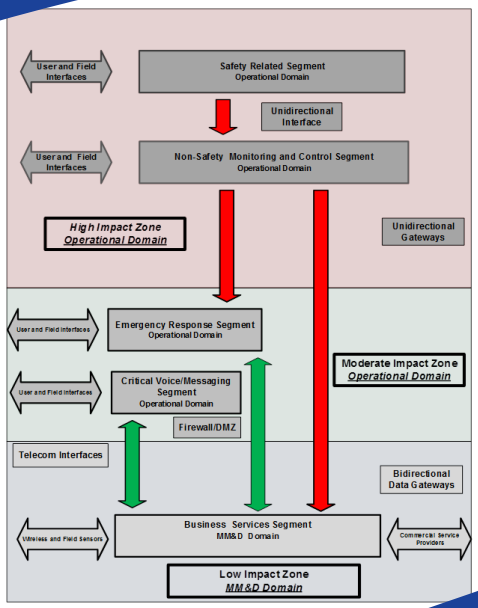
EPRI | ELECTRIC POWER RESEARCH INSTITUTE

2016 TECHNICAL REPORT

Cyber Security

Isolation for Maintenance, Monitoring, and Diagnostic Applications in Nuclear Power Facilities



Cyber Security

Isolation for Maintenance, Monitoring, and Diagnostic Applications in Nuclear Power Facilities

3002008206

Final Report, November 2016

EPRI Project Manager
M. Gibson

All or a portion of the requirements of the EPRI Nuclear Quality Assurance Program apply to this product.

YES  NO

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(S) 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(S) 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 ELECTRIC POWER RESEARCH INSTITUTE (EPRI) PREPARED THIS REPORT.

THE TECHNICAL CONTENTS OF THIS PRODUCT WERE **NOT** PREPARED IN ACCORDANCE WITH THE EPRI QUALITY PROGRAM MANUAL THAT FULFILLS THE REQUIREMENTS OF 10 CFR 50, APPENDIX B. THIS PRODUCT IS **NOT** SUBJECT TO THE REQUIREMENTS OF 10 CFR PART 21.

NOTE

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

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI) prepared this report.

Principal Investigator
M. Gibson

The following personnel provided input and content review:

- Michael Thow – EPRI
- Bradley Yeates – Southern Company
- Robert Austin III – EPRI

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

Cyber Security: Isolation for Maintenance, Monitoring, and Diagnostic Applications in Nuclear Power Facilities. EPRI, Palo Alto, CA: 2016. 3002008206.

PRODUCT DESCRIPTION

Power generating facilities face competitive pressures that require their owners and operators to achieve the highest levels of process and operational efficiencies in order to continue safe and effective operations. As with nearly all others industries, power generation can and should leverage sensor, communications, and computer technology to affect these efficiencies. While there are numerous technical, organizational, and business objectives that must also be considered, the complexity and uncertainty of cyber security considerations are having limiting effects which are slowing a more widespread integration of cyber technology within the power generation sector.

Objectives

To assist in mitigating these limiting effects, this report will present several segregation and segmentation concepts and techniques that can be utilized by site and fleet cyber security, engineering, and information technology support personnel. These concepts and techniques guide the crafting of data flows with characteristics that achieve the data isolation objectives and ensures the integrity of data and control actions.

Approach

To create a meaningful framework to describe and implement a cyber security isolation strategy, it is useful to divide plant functions into the smallest number of isolation domains that still allow key power production and support activities to take place in an efficient manner. To achieve this, the assets and organizations of a nuclear power plant have been divided into two functionally defined isolation domains:

- Operational Domain
- Maintenance, Monitoring, and Diagnostic (MM&D) Domain

These two domains are a natural legal and technical division as a result of the functional scope of the various regulations and the technical good practice of dividing up a system or organization into domains of like function and criticality.

Results

To achieve our isolation objectives, three types of isolation techniques address the most common use cases when isolating the Operational Domain from the MM&D Domain:

Communications Isolation: Data parameters are transmitted from the Operational Domain to the MM&D Domain through boundary devices or methods.

- Accomplished via unidirectional methods such as analog interfaces and one-way techniques.
- Allows for shared sensors/data sources and shared pre-filtering and analysis.
- No direct functional or organizational feedback loops exist that can affect Operational Domain functions.

Functional Isolation: Data is collected directly by sensors and equipment dedicated to the MM&D Domain.

- Accomplished by using dedicated sensors and data sources for the MM&D Domain
- No shared data sources
- Electrically and logically isolated
- No data connectivity
- No direct communications or organizational feedback loops exist that can affect Operational Domain functions

Organizational Isolation: Data from the MM&D Domain is isolated from all Operational Domain usage via administrative and engineering controls

- Unevaluated and unqualified data from the MM&D Domain is blocked from usage in the Operational Domain by shaping Operational Domain task requirements to preclude that inappropriate use
- No direct communications or functional feedback loops exist that can affect Operational Domain functions

These isolation techniques can be used singly or in combination to provide an interface between the Operational Domain and the MM&D Domain that will ensure that data is used at the appropriate criticality level. It also ensures that lower criticality data sources, which have less verification and integrity, do not endanger the functional integrity of higher criticality data sources.

