ARC CLIENT REPORT

APRIL 2015

Network Security Benchmarking Study

Prepared for: ARC Industry Participants

Project Team:
Peter Reynolds
Eric Cosman
Paul Steinitz
Paul Miller

ARC Advisory Group

Copyright © 2015 ARC Advisory Group

Mutual Confidentially Statement

ARC Advisory Group agrees to conduct this Custom Consulting study under the strictest confidence. That includes not sharing the Client's name with any of the companies being interviewed to collect the data requested. The Client mutually agrees to not divulge the fact that ARC has completed a custom consulting project for the Client, nor any of the data or recommendations made to the Client to anyone outside of the Client's company, specifically any of the companies interviewed for the data. Should it become necessary to share information from this study outside of the Client Company for any reason, the Client must advise ARC Advisory Group in writing of such a need and secure ARC's approval in writing of such an action?

Disclaimer

While every effort has been made to ensure the accuracy and the completeness of the information presented in this report, ARC Advisory Group accepts no liability what so ever for consequences of any actions taken on the findings of the report.

Report Follow-up Services

An ARC industry report, while comprehensive, cannot possibly answer every question or pro-vide all information desired by every client. To ensure that our clients have access to ARC's database and consulting staff, we provide follow up services at cost. The goal of this program is to provide clients with additional data and analysis that are of specific interest. We hope that through the use of these services our clients will have the best possible information for making decisions and developing strategies. Naturally, ARC welcomes questions that are procedural or involve clarification of methodology or definitions at no charge to subscribers.

Telephone us at 781-471-`1000 or visit www.arcweb.com to let us know the information you require. We will discuss your needs, call you back, tell you how much it will cost, and how long it will take. Our fees for follow-up services will be at our cost for labor, plus expenses incurred. ARC recommends that clients seek a quote in advance.

Executive Overview

This report provides the results of a research study performed by ARC Advisory Group for our Clients to assist in the development of a secure network architecture for Manufacturing Operations Management (MOM)[1] and related applications, Industrial Control Systems (ICS) and the associated network interfaces.

Research Study

Many clients have requested ARC to study the current situation for network security, benchmark the best practices for network security, and compare its architecture to the benchmark results. Information was collected via a combination of a general survey and more focused individual interviews.

Key Findings

The survey and interviews generated several significant findings:

- MOM applications in the Oil and Gas industry may be centralized at the enterprise (level 4) layer or de-centralized to a plant network (level 3) layer.
- A small majority of respondents indicated that they enforce "outbound only" data flow from their ICS to MOM applications in their plants (more so in continuous process plants than in plants with batch processes).
- Unidirectional data diodes are not widely used throughout this industry. However, some companies interviewed expressed positive interest.
- Some companies reported the need to separate MOM applications as far as possible from industrial control segments by network segregation.
- Risk analysis process for determining network segmentation and cybersecurity defense layers is currently weak.

[1] Manufacturing Operations Management (MOM) is a class of solutions that includes the older term Manufacturing Execution Systems (MES).

- Organizational factors have influenced some companies to centralize applications away from the plant support organization. The “best” network for MOM will depend on organizational design and the business strategy for centralizing functions facilitated by MOM applications.

Study Description

This study consisted of a survey that received over seventy responses, including several from representatives of major Oil & Gas, Refining and Petrochemical companies, followed by more focused interviews with industry participants about cybersecurity process, technology, and organizational factors.

Study Goals

The following specific goals were established for this study:

1. Benchmark with different Oil & Gas, Refining and Petro-Chemical companies concerning the following topics:
   - Cybersecurity-related risk management in the industrial network zones
   - The ideal network segmentation for the MOM, APC, Modeling, and other plant operation applications.
   - The use of data diodes and similar technologies for unidirectional data transfer between MOM applications and Enterprise applications and the effect on the business and operating the facility
   - Methods and technologies for bi-directional between Applications on the WAN (MOM or Enterprise) and systems in PAN network
   - The "best" network required to run the business of oil and gas, Refining and Petro-Chemical plants
2. Identify possible criteria for identifying and assessing risks associated with designing the security strategy.
3. Identify required security restrictions that may be used to ensure accurate implementation of the needed or mandated measures.

