or reassigned, but this applies only to high-impact BES cyber systems.

Impact on Legacy Control Systems

Meeting the standard's requirements for personnel risk assessment, training, and security awareness is not affected by outdated or unsupported legacy control systems.

Access Revocation

The standard requires that physical and cyber access to cyber assets be controlled. Physical access control is not affected by the features or obsolescence of the control system; it requires a physical security perimeter (PSP) around the cyber assets with access control. Similarly, cyber access can be controlled by an ESP secured with network access policies and firewalls.

Version 5 of the standard requires changing of shared passwords after personnel have been terminated or reassigned, but this applies only to high-impact BES cyber systems. Certain old control systems have standard, unchangeable passwords on their engineering stations and/or operating consoles.

CIP-005: Electronic Security Perimeters

Version 4

This standard requires the identification and protection of the ESP(s) inside which all critical cyber assets reside, as well as all access points on the perimeter.

It dictates that ESP(s) as well as all access points to the perimeter(s) be identified and documented and that all critical cyber assets reside within the ESP(s). Any noncritical cyber asset inside an ESP must be treated as if it were a critical cyber asset.

Responsible entities must implement electronic access controls, continuously monitor access, and conduct annual vulnerability assessments at access points. Documentation must be maintained to support compliance.

Version 5

This standard is designed to manage electronic access to high- and medium-impact BES cyber systems by specifying a controlled ESP in support of protecting BES cyber systems against compromise that could lead to misoperation or instability in the BES.

It requires that all high- and medium-impact BES cyber assets connected to a network through a routable protocol reside within a defined ESP. It requires inbound and outbound access permissions, including the reason for granting access, and that all other access is denied by default. It also requires methods for detecting known or suspected malicious communications for both inbound and outbound communications.

CIP-005-5 also requires the utilization of an intermediate system so that the cyber asset initiating interactive remote access does not directly access an applicable cyber asset and that all interactive remote access use multifactor authentication encryption that terminates at the intermediate system.

Impact on Legacy Control Systems

Both Versions 4 and 5 of this standard appear to have no specific requirements for the cyber assets inside of the ESP. It seems that compliance efforts will not be hampered by legacy and unsupported control systems.

CIP-006: Physical Security of Critical Cyber Assets

Version 4

CIP-006-4 requires the implementation of a physical security program for the protection of critical cyber assets.

The responsible entity has to document, implement, and maintain a physical security plan, approved by senior management. The standard requires documenting, implementing, and maintaining an approved physical security plan that requires each ESP (as well as its access control equipment) to reside inside a protective PSP. All physical access points must be identified, access controlled, and monitored. Physical entry must be logged, and all systems used to support these requirements must be maintained and tested.

Version 5

The purpose of the CIP-006-5 cyber security standard is to manage physical access to BES cyber systems by specifying a physical security plan in support of protecting BES cyber systems against compromise that could lead to misoperation or instability in the BES.

It requires operational or procedural controls to restrict physical access and, for medium-impact BES cyber system, use at least one method of physical access control to allow unescorted access into each applicable PSP to authorized individuals only (high-impact BES cyber systems require two or more different methods of access control).

It also requires logging authorized access and monitoring unauthorized access to the PSP or its access control systems and alarming it to the appropriate personnel. It also requires logging and escorting visitors and maintaining and testing the physical access control system.

Impact on Legacy Control Systems

Both Versions 4 and 5 of this standard appear to have no specific requirements for the cyber assets inside of the PSP. It seems that compliance efforts will not be hampered by legacy and unsupported control systems.

CIP-007: Systems Security Management

Version 4

This standard requires responsible entities to define methods, processes, and procedures for securing those systems determined to be critical cyber assets, as well as the other (noncritical) cyber assets within the ESP(s). The following paragraphs are numbered according to the requirements in the standard for cross-referencing purposes.