Application, Value, and Use

This report can be used by design engineers, cyber security specialist, and information technology practitioners as an introduction to segmentation and segregation methods that can be used to overcome cyber security barriers to implement new and more effective monitoring and diagnostics methods. These concepts can reduce the cost of integrating sensor and communications technology by aligning the cyber security protection techniques to the appropriate levels of risk and criticality of the data paths being protected.

Keywords

Cyber security
Isolation
Segmentation
Segregation

Deliverable Number: 3002008206

Product Type: Technical Report

Product Title: Cyber Security: Isolation for Maintenance, Monitoring, and Diagnostic Applications in Nuclear Power Facilities

---

PRIMARY AUDIENCE: Fleet and Site Cyber Security Program Support Organizations

SECONDARY AUDIENCE: Fleet and Site Systems, Design Engineering, and Plant Monitoring Organizations

KEY RESEARCH QUESTION

Power generating facilities face competitive pressures that require their owners and operators to achieve the highest levels of process and operational efficiencies in order to continue safe and effective operations. These competitive pressures have exposed inefficiencies in the identification and integration of new technologies that have the potential to cut labor resources and reduce operational risk. As with nearly all others industries, power generation can and should leverage sensor, communications, and computer technology to affect these efficiencies. While there are numerous technical, organizational, and business objectives that must also be considered, the complexity and uncertainty of cyber security considerations are having limiting effects which are slowing a more widespread integration of cyber technology within the power generation sector.

RESEARCH OVERVIEW

To assist in mitigating these limiting effects, this report will present several segregation and segmentation concepts and techniques that can be utilized by site and fleet cyber security, engineering, and information technology support personnel. These concepts and techniques guide the crafting of data flows with characteristics that achieve the data and system isolation objectives which promote confidence in the integrity of critical data and control actions.

KEY FINDINGS

Traditional Information Systems design practices encourage functional consolidation (as opposed to segregation) in order to enhance programming efficiencies and simplify computer systems deployment. While these practices are desirable in some business scenarios, over consolidation is a key business and regulatory risk. Strategic design objectives should dictate how automating plant functions with critical safety and/or economic consequences can be accomplished efficiently. Primary consideration should be insuring functional independence of the critical operational objectives, which increases operational resiliency and enhances the ability to detect and respond to anomalies. To achieve our isolation objectives, two isolation domains are defined and three types of isolation techniques are identified to address the most common use cases when isolating the Operational Domain from the Maintenance, Monitoring, and Diagnostic (MM&D) Domain:

Communications Isolation: Data parameters are transmitted from the Operational Domain to the MM&D Domain through boundary devices or methods.

- Accomplished via unidirectional methods such as analog interfaces and one-way techniques.
- Allows for shared sensors/data sources and shared pre-filtering and analysis.
- No direct functional or organizational feedback loops exist that can affect Operational Domain functions.

Functional Isolation: Data is collected directly by sensors and equipment dedicated to the MM&D Domain.

- Accomplished by using dedicated sensors and data sources for the MM&D Domain
- No shared data sources
- Electrically and logically isolated
- No data connectivity
- No direct communications or organizational feedback loops exist that can affect Operational Domain functions

Organizational Isolation: Data from the MM&D Domain is isolated from all Operational Domain usage via administrative and engineering controls

- Unevaluated and unqualified data from the MM&D Domain is blocked from usage in the Operational Domain by shaping Operational Domain task requirements to preclude that inappropriate use
- No direct communications or functional feedback loops exist that can affect Operational Domain functions

These isolation techniques can be used singly or in combination to provide an interface between the Operational Domain and the MM&D Domain that will ensure that data is used at the appropriate criticality level. It also ensures that lower criticality data sources to not endanger the functional integrity of higher criticality data sources.

WHY THIS MATTERS

This research represents an initial look at techniques that can have immediate use in reducing the barriers presented by cyber security requirements that are hindering effective use of technology to reduce plant operation costs.

HOW TO APPLY RESULTS

The techniques presented here can be readily integrated into the engineering design and evaluation process as well as the Business IT review and implementation processes. This will allow these methods to be considered as early in the technology deployment process where they have the best chance of reducing uncertainty and cost.