Research Results

The combination of web survey and individual interviews provide the basis for the analysis presented in this report. Results from each stage are presented in the following sections.

User Web Surveys

Between November 2014 and March 2015, ARC conducted a web-based survey of knowledgeable industry practitioners to help create benchmarks for network security practices for Manufacturing Operations Management (MOM) and related systems. Most respondents were owner-operators or end users, with additional input from engineering firms, system integrators, and consultants specializing in the Oil and Gas, Petrochemicals, and Chemicals industries. We learned that, overall, cybersecurity maturity and knowledge levels are still relatively low at many owner-operator companies and, in many cases, the system integrators and consultants have greater expertise in networks, systems, and processes.

ARC research projects occasionally exclude responses from SIs and consultants, so as not to bias the results. However, for cybersecurity research, ARC finds their contribution valuable and can find no particular bias toward services or other factors.

Web Survey Demographic Information

Each survey respondent was asked to qualify their submissions by providing a company name, title, and valid email address for future communications to validate the research. Since many owner-operators in the Oil and Gas industry rely heavily on engineering firms, system integrators, and consultants, ARC believes their input and opinions are significant and should be included in this analysis.

Table 1 – Demographics

Demographic Group	Representation
End User	60%
Supplier or OEM	8%
Engineering, System Integrator or Consultant	32%

Each web survey respondent also provided information about their respective industry and geographical location.

Table 2 – Industries

Industry	Representation
Oil and Gas, Refining and Petrochemical	67%
Power Generation	5%
Chemical	18%
Other	10%

Much of the analysis in this research focuses on the large process industry segments of upstream and downstream Oil and Gas and Petrochemicals.

Geographical location was also considered to help ensure a representative sample.

Table 3 – Geographic Regions

Region	Representation
North America	50%
Europe	16%
Middle East	12%
China, India, Japan and Latin America	22%

User Interviews

Targeted interviews were completed from February through March of 2015. Companies were specifically chosen to reflect various sizes relative to the Client. Different geographical locations were also chosen so as to gain a broad view of network security. Since the survey respondents revealed that nearly 40 percent relied on specialized external consultants with operational technology (OT) backgrounds, our analysis includes inputs from a small number of experienced consultants with specialized knowledge of Oil and Gas operational technology (OT).

Security Architecture Design Guidance

Among the web survey participants, it was not surprising to find that a large portion of end users have a MOM system designed by system integrators. Automation applications are often designed and implemented by in-house Automation and Engineering staff. Enterprise or corporate IT providers provide guidance on the design of the MOM security architecture. This is due to the technical complexity of many manufacturing automation systems and the way capital projects are delivered.

The specific responses to this survey question follow:

Source	Representation
Designed by System Integrator, or Automation or Application Provider	40%
Implemented by in-house Automation and Engineering staff	20%
Implemented by in-house Automation and Engineering staff in conjunction with Enterprise or Corporate IT	40%

Table 4 – Sources of Guidance

Network Structure

To support benchmarking against peers, it was necessary to develop a common taxonomy for describing the various zones of the client network. This taxonomy is based on the established industry reference model described in the ISA/IEC-62443 series of standards. This model is shown in Figure 1.