1. **Test procedures**. Test procedures are required to ensure that new cyber assets and significant changes (for example, implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware) do not adversely affect existing cyber security controls.
2. **Ports and services**. Only those ports and services required for normal and emergency operations may be enabled. All other services and ports must be disabled. Appendix 1 in the standard notes that the term *ports* refers to logical ports, for example, TCP ports.
3. **Security patch management**. A security patch management program is required for tracking, evaluating, testing, and installing applicable cyber security software patches. Patches and upgrades must be evaluated, implemented, and documented within 30 days. Where a patch is not installed, compensating measure(s) applied to mitigate risk must be documented.
4. **Malicious software protection**. Antivirus and other malicious software (malware) prevention tools must be used, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware. Virus and malware prevention signatures must be kept up to date. In the case where antivirus software and malware prevention tools are not installed, the responsible entity must document compensating measure(s) applied to mitigate risk exposure.
5. **Account management**. Technical and procedural controls are required to enforce access authentication of, and accountability for, all user activity, and minimize the risk of unauthorized system access. This includes ensuring that individual and shared system accounts and authorized access permissions are kept to the minimum required to perform work functions and approved as set forth in CIP-003-4.

   Methods, processes, and procedures are required for generating logs of sufficient detail to create historical audit trails of individual user account access activity.
   A policy is required for minimizing and managing the scope and acceptable use of administrator, shared, and other generic account privileges, including factory default accounts. Strong passwords must be used and changed at least annually, as technically feasible.

6. **Security status monitoring**. All cyber assets within the ESP, as technically feasible, must implement automated tools or organizational process controls to monitor system events that are related to cyber security. Security monitoring controls must issue alerts, and logs related to cyber security must be maintained, where technically feasible.
7. **Disposal or redeployment**. Data storage media shall be destroyed or erased before cyber assets used within the ESP are disposed or redeployed outside of the ESP.
8. and 9. **Cyber vulnerability**. Assessment and a documentation review must be done at least annually.

Version 5

The purpose of CIP-007-5 is to manage system security by specifying select technical, operational, and procedural requirements in support of protecting high- and medium-impact BES cyber systems against compromise that could lead to misoperation or instability in the BES. The following paragraphs are numbered according to the requirements in the standard for cross-referencing purposes:

1. **Ports and services**. Where technically feasible, only logical network accessible ports that have been determined to be needed may be enabled. If a device has no provision for disabling or restricting logical ports on the device, those ports that are open are deemed needed. Also, protection is required against the use of unnecessary physical ports (for example, network connectivity, keyboards, or removable media).
2. **Security patch management**. A process must be implemented for tracking, evaluating, and installing cyber security patches for applicable cyber assets at least once every 35 days. The tracking portion shall include the identification of the sources tracked for the release of cyber security patches for applicable cyber assets that are updatable and for which a patching source exists. Patches must either be applied or a plan must be created and implemented for mitigating the vulnerabilities addressed by each security patch.
3. **Malicious code prevention**. Methods must be deployed to deter, detect, or prevent malicious code (for example, through antivirus software, system hardening, policies). If malicious code detection uses signatures, these signatures must be tested and updated.
4. **Security event monitoring**. Events must be logged at the BES cyber system level (per BES cyber system capability) or at the cyber asset level (per cyber asset capability) for identification and after-the-fact investigations of cyber security incidents, including successful logins, failed login attempts, and detected malicious code. Alerts must be generated for failed login attempts and detected malicious code.
5. **System access control**. Interactive user access must be authenticated where technically feasible. All enabled default or generic account types, and users who have authorized access to shared accounts must be identified. Known default passwords must be changed if the cyber asset allows it. Strong passwords and password changes every 15 months (both as supported by cyber asset) must be enforced technically or procedurally for password-only authentication. Where technically feasible, the number of unsuccessful logins must be limited and alerts generated when the threshold is exceeded.

Impact on Legacy Control Systems

Because this standard focuses on security of the cyber assets themselves, its implementation is affected to a large extent by the degree to which cyber assets support cyber security and access control. Neither version specifies how requirements should be met, which provides leeway for using security procedures in lieu of automatic security features when the latter are unavailable on legacy systems. Both versions of the standard make provision for cyber assets that do not support certain requirements, although this is stated more consistently in Version 5. Version 4 often refers to achieving objectives *technically or procedurally*. The security industry uses the term *compensating controls* for alternative approaches to implementing a requirement. Note that if a requirement cannot be implemented, a technical feasibility exception may be required for submission. The following is a brief discussion about achieving NERC CIP-007 compliance on legacy systems.