EPRI CONTACTS: Matt Gibson, Principal Technical Leader, mgibson@epri.com
Michael Thow, Senior Technical Leader, mthow@epri.com

PROGRAM: 2016 Program 41.05.03 Instrumentation and Control Program

IMPLEMENTATION CATEGORY: Category 2 – Plant Optimization

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

CONTENTS

PRODUCT DESCRIPTION ..... **VI**

EXECUTIVE SUMMARY ..... **X**

1 **INTRODUCTION** **1-1**

Data Flow Model 1-1

Key Technologies 1-5

2 **ISOLATION CONCEPTS** **2-1**

Operational Domain 2-2

MM&D Domain 2-3

Isolation Model 2-3

Isolation Techniques 2-5

3 **COMMUNICATIONS ISOLATION** **3-1**

Unidirectional Gateways 3-1

Analog Interfaces 3-3

Turbine Monitoring Systems 3-4

Standalone PLC or Single Loop Controller 3-4

Highway Addressable Remote Transducer (HART) Protocol 3-5

4 **FUNCTIONAL ISOLATION** **4-1**

Advantages of Functional Isolation 4-2

Encapsulation for Functional Isolation 4-2

5 **ORGANIZATIONAL ISOLATION** **5-1**

6 **REFERENCES** **6-1**

References 6-1

LIST OF FIGURES

Figure 1-1 Basic Data Flow Model 1-1
Figure 2-1 Example Plant Wide Isolation Architecture 2-4
Figure 3-1 Unidirectional Interfaces 3-2
Figure 3-2 A Current loop Interface –How it Works 3-3
Figure 3-3 Turbine Monitoring Data [2] 3-4
Figure 3-4 Data from a Standalone PLC 3-5
Figure 4-1 Vibration Monitoring (Wireless configuration shown) 4-2
Figure 4-2 Fiber Optic Cable Profile 4-3
Figure 4-3 Fiber Backbone Segment Arrangements 4-3
Figure 4-4 DAS Isolation Techniques 4-4
Figure 5-1 Organizational Isolation Use Cases 5-2

LIST OF TABLES

Table 1-1 Example Primary Data Characteristics 1-2
Table 1-2 Example Traits of Propagation 1-3
Table 1-3 Example Data Destination Requirements 1-4

1
INTRODUCTION

Power generating facilities face competitive pressures that require their owners and operators to achieve the highest levels of process and operational efficiencies in order to continue safe and effective operations. As with nearly all others industries, power generation can and should leverage sensor, communications, and computer technology to affect these efficiencies. While there are numerous technical, organizational, and business objectives that must also be considered, the complexity and uncertainty of cyber security considerations are having limiting effects which are slowing a more widespread integration of cyber technology within the power generation sector.

To assist in mitigating these limiting effects, this report will present several segregation and segmentation concepts and techniques that can be utilized by site and fleet cyber security, engineering, and information technology support personnel. These concepts and techniques guide the crafting of data flows with characteristics that achieve the data isolation objectives and ensures the integrity of data and control actions.

Data Flow Model

We can conceptualize basic data flow as being comprised of one or more primary data sources, stages of propagation, and one or more data destinations. The primary data source represents the origin of data, which through procedural or other controls, is recognized as the official source.

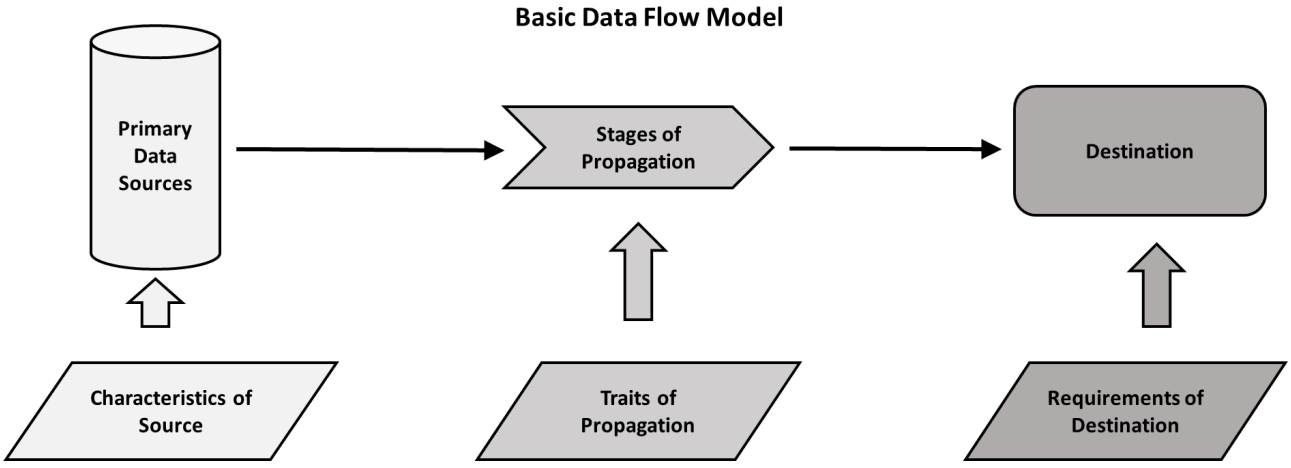


Figure 1-1
Basic Data Flow Model

The basic data flow model, Figure 1-1, illustrates the passage of data originating at the primary Source, passing through one or more stages of propagation as required, and coming to rest at one or more data destinations.