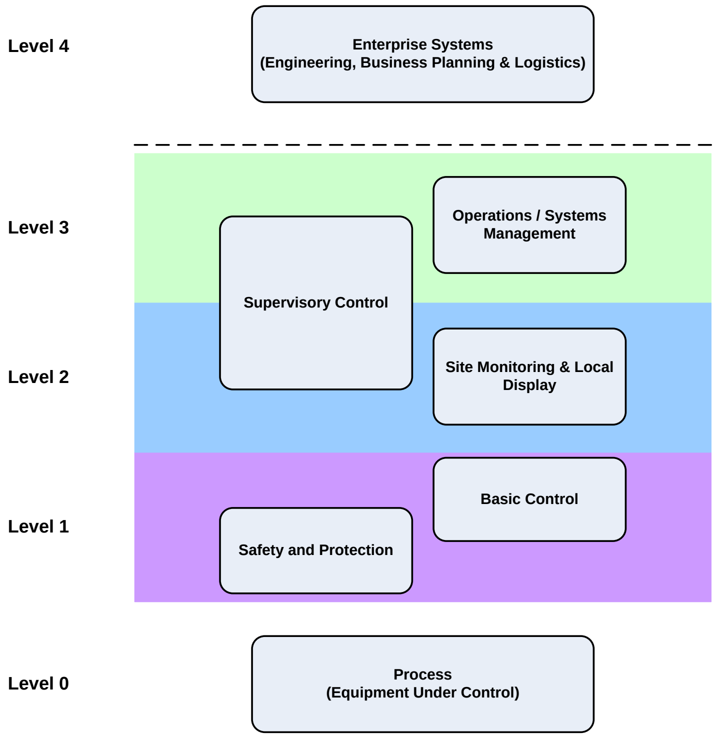

Level 4
Enterprise Systems
(Engineering, Business Planning & Logistics)
Level 3
Operations / Systems Management
Supervisory Control
Level 2
Site Monitoring & Local Display
Level 1
Basic Control
Safety and Protection
Level 0
Process
(Equipment Under Control)

Figure 1 – ISA/IEC-62443 Reference Model

Network Segmentation Practice

Companies would classify the ISA-95 levels according to the following. Level 4 networks are part of the Enterprise wide-area networks (WAN), and scope of responsibility for level 3 and 2 tended to be part of the plant networks.

Based on the ISA-95 model, each network level embodies different roles and functions, with levels 2 and 3 typically related to the plant networks and level 4 to the enterprise wide area network (WAN):

- Level 4 – Manage the Business
- Level 3 – Manage the Plant
- Level 2 – Manage the Process

Based on the above, MOM functions could reside at either level 3, 3.5 (DMZ), or level 4. Out of the 70 survey respondents, approximately one-third would place MOM within level 3, one-third at level 3.5, and another one-third at level 4. Among respondents from the Oil and Gas, Refining, and Petrochemicals industries, a higher percentage (40 percent) of companies include MOM at the enterprise level.

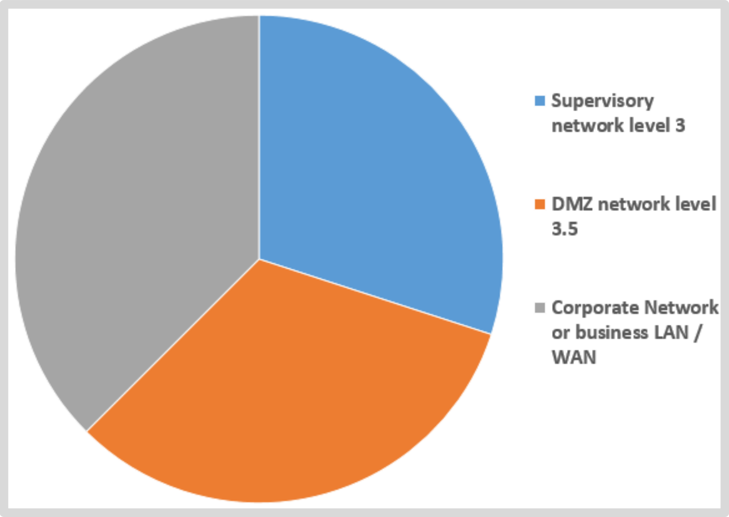


Figure 2 – MOM Applications are Part of Which Network Layer?

Perhaps the most fundamental prerequisite for an effective cybersecurity management program is the availability of a complete inventory of potentially impacted applications, including a description of the positioning of each application within the reference architecture.

In addition to the application inventory, it is also important to have a current and accurate description of the network configuration, as this forms the basis for establishing the appropriate security zones. The goal is to determine the “best” network for a given set of circumstances.