Disabling Unnecessary Logical Ports

Cyber assets using Windows operating systems and some other cyber assets may likely have unnecessary TCP and user datagram protocol ports left open. Logical ports can be disabled in the cyber asset's configuration, or, if this is not possible, a firewall can be placed in line with the asset's network connection. Under Version 5, if ports cannot be disabled, they are deemed necessary.

Disabling Unnecessary Physical Ports

Computer systems and some controllers will likely have unused physical ports. Unused network, parallel, serial, and USB ports external to the cyber asset's device casing can be disabled through software configuration, by disconnecting internal cables and/or removing the port connector (assuming this will not void the warranty of a legacy system), by adding prominent signage and tamper tape, or by physically obstructing the port.

Disabling Unnecessary Drivers

The Windows operating system typically loads many unnecessary drivers. Other operating systems may do the same. If supported by the cyber asset, unused drivers can be disabled in the asset's startup/boot configuration.

Security Patch Management

Microsoft and other software vendors typically stop supporting software a decade or so after its first release. Thereafter, security patches are no longer produced.

Meeting the requirements of CIP-007 under the absence of security patches for unsupported software and operating systems (especially Microsoft operating systems) could understandably be a cause for concern. However, the CIP-007 standard does not state a requirement for the application of security patches to all cyber assets; the requirement is only to the systems for which patches are being produced. Version 5 of the standard provides guidelines that state that a patch source is not required for "cyber assets that have no existing source of patches such as vendors that no longer exist."

Malicious Code Prevention

Antivirus software running only on old operating systems may become obsolete and no longer supported by the OEM. New viruses and malware are developed daily, and these will most likely not be detected by outdated antivirus software.

Similar to security patches, the unavailability of updated virus signatures for obsolete operating systems could be a cause for concern. Again, the CIP-007 standard does not state a requirement that all cyber assets must be protected by antivirus software. Version 4 states that antivirus and malware prevention tools must be used, "where technically feasible." In the case where antivirus software and malware prevention tools are not installed, compensating measure(s) must be applied to mitigate risk exposure. Version 5 guidelines provide examples of alternatives: white-listing solutions, network isolation techniques, portable storage media policies, intrusion detection/prevention solutions, and so forth. Assuming an obsolete operating system, network isolation techniques, portable storage media policies, and system hardening such as recommended by the Center for Internet Security [37] may provide reasonable protection against malicious software.

System Access Control

Operating systems have had account management and user authentication capabilities for many years, but the oldest operating systems may not have these features. In this case, Version 4 of the standard allows for "procedural methods" of controlling access to cyber assets. These may include locking engineering stations and having to sign for a key to get access, or securing physical access to these cyber assets. Version 5 of the standard requires user authentication "where technically feasible."

Neither of the versions restricts the use of cyber assets that do not possess inherent access control, provided that other sufficient methods for access control are in place and documented. The guidelines in Version 5 elaborate that physical security suffices for local access configuration if the physical security can record who is in the PSP and at what time.

Security Event Monitoring

Cyber threats have escalated over the last decade, and modern cyber assets and operating systems have many more features detecting security events than systems of one or two decades ago. Version 4 states that security status monitoring is required "as technically feasible," whereas Version 5 states that security event monitoring must be done "per cyber asset capability." Neither of the versions restricts the use of cyber assets that do not provide security event monitoring.

Other Requirements

Other requirements, that is, disposal or redeployment of cyber assets, cyber vulnerability assessment, and documentation review, are not affected by the lack of security features and OEM support of obsolete cyber assets. Meeting these requirements will unlikely be hampered by legacy control systems and associated computer systems.

CIP-008: Incident Reporting and Response Planning

Version 4

This standard ensures the identification, classification, response to, and reporting of cyber security incidents related to critical cyber assets. It requires a response plan and documentation of incidents.

Version 5

The purpose of this standard is to mitigate the risk to the reliable operation of the BES as the result of a cyber security incident by specifying incident response requirements. It requires a process to identify, classify, and respond to cyber security incidents and to determine whether the incident is reportable. It also requires testing the response plan every 15 months as well as other management processes.

Impact on Legacy Control Systems

Both Versions 4 and 5 of this standard appear to have no specific requirements for cyber assets. Compliance efforts should not be hampered by legacy and unsupported control systems.