Primary data sources may be used to support a variety of business purposes. The primary data source may be a sensor or a software database. The primary data sources have properties that substantiate its integrity as well as properties that are associated with its performance. Table 1-1 illustrates the types of properties that must be considered and evaluated when designing and implementing the isolation techniques described later in this report. The isolation method chosen will be a key design input in primary data source selection and configuration.

Data from the primary data source may be propagated through one or more stages. Each stage of propagation has traits that enhance or diminish the degree of reliability of the data from the primary data source. Traits of propagation are evaluated and established to support the requirements of the data destination. As with the primary data source, the isolation techniques chosen will need to support the traits of propagation needed to ensure the data destination gets the data in the form and condition needed for the applications. Table 1-2 describes these traits. Each of the four main propagation trait categories can be dramatically affected by the conversion from analog to digital and back again as well as the various averaging, truncation, and rounding that may occur during transmission protocol manipulation.

The data destination is the intended representation of the data from the primary data source. The data destination has requirements that determine how the primary data source is used to support business processes.

Table 1-1
Example Primary Data Characteristics

Data characteristics	Description
Accuracy /Uncertainty	The measure of the possible difference between the apparent value and the true value
Availability	The amount of time the data is reachable
Bit resolution	In digital data this determines the resolution and is usually part of an Analog to Digital conversion specification. 12 bit = 4096 possible values. 16 bit = 65536 possible values.
Business Purpose	What aspect of commerce the data will be used to substantiate
Degree of Risk	The measure of how important the data is to nuclear safety, plant operation, or critical commerce
Calibration	An activity to compare and adjust a measured value to a more accurate standard. Determines accuracy of sensor data.
Compression	A data reduction technique that results in less data to represent more complex data. May, and usually does, result in some loss of fidelity and synchronization.
Convergence	To combine, merge, or blend data
Divergence	To separate into different data streams

Table 1-1 (continued)
Example Primary Data Characteristics

Data characteristics	Description
Format	Arrangement, order or layout of data
Precision	The mathematically granularity at which data is displayed or stored.
Refresh Rate/Scan Rate	The periodicity of data renewal or sampling rate of a sensor or input processor
Security	The limitations applied to protect data from accidental or deliberate alteration, destruction, or revelation. This includes cryptography techniques
Sensitivity	The degree of confidentiality required by the data destination
Testing Effects	Corruption of data values due to sensor calibration activities, troubleshooting activities, or other tests and experiments using artificial data
Units of Measure	The amount, degree, or quantity specified in pre-established terms or engineering units

Table 1-2
Example Traits of Propagation

Propagation Stages	Propagation Traits	Description
Convergence	Combining	Grouping of data together
	Linking	Connect two or more data types
	Collating	Assemble data in a specified manner
	Merging	The blending of data from multiple sources
Divergence	Separation	The extraction of data from a larger or more complex data set
	Splitting	The creation of two data streams with non-equal data from a larger data set
Filter	Averaging	The arithmetic mean, median, or mode of two or more data values
	Data Reduction	The processing of raw data that results in less physical data while attempting to approximate the original raw data set
	Grouping	Two or more data items related in some way treated as a unit
	Indexing	A data item that points to a particular item in a set
	Normalization	Reduce a data structure, relationship, or database to a simpler more stable form
	Sorting	Arrange items in a designated order
	Summing	The cumulative representation of data types, items, fields or values
	Cryptography	Encryption and Hashing to ensure integrity and confidentiality

Table 1-2 (continued)
Example Traits of Propagation

Propagation Stages	Propagation Traits	Description
Modification	Calculations	Perform mathematical functions on data
	Truncations	To remove one or more digits at the beginning or ending of a data representation
	Rounding	Delete or omit one or more of the least significant digits according to some specified rule
	Scaling	Adjust the representation of a quantity so that its value is brought within a specified range

Table 1-3
Example Data Destination Requirements

Data Destination Requirements	Description
Accuracy/Uncertainty	Degree to which a measured or recorded value represents the true value
Availability	The percentage of time data is reachable and usable
Business Purpose	What aspect of commerce the data will be used to substantiate
Compression	A data reduction technique that results in less data to represent more complex data. May and usually does result in some loss of fidelity and synchronization.
Convergence	To combine, merge, or blend data
Degree of Risk	The measure of how important the data is to nuclear safety, plant operation, or critical commerce
Display	The representation of Primary Source data in the format that best supports the business process
Divergence	To separate into separate data streams
Format	Arrangement, order or layout of data
Precision	The mathematically granularity at which data is displayed or stored.
Refresh Rate	The periodicity of data renewal
Scaling	The difference between the original Primary Data Source representation and resulting adjustment displayed in the Data Destination
Security	The limitations applied to protect data from accidental or malicious alteration, destruction, or revelation. This includes cryptography techniques
Sensitivity	The degree of confidentiality required by the Data Destination
Units of Measure	The amount, degree, or quantity specified in pre-established terms

This is usually where the data is used or "consumed." Evaluating the data destination properties in Table 1-3 against the incoming data after it has been collected and transmitted can help determine if it is adequate for the intended use. If the data destination requirements are equivalent to the characteristics of the primary data source, the traits of propagation must not individually, or as a group, detract from the integrity of the primary data source.