With the applications identified and the network characterized, the next step is to identify any specific security restrictions based on business and operational needs.

Data Flow Analysis

When asked about the security architecture and if they employ unidirectional data flow between MOM and lower level networks, 13 percent of respondents permitted no data flow between MOM and level 2 automation and ICS layers. Forty percent allowed one-way or unidirectional traffic. Just under 50 percent supported bi-directional data flow. The percentage split between companies supporting two-way data flow was not significantly different for the Oil & Gas, Refining, and Petrochemical industry segments.

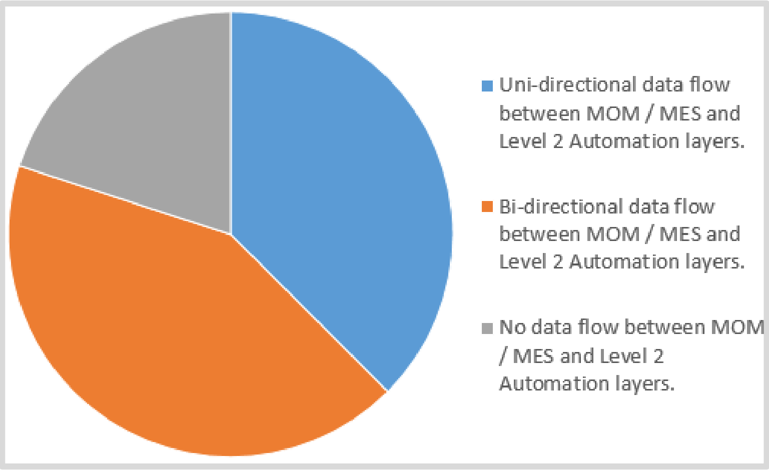


Figure 3 – Does your Security Architecture Permit Unidirectional Data Flow between MOM and Lower level ICS and Systems?

To control access to MOM and ICS or Enterprise layers, most companies have deployed some form of a firewall appliance with a certain degree of packet inspection. More mature organizations have provided a wider range and depth of defenses to supplement the firewall technology. One company reported firewalls difficult to justify and used a combination of access control lists (ACL's) and router-based security to control access to networks, but this was not typical.

Table 5 – Data or traffic access controls

Technology	Reported Adoption
Firewall with basic rules managed by internal staff	60%
Firewall with basic rules managed by external security provider	10%
Firewall with Stateful packet inspection (SPI - Analyze the packet header and footer to validate the session)	27%
Firewall with Deep Packet inspection (DPI - Analyze the full data part and content of the packet)	28%
Digital or Data Diode Appliance	8%
Air Gap and no connection between networks.	12%
Other (please specify)	5%

Data Exchange Methods

New technologies capable of providing controlled access to networks are emerging. Unidirectional gateways or data-diode appliances are available for a variety of requirements. However, there is some ambiguity in the terms used. End users may not differentiate between data diodes that were originally purpose-built for the military and newer unidirectional gateways built to be installed and used with multi-tiered databases like process historians.

Based on both web survey input and several interviews with Oil and Gas and Petrochemicals companies, it appears that data diodes are not prevalent, but have seen some mixed acceptance.

One interviewee from a major oil company specifically stated that uni-directional gateways or data diodes are explicitly excluded from their standard architecture. They believe that equivalent protection is possible using well-managed firewalls and a well-designed and well-managed network infrastructure, including the use of a demilitarized zone (DMZ).

A small percentage of respondents from the cybersecurity consultant group expressed the belief that data diodes will see greater acceptance within the industry.

In the Oil & Gas and Petrochemicals industry, it is not surprising to see the limitations placed on data flow. The slightly predominant "outbound only" rule from ICS to MOM reflects the application architecture for this industry. The Oil and Gas, Refining, and Petrochemicals industries tend to have different business requirements for real-time data than Specialty Chemicals and other batch process industries. Planning horizons tend to be longer and ERP systems (like SAP) tend not to be as tightly coupled.