CIP-009: Recovery Plans for Critical Cyber Assets

Version 4

CIP-009 ensures that recovery plans are put in place for critical cyber assets and that these plans follow established business continuity and disaster recovery techniques and practices.

The standard requires recovery plans, exercises, and change control to the plans. It also requires backup and storage of information required to successfully restore critical cyber assets. It also requires that the restoration mechanisms be tested annually.

Version 5

The purpose of this standard is to recover reliability functions performed by high- and medium-impact BES cyber systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

It requires a recovery plan with activation conditions and roles and responsibilities of responders. It requires the backup, verification of completion, and storage of information to recover BES cyber system functionality. It requires preserving the data, per asset capability, that led to the trigger of a security incident response. Recovery plans must be tested at least every 15 months, including testing a representative sample of recovery information. Tests must be documented and plans updated according to lessons learned.

Impact on Legacy Control Systems

The requirements specified by Versions 4 and 5 of the standard are mostly procedural, but backup and restoration requirements are technical. Even legacy control systems and HMIs have the ability to download and upload their configurations, although this will likely have to be done

manually. For system restoration, old HMIs typically require the installation of system software, so it will be important to have that software available and also backed up. Old programming tools could be backed up by creating mirror or ghost images of their storage media. Although, in some cases, it could be technically challenging to establish an effective procedure for backing up and restoring legacy control system information, it is unlikely that the entire control system will have to be upgraded because one of its components cannot be backed up or restored.

CIP-010-1: Configuration Change Management and Vulnerability Assessments

CIP-010-1 is a new standard in CIP Version 5 and was established to prevent and detect unauthorized changes to high- and medium-impact BES cyber systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES cyber systems from compromise that could lead to misoperation or instability in the BES.

It requires the development of a baseline configuration for all systems. The baseline must include the following items:

- Operating system(s) (including version) or firmware where no independent operating system exists
- Any commercially available or open-source application software (including version) intentionally installed on the cyber asset (intentionally meaning the software is necessary for operation of the asset and excludes software such as notepad, calculator, dynamic link libraries, drivers, and so forth, installed with the operating system)
- Any custom software installed
- Any enabled logical network accessible ports
- Any security patches applied to the system

It then requires a change-management program for any changes to the established baseline, including an assessment of impact on and compliance to CIP-005 and CIP-007. The new standard also requires a monthly audit of the configuration to ensure that no changes have occurred and to investigate and document unauthorized changes. It also calls for frequent vulnerability assessments to be done at least on paper (for high-impact BES cyber systems, an active vulnerability assessment must be done at least every three years).

Impact on Legacy Control Systems

The specification does not specifically require baselining and auditing the control logic and other process control-related configuration of control systems and HMIs, which, if specified, would have resulted in a very substantial undertaking. However, a very real attack vector exists through the control system configuration. Maintaining baseline configuration and configuration control of control system configuration files and control logic should be considered as part of the cyber security strategy.

IT management software tools exist for modern operating systems to fully automate the baselining and auditing processes, but, on older systems, all of the required information might have to be obtained through manual inspection of the systems. This could be a tedious process.

CIP-011-1: Information Protection

CIP-011-1 is also a new standard in CIP Version 5 and was established to prevent unauthorized access to high- and medium-impact BES cyber system information by specifying information protection requirements in support of protecting BES cyber systems against compromise that could lead to incorrect operation or instability in the BES.

It requires methods to identify information that meets the definition of BES cyber system information and procedures for protecting and securely handling BES cyber system information, including storage, transit, and use. It also requires methods such as sanitation, destruction, or encryption to prevent the unauthorized retrieval of BES cyber system information from cyber assets that have been released from their original purpose for reuse or destruction.

Impact on Legacy Control Systems

This new standard has requirements that are not affected by the features and obsolescence status of, or support for, control systems and related computer equipment. Compliance efforts should not be hampered by legacy and unsupported control systems.

Summary

The NERC CIP standards require a substantial amount of processes and procedures but also access control, changes to network layouts, and restrictions to the computer-system openness. Newer control systems, network hardware, and operating systems have many more features supporting cyber security compared to systems dating back to the 1980s and 1990s.