- If the data destination requirements are less rigorous than the characteristics of the primary data source, the traits of propagation may not individually or as a group allow the data quality to fall below the data destination requirements.
- If the data destination requirements are more than the characteristics of the aggregate of the primary data sources, the traits of propagation must collectively add control features that meet the data destination requirements. Good examples are encryption and integrity checking where they are added in the stages of propagation even though they do not exist at the source.

Key Technologies

Technologies being used or investigated for expansion that will rely on effective data flow security include:

- Wired and Wireless Sensors. These devices provide the data sources for the plant process and equipment condition parameters that are stored, trended, and analyzed to generate the business intelligence needed to affect efficiency improvements and cost reductions. These sensors are primary data sources.
- Data Analytics. This evolving data science is emerging as a key tool in understanding how plants actually work and the relationship between components and processes. Computationally and data intensive, data analytics will challenge utility practitioners to learn and effectively utilize this data science technique. This area primarily affects the propagation and transformation of data.
- Mobile Work Management. Worker mobility is currently thought to be a "must have" to enable owners and operators to craft new and improved work processes and business objectives that focus on:
  - Reducing the amount of wasted time transiting to and from the jobsite
  - Completing and documenting work activities
  - Obtaining accurate and current procedural and technical information
  - Allowing a real-time view of worker activity for planning and deployment purposes
  - Processed data as a key data destination and primary data source

Most regulatory requirements are based on functional criticality. 10CFR73.54 which governs cyber security at nuclear plants in the United States, NERC CIP cyber requirements which governs non-nuclear power generation assets in the North America, and IEC 62645, *Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems*, are all based on functional criticality. Isolating functions becomes key to partitioning critical equipment from non-critical equipment and becomes an effective method to manage both technical cyber risk and regulatory risk.

The need for improved Maintenance, Monitoring, and Diagnostics Technology to reduce plant operating cost will require that plant staff understand and make use of data flow models and data flow analysis to understand how best to deploy specific technologies. The following discussion of segmentation and segregation is informed by the data flow concepts described above to achieve the appropriate level data integrity, availability, and functional assurance.

2
ISOLATION CONCEPTS

The separation of functions is a well understood component of business, legal, security and safety architectures. Indeed, separation of function has been used for millennia to ensure that organization and political entities did not achieve such power as to endanger the integrity and future existence of the polity. One such instance is the United States Constitution with its separation of power between the Executive, Legislative, and Judicial branches. Businesses, likewise, use separation of function as an internal control to reduce fraud, corruption, and other threats to protect their integrity and continued existence [1]. This is why managers cannot approve an expense that directly benefits them. Well known corporate governance law such as Sarbanes-Oxley emphasizes the use of separation of function as a key governance tool.

In information technology, separation of function is often described in terms of network segregation or application partitioning. Mainframe computers use segmentation to create virtual areas within their memory address space that are protected from each other and the underlying operating systems use hardware enforced segmentation techniques. Network segmentations are described in numerous network hardening guides and policy documents. Virtual Local Area Networks (VLAN), Virtual Private Networks (VPN), router and firewall based physical network segregation, and hardware based unidirectional gateways are popular techniques. [3]
Within safety systems, separation of functions dictates that controls systems be isolated from protections systems. Such that the protection systems functions remain unimpaired. This isolation methods is well analyzed in existing plants. Even control systems are subjection to functional segmentation analysis to ensure that plant control functions are not inappropriately co-mingled and produce an unanalyzed plant condition when they malfunction.

Separation of function, therefore should be considered a basic concept that can be applied in many forms and within many different use cases to achieve the desired system and organizational isolation.

Key Information Point

Separation of Function is the concept of having critical organizational or systems functions divided from each other by technical or administrative controls such that no one compromise would result in a negative consequence beyond that in which a risk has been accepted for a desired benefit.

Various levels of isolation and independence can be achieved through the use of various segregation, separation, and segmentation techniques. These techniques can all be considered a means to achieve varying degrees of isolation or independence of function and for the purpose of this report “isolation” is used as a synonym for segregation, separation, segmentation, and independence.

While isolation in degrees has great benefit to system and organizational integrity, it is not without negative impacts. Isolation is in conflict with integration and today's technological systems have sought greater and greater levels of integration to achieve higher levels of cumulative functionality. This has resulted in a reduction in robustness and resiliency to both malicious attacks and non-malicious error and failures.