This "loosely coupled" operational planning requirement does not typically require data flow to write down to the ICS layer. Most companies that deploy MOM applications tend to facilitate information transfer by supplying enterprise or level 4 computing and networks directly to operations. This avoids the risk of automating the data flow to the ICS. Other methods for supplying MOM to locations where only DCS networks are in place included supplying written orders for production.

Level 3 advanced process control (APC) and multi-variable control (MPC) applications, which do require read and write capabilities between the ICS MOM layers, are the exception here. Survey respondents and companies participating in the interviews acknowledged the best location for APC is as a (low) level 3 application that acts in a supervisory mode to the ICS.

Organizational Factors Influencing Network Segmentation

The survey also included a question who in (or outside) the organization has responsibility for securing operations systems. The following table summarizes the responses:

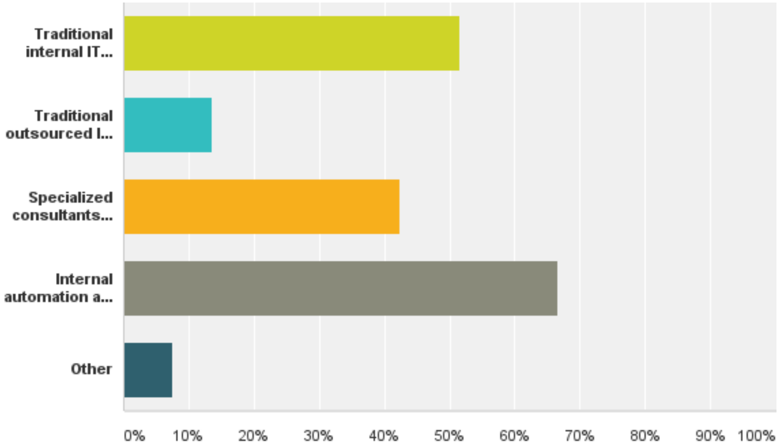


Figure 4 – Who Does Your Company Depend on to Help Secure Systems?

Risk Management

To assemble and operate an effective cybersecurity management system, it's essential to first assess the relative risk. The nature and degree of countermeasures employed must reflect this risk.

Although the web survey generated 70 responses, many answers to risk assessment-related questions were either left blank or indicated that company maturity was low. These answers are shown in the following table.

Table 6 – Survey Comments on Risk Management Methods

Response Comments
"No clear procedure for this"
"Not applicable"
"As per ISA99"
"Data loss and confidentiality"
"Risk matrix to quantify risk"
"Probability versus impact"
"... risk matrix of 'likelihood' versus 'consequences' on all potential threat vectors with ICS cybersecurity categorized as a Business Continuity and Reputation risk."

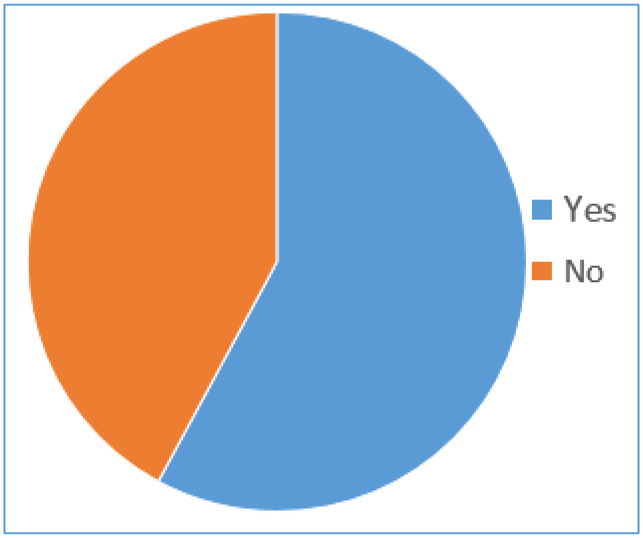
Based on the responses to the general web survey and the subsequent, more detailed company interviews it is clear that there is a general lack of clarity and understanding on how to evaluate rick and what criteria should be used to guide decisions.