Although the NERC CIP standards require elevated levels of cyber security for certain power plants, the standards do not dictate how the requirements must be met, and, in several cases, provide explicit leniency toward systems that do not natively support the requirements. When outdated technology falls short of meeting the requirements, procedures, work processes, and alternative solutions can be implemented to achieve compliance. NERC CIP 5 provides several alternatives for becoming compliant with technology not directly supporting modern solutions.

It would appear that the NERC CIP requirements can be met with legacy, low-security control systems, provided that alternative measures or compensating controls (such as additional procedures) are put in place.

7
CONCLUSIONS

Many power producers become concerned with the life cycle of a DCS only when they receive notification from the OEM that the system is no longer supported. Although this situation could result in a reactive effort to gain information, develop a plan, obtain funding, and execute an upgrade project, hasty action is often not necessary. Spare parts and repairs are typically available at a reasonable cost from third-party providers long after the OEM has terminated support. This gives a plant the chance to carefully evaluate all options and adopt a life cycle management strategy that suits the company's business needs.

Several upgrade options exist for modernizing old control systems. Control systems can be viewed as modular units consisting of HMI, controllers, I/O, terminations, and field devices. In many cases, the system architectures allow for the replacement of only certain parts of the control system. At minimum, OEMs all provide the ability to upgrade control systems while retaining the original field wiring and terminations. Partial upgrades and migrating control system configuration from the old system to the new one may cost only 25% of a complete upgrade.

A range of options exists for managing the life of control systems. These options also provide a range of cost implications and risk of failure and obsolescence. One option is to follow the OEM's recommendations for when upgrades are necessary, whereas another would be to upgrade components only if it can be cost-justified. Other options also exist. The type of strategy used will depend largely on the culture of the company and the long-term business plan for the plant.

It seems challenging, if not impossible, to justify control system upgrades based on the resultant benefits alone. Unless a serious reliability problem exists, the reduction in unit trips and maintenance costs also seems to add too little to the equation to show a return in the three- to five-year timeframe. Upgrades seem to pay for themselves over one to two decades. It is only if management agrees that control-system equipment must be covered by an OEM service plan that upgrade approvals become less challenging.

OEMs offer life cycle planning services in which they audit the installed base of control systems in a plant or fleet. They use these data in conjunction with product life cycle plans and business objectives for each unit being considered to develop a life cycle management plan for the entire plant or fleet.

NERC CIP may push a plant toward control system modernization, but it does seem possible to meet all of its requirements without having to replace low-security, obsolete computer equipment. In some cases, compliance will require the use of alternative methods and additional procedures.

8
REFERENCES

1. *Automation Life Cycles—Important Consideration for Purchases, Migrations & Upgrades*, Bill Lydon, Automation.com, March 29, 2013.
2. *The Product Life Cycle*, QuickMBA.com, Internet Center for Management and Business Administration, Inc., 2010.
3. Invensys Operations Management and ARC, *Modernizing Aging Process Automation Systems—Options and Best Practices*, ControlGlobal.com, November 5, 2010.
4. Automation & Control Engineering, Group Discussion on LinkedIn.com, http://lnkd.in/AwXe4D, June 2013.
5. K. Keiser and T. Stauffer, "Approaches for Migration of Legacy DCS Systems to Maximize Return on Existing Assets." Presented at the ISA EXPO, Spring House, PA, October 25−27, 2005.
6. *Straight Talk on DCS Migration*, Panel Discussion, ISA and Maverick Technologies, http://www.youtube.com/watch?v=9IjlVkpP4xg, 2013.
7. D. Hebert, *Best Practices in Control System Migration*, ControlGlobal.com, January 5, 2007.
8. *I&C Obsolescence Management Strategy: Pilot Study and Lessons Learned*. EPRI, Palo Alto, CA: 2008. 1015083.
9. F. Ruebeck, *Heritage of Bailey Controls*, http://www.classicautomation.com, 2012.
10. R. Becker, *Evolution, Not Revolution*, ABB, http://www.abb-conversations.com/2013/06/evolution-not-revolution/, June 12, 2013.
11. *Symphony Harmony Distributed Control Systems—Benefits of an Evolution Strategy*, ABB, 3BUS095397 EN US Letter Power Generation 0611, 2011.
12. *WDPF-to-Ovation Migration*, Emerson Process Management, Power & Water Solutions, 2007.
13. *Mark IV to Mark VIe Migration Gas Turbine Controls Upgrade*, General Electric Company, 2005.
14. *Mark VIe Control Migration from Mark V Control*, General Electric Company, 2010.
15. *I/A Series System Life Cycle Product Phase Listing*, Invensys Systems, Inc., 2012.
16. N. James, *Control System Migration*, ControlGlobal.com, January 12, 2009.
17. H. Bloch, *Using Simplified Life Cycle-Cost Computations to Justify Upgrades*, Chemical Engineering, January 2013, pp 53–56.