To create a meaningful framework to describe and implement a cyber security isolation strategy, it is useful to divide plant functions into the smallest number of isolation domains that still allow key plant power production and support activities to take place in an efficient manner.

To achieve this, we have divided the assets and organizations of a nuclear power plant into two functional domains:

- Operational Domain
- Maintenance, Monitoring, and Diagnostic (MM&D) Domain

These two domains are a natural division as a result of the technical good practice of dividing up a system or organization into domains of like function and criticality, including the functional scope of various regulatory requirements.

Operational Domain

The operational domain consists of those systems, equipment, data, and control methods that are used to directly control the plant either through automatic control or "operator in the middle" techniques. Operational domain systems and processes will have high levels of integrity, accuracy, and availability due to their use in real time to either directly control or inform the operator who will directly control the plant without further validation. The Operational Domain is also characterized as those systems and functions that are deemed critical through regulatory requirements. An example from U.S regulation is 10CFR73.54 which, based on function, compels the licensee to:

> "(1) The licensee shall protect digital computer and communication systems and networks associated with:
>
> (i) Safety-related and important-to-safety functions;
>
> (ii) Security functions;
>
> (iii) Emergency preparedness functions, including offsite communications; and
>
> (iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions."

As can be seen from this regulatory requirement, the designation of critical equipment is commonly based on function. Isolation by function is critical to integration of new technology at the correct functional criticality level. The Operational Domain includes these functions.

NERC-CIP and other standards and regulations have a similar approach to using criticality to define requirements.

MM&D Domain

The MM&D domain consists of those systems, equipment, data acquisition, analysis, and diagnostics methods that are used to evaluate plant performance, diagnose or predict plant malfunctions. The MM&D domain is characterized by systems and technology that are utilized through an engineering analysis and evaluation process and may involve unfiltered or uncalibrated data with varying degrees of accuracy, integrity, and completeness. Since the MM&D domain equipment is not used in real time, it does not have the high availability requirements of the operational domain. MM&D data is not directly used for Operational Domain actions until it has been evaluated for integrity, accuracy and completeness by engineering personnel.

Key Organizational Performance Point

The inherent conflict between isolation and integration must be balanced to achieve robust and resilient systems and organizations while still achieving meaningful and efficient benefits.

Isolation Model

A nuclear power plant can be divided into functional segments within the two isolation domains. These segments reflect further isolation between functions within a domain. Functions are not mixed unless they provide essential communications or integrated functions whose benefit outweighs the risk of interconnection.

Figure 2-1 illustrates and provides an example of how a nuclear power plant might be architected to have segments and domains divided by isolating boundaries and devices that enforce desired data flows and process integrity.

This isolation model provides a back drop for the primary discussion of techniques for isolation of the Operational Domain from the MM&D Domain. Each isolation technique has traits of propagation that shape the security and integrity of the data flow. Those traits must be analyzed and the most effective tradeoffs established in order to achieve the MM&D objectives of the design.

Isolation within domains will not be addressed in this report but are included in the isolation architecture for clarity.