Generally, Oil and Gas companies rely on the automation suppliers or system integrator to apply the appropriate protection measures for networks. Some more mature companies are looking to the developing ISA/IEC 62443 series of standards to address this. Within that series, the ISA/IEC-62443-3-2 standard (Security Risk Assessment and System Design) will soon be issued for committee review and comment.

A small set of companies have begun to link cybersecurity and safety, applying the principles of HAZOP, process safety, and plant risk to ICS systems. For MOM applications, most companies followed the typical IT or enterprise risk management approaches by analyzing MOM with other business applications. The one exception was that if a particular MOM system was pushing data down to ICS, that system would be included in the process safety analysis.

Remote Support

Survey responses also showed that the majority of owner operators leverage remote support for industrial control systems. The trend for industrial control and automation systems is more complexity and require a capability that is beyond the level of support for organizations in the plant. External maintenance and support is required to maintain effectiveness of the systems. The Oil & Gas, Refining and Petro-chemical industries were not significantly different than the overall industry segmentation.



Does you company support Remote Access to Industrial Control Networks?

Appendix A: Web Survey

The initial data for this study was collected in the form of a web survey titled, "Best Practices for the Industrial Control System (ICS) and MOM Network."

Survey Questions

The survey contained a total of fifteen questions. In most cases, specific response options were provided, but in some cases, respondents had the option to provide comments.

The questions involved information about the individual respondents, their security programs and risk assessment criteria/approaches, and miscellaneous questions about ICS security and related standards.

Respondent Information

1. Are you an end user, supplier, or involved in the industry in another capacity?
   - End User
   - Supplier
   - OEM/Rep
   - Engineering Firm/Systems Integrator
   - Education
   - Consultant

2. What is your primary industry?
   - Upstream or Midstream Oil and Gas
   - Refining
   - Petrochemical
   - Power Generation
   - Chemical
   - Water and Wastewater
   - Life Sciences
   - Food and Beverage
   - Cement and Glass
   - Other (please specify)

3. What region are you located in?
    - North America
    - Brazil
    - Latin America
    - Europe
    - Russia
    - Middle East
    - China
    - India
    - Japan
    - Rest of Asia
    - Other (please specify)

Security Program Information

4. Describe the elements of your ICS security architecture controls and program
    - Rigorous patch management
    - Network segmentation
    - Authentication diversity
    - Application Control or White-listing
    - Security information and event management (SIEM)
    - Intrusion detection systems
    - Other (, please specify)
5. Please describe security design methodology for ICS networks
    - Designed by System Integrator, or Automation or Application Provider
    - Implemented by in-house Automation and Engineering staff.
    - Implemented by in-house Automation and Engineering staff in conjunction with Enterprise or Corp IT
    - Other (, please specify)

6. Plant Manufacturing Operations and Production Management applications are part of which network layer (Check only one that best fits your architecture)
    - Supervisory network level 3
    - DMZ network level 3.5
    - Corporate Network or business LAN / WAN
    - Other (please specify)

7. Does your security architecture permit unidirectional data flow between Manufacturing Operations Management/Production Management and lower level control networks?
   - Unidirectional data flow between MOM and Level 2 Automation layers.
   - Bidirectional data flow between MOM and Level 2 Automation layers.
   - No data flow between MOM and Level 2 Automation layers
   - Other (please specify)

8. In regards to data or traffic flows between ICS and other networks, what access controls are in place to manage this?
   - Firewall with basic rules managed by internal staff
   - Firewall with basic rules managed by external security provider
   - Firewall with Stateful packet inspection (SPI - Analyze the packet header and footer to validate the session)
   - Firewall with Deep Packet Inspection (DPI - Analyze the full data part and content of the packet)
   - Digital or Data Diode Appliance
   - Air Gap and no connection between networks.
   - Air Gap and Sneaker-net connection
   - Other (please specify)

9. In addition to technology, what work processes are used to help maintain network security?

Risk Assessment

10. How do you evaluate risk to determine the appropriate level of security controls to protect ICS systems?

11. What risk criteria are used to determine the levels of ICS network protection?

12. What risk criteria are used to determine the levels of MOM network protection?

Miscellaneous

13. Who does your company depend on to help secure its systems?
    - Traditional internal IT departments
    - Traditional outsourced IT Departments
    - Specialized consultants with OT backgrounds
    - Internal automation and plant engineering
    - Other

14. Does your company support remote access to industrial control networks?

15. What standards are utilized to deploy ICS and industrial application software and solutions at your facility?

Appendix B: Interview Methodology

ARC conducted each of the confidential interviews using a common interview guide. This consisted of several questions grouped into specific categories corresponding to the major areas of interest for the study.