18. J. Ford, *How Much Is Your Legacy DCS Costing You?* Maverick Technologies, http://www.mavtechglobal.com/ideas/2012/01/25/how-much-is-your-legacy-dcs-costing-you/, January 25, 2012.

19. *Circuit Card Life-Cycle Management Good Practices from Non-Nuclear Power Industries in Europe*. EPRI, Palo Alto, CA: 2011. 1022679.

20. *Military Handbook for Reliability Prediction of Electronic Equipment*, U.S. Department of Defense, MIL-HDBK-217F, 1991.

21. *Reliability Prediction Procedure for Electronic Equipment*, Telcordia, Document Number SR-332, Issue 3, January 2011.

22. *Reliability Data Handbook: Universal Model for Reliability Prediction of Electronics Components*, PCBs and equipment, International Electrotechnical Commission, IEC TR 62380, 2004.

23. ITEM ToolKit, Item Software, http://www.itemsoft.com/item_toolkit.html, August 26, 2013.

24. M. G. Pecht and F. R. Nash, "Predicting the Reliability of Electronic Equipment." Proceedings of the IEEE, Vol. 82, No. 7, July 1994.

25. D. J. Wilkins, *The Bathtub Curve and Product Failure Behavior. Part One—The Bathtub Curve, Infant Mortality and Burn-in*, http://www.weibull.com/hotwire/issue21/hottopics21.htm, Reliability HotWire, Issue 21, November 2002.

26. D. J. Wilkins, *The Bathtub Curve and Product Failure Behavior. Part Two—Normal Life and Wear-Out*, http://www.weibull.com/hotwire/issue22/hottopics22.htm, Reliability HotWire, Issue 22, December 2002.

27. *Power Plant Cycling Costs*, AES 12047831-2-1. Prepared by Intertek APTECH for the National Renewable Energy Laboratory, 2012.

28. *2012 Brief: Average Wholesale Electricity Prices Down Compared to Last Year*, U.S. Energy Information Administration, http://www.eia.gov/todayinenergy/detail.cfm?id=9510, January 9, 2013.

29. J. Conca, *The Direct Costs of Energy: Why Solar Will Continue To Lag Hydro And Nukes*, http://www.forbes.com/sites/jamesconca/2012/07/08/the-direct-costs-of-energy-hydronuclear-best-solar-still-lagging/, July 8, 2012.

30. A. Ginter, *Securing Industrial Control Systems*, Chemical Engineering, July 2013.

31. CNN, *China Gained U.S. Weapons Secrets Using Cyberespionage*, http://www.cnn.com/2013/05/28/world/asia/china-cyberespionage, May 29, 2013.

32. *Stuxnet*, http://en.wikipedia.org/wiki/Stuxnet, 2013.

33. *Shamoon*, http://en.wikipedia.org/wiki/Shamoon, 2013.

34. L. Neitzel, *Six Steps to Control System Cyber Security*, InTech, May/June 2013, pp 45–48.

35. *Reliability Standards for the Bulk Electric Systems of North America*, NERC, http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf, November 8, 2013.

36. A. M. Freed, *NERC CIP Version 5: One Giant Leap*, tripwire.com, http://www.tripwire.com/state-of-security/regulatory-compliance/nerc-cip-version-5-one-giant-leap/, June 20, 2013.

37. Center for Internet Security, http://www.cisecurity.org/, 2013.

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute Inc., (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together...Shaping the Future of Electricity

Program:

Instrumentation Controls and Automation

© 2013 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

3002001123

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com