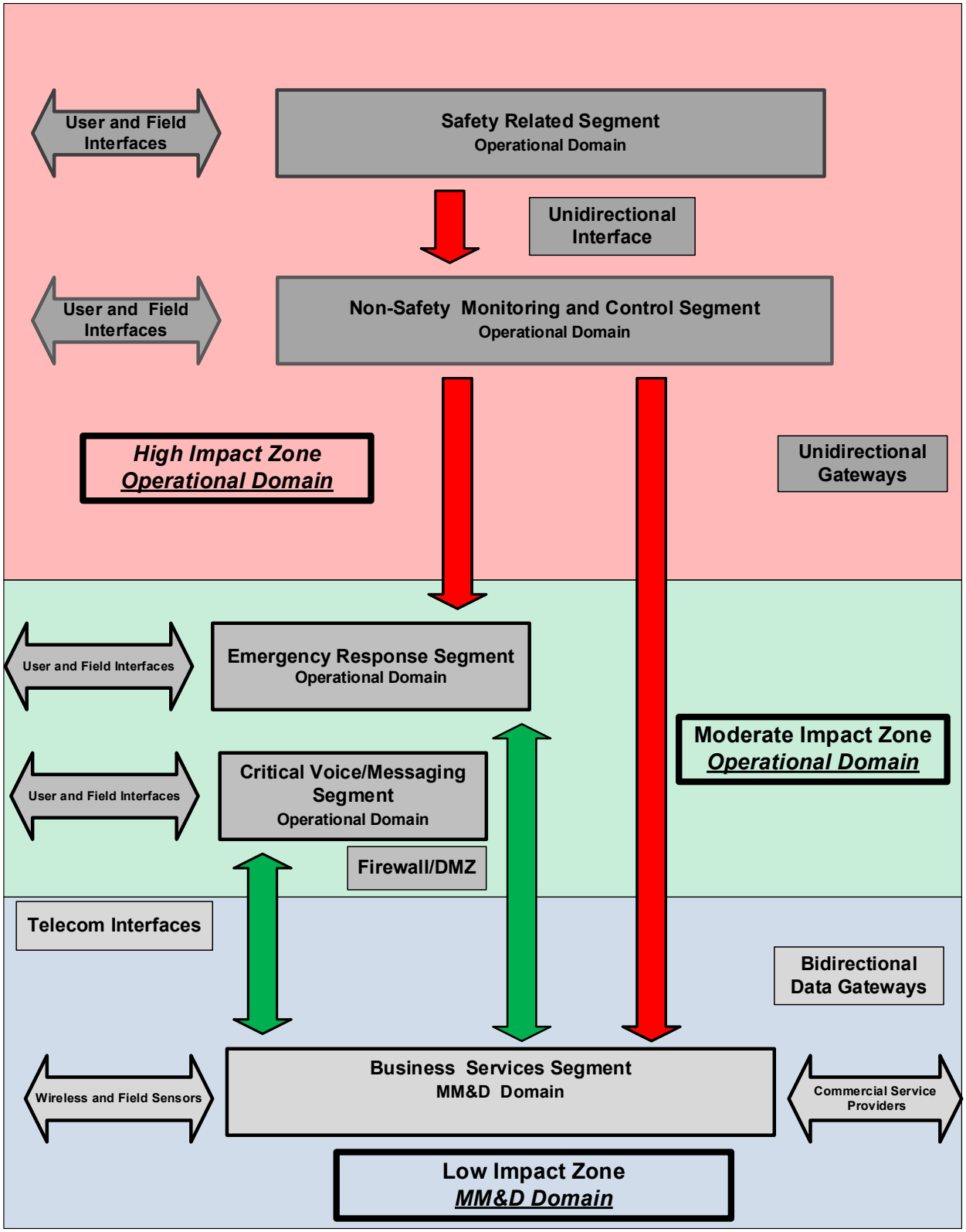


Figure 2-1
Example Plant Wide Isolation Architecture

Isolation Techniques

To achieve our isolation objectives, three type of isolation techniques have been identified to address the most common use cases:

- Communications Isolation: Data parameters are transmitted from the Operational Domain to the MM&D Domain through boundary devices or methods.
  - Accomplished via unidirectional methods such as analog interfaces and one-way techniques.
  - Allows for shared sensors/data sources and shared pre-filtering and analysis.
  - No direct functional or organizational feedback loops exist that can effect Operational Domain functions.
- Functional Isolation: Data is collected directly by sensors and equipment dedicated to the MM&D Domain.
  - Accomplished by using dedicated sensors and data sources for the MM&D Domain
  - No shared data sources
  - Electrically and logically isolated
  - No data connectivity
  - No direct communications or organizational feedback loops exist that can effect Operational Domain functions
- Organizational Isolation: Data from the MM&D Domain is isolated from all Operational Domain usage via administrative and engineering controls
  - Unevaluated and unqualified data from the MM&D Domain is blocked from usage in the Operational Domain by shaping Operational Domain task requirements to preclude that inappropriate use
  - No direct communications or functional feedback loops exist that can effect Operational Domain functions

Collectively, these isolation techniques can be used to provide an interface between the Operational Domain and the MM&D Domain that ensure that data is used at the appropriate criticality level. It also ensures that lower criticality data sources to not endanger the functional integrity of higher criticality data sources [4].

Organizational Isolation

While any given implementation will use either Communications Isolation or Functional Isolation to move data to the MM&D Domain. Organizational Isolation must always be considered and addressed.

3
COMMUNICATIONS ISOLATION

Communications isolation describes the techniques used to ensure that as data is transmitted between domains there are no feedback mechanisms that would affect the integrity of the operational domain. Interfaces must be constrained to transmit only the minimum allowed data, data management elements, and nothing else. Communications isolation allows the collection the large amounts of Operational Domain data and monitoring information to be transmitted safely to the MM&D Domain for further analysis and aggregation with additional MM&D data.

While isolation techniques can be used with the Operational Domain to segregate core critical segments from less critical segments, this report concentrates on the boundary between the Operational Domain and the MM&D Domain.

Communications Isolation: Common data parameters are transmitted from the Operational Domain to the MM&D Domain through boundary devices or methods.

- Accomplished via unidirectional methods such as analog interfaces and data diodes.
- Allows for shared sensors/data sources and shared pre-filtering and analysis.
- No direct functional or organizational feedback loops exist that can effect Operational functions.

On the Operational Domain side, common primary data sources include the plant process computer and similar operator aide applications that acquire, process, control, and display information and control results to the main control room operator using high integrity and validated data sources. Various data acquisition systems and plant wide distributed control systems (DCS) are also included in the Operational Domain. Essentially, primary data sources that implement control and/or monitoring that is used for direct or "Operator in the Loop" decision making is in the Operational Domain and represents an important collective source of data that can be transmitted to the MM&D domain via an isolated communications interface.