Organization

1. What are the number of sites for your company? (The assumption is that a single site may include multiple plants or operating facilities)

2. Do you have a central organization responsible for standards and governance? (Typical examples include central engineering or IT)

3. How do you ensure compliance?

4. Are industry standards used to guide internal standards? (If so, please cite specific examples)

Network Security Architecture

5. How would you describe your security architecture and the organizing of your networks that support MOM and ICS?

6. When considering the ISA-95 reference model (levels 1 through 4), on which level does MOM typically reside?

7. When considering the ISA-95 reference model (levels 1 through 4), on which level does Advanced Process Control (APC) typically reside?

8. At which level(s) are other plant operational applications typically deployed? Please describe your applications.

Risk Management

9. What risk assessment criteria are used to determine layers of protection or security for the ICS elements of the industrial network?

10. What risk assessment criteria are used to determine layers of protection or security for the MOM elements of the industrial network?

11. What are tolerable risks for ICS and MOM?

Data Flows and Architecture

12. Does your typical configuration support bidirectional data flow between levels 2 and 3 of the reference model?

13. Does your typical configuration support bidirectional data flow between levels 3 and 4 of the reference model?

Network Protection and Security

14. What technologies are used to protect access to networks?
    - Firewall?
    - F/W Stateful packet inspection?
    - F/W Deep Packet Inspection?
    - Air Gap only
    - Data Diode
    - Unidirectional Gateway (with Database replication)

15. What issues have you encountered in implementing network security?

16. Is the design of network security outsourced?

17. Is the operation and monitoring of network security outsourced?

Appendix C: Abbreviations

The following abbreviations may be used in this document.

ACL	Access Control List
APC	Advanced Process Control
APS	Advanced Process System
CMM	Collaborative Manufacturing Management
COTS	Commercial Off-the-Shelf
CPAS	Collaborative Process Automation System
CPI	Chemical Process Industry
CPM	Collaborative Production Management
DAS	Data Acquisition System
DCS	Distributed Control System
DPI	Deep Packet Inspection
DMZ	Demilitarized Zone
GUI	Graphical User Interface
HSE	High-Speed Ethernet
I/O	Input Output
IA	Industrial Automation
IEC	International Electrotechnical Commission
IP	Internet Protocol OR Intellectual Property
ISA	International Society for Automation
IT	Information Technology
LAN	Local Area Network
LIMS	Laboratory Information Management System
MAN	Metropolitan Area Network
MES	Manufacturing Execution System
MPC	Multivariable Predictive Control
MOC	Management of Change
MOM	Manufacturing Operations Management
MRO	Maintenance, Repair & Operations
NIST	National Institute of Standards and Technology
OI	Operator Interface
OM	Operations Management
OpX	Operational Excellence
OS	Operating System
OT	Operational Technology
PAM	Plant Asset Management
PAN	Plant Automation Network

PAS	Process Automation System
PCS	Process Control System
PCS	Process/Plant Control System
PIM	Plant Information Management
PIMS	Process Information Management System
PLC	Programmable Logic Controller
PP	Production Planning
QM	Quality Management
ROI	Return on Investment
RTO	Real-time Optimization
SCADA	Supervisory Control and Data Acquisition
SI	Systems Integrator
SIS	Safety Instrumented System
SPC	Statistical Process Control
SQC	Statistical Quality Control
SQL	Structured Query Language
TCO	Total Cost of Ownership
TCP/IP	Transmission Control Protocol / Internet Protocol
USB	Universal Serial Bus
VAN	Value Added Network
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network