Data parameters gathered on the Operational Domain side but intended only for transmission and use in the MM&D domain will have to meet the integrity, accuracy, and upkeep requirements of the Operational Domain since they cannot be reliably isolated for Operational Domain organizational use.

Many technologies and monitoring strategies will benefit from using Functional Isolation (discussed later) vs. integration with the Operational Domain and transmission through isolated communications interfaces.

Unidirectional Gateways

A popular digital (binary) interface that achieves excellent isolation is the hardware enforced unidirectional gateway. Commonly called "data diodes" to describe the one-way aspect of data

flow, these devices utilize a transmission channel that is physically implemented such that there is no method to transmit in the prohibited direction. For example, an optical transmitter is used on one end and an optical receiver is used on the other end so that only data flow in one direction is possible. Depending on the brand and model of gateway, the transmitter and receiver can be separated over a considerable distance of fiber optic cable to ensure that malicious bypasses are prevented. Hardware enforcement is a key attribute of this gateway as using hardware eliminates the software attack surface of typical routes or firewalls and guarantees deterministic behavior.

Unidirectional gateways primarily implement wired Ethernet speed and protocols by using blind proxies on each end that interface with the primary sending source and the receiving destination. These blind proxies simulate bidirectional flow and session acknowledgements as well as some application level handshaking to give the appearance that bidirectional communication is taking place.

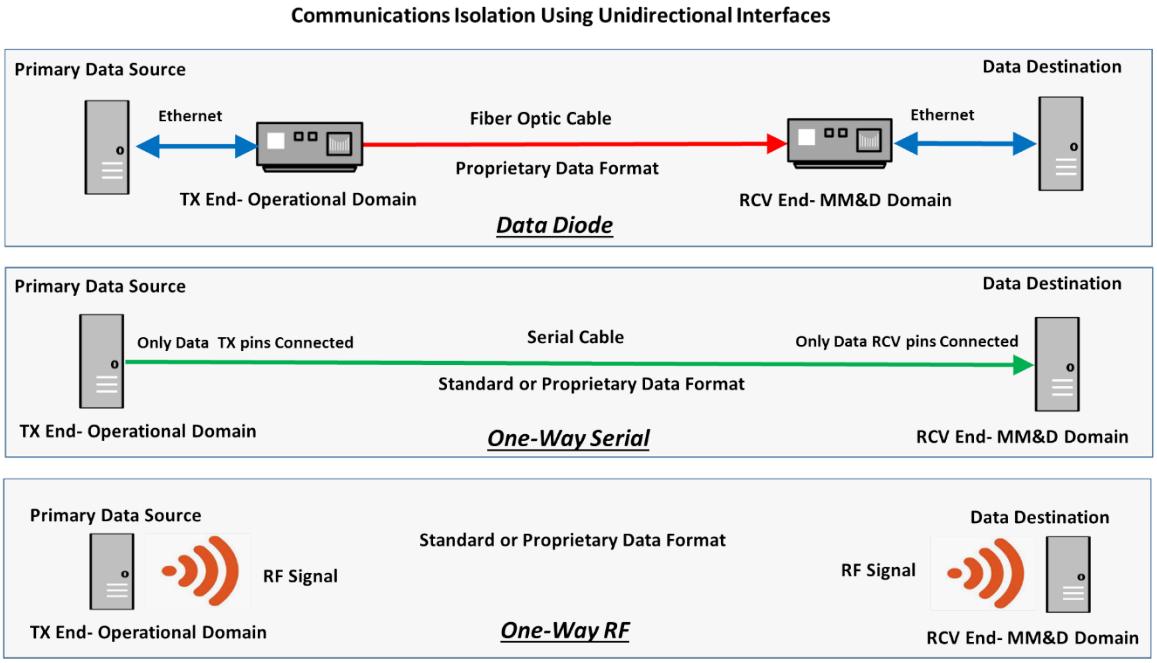


Figure 3-1
Unidirectional Interfaces

Less sophisticated gateways can be implemented by use of a single transmit-to-receive pin connection using a serial RS-232/RS-422 physical layer communication. Control pins should not be connected to prevent any feedback loops. The elimination of flow control signals provides a similar level of digital isolation as an optical data diode. This configuration will have less electrical isolation, but that may not be a consideration. An appropriate protocol must be selected or engineered that will work over a one-way data path.

Although not yet commonly used for security isolation, transmit only RF (wireless) interfaces can also be used in the same manner as Ethernet or serial unidirectional gateways. A transmit only primary source device broadcasts digital data to be picked up by receive only gateway(s) that pass the information to a final destination. Unidirectional RF broadcasts have a long history of reliable use and provide excellent isolation for the sending device, as no physical connection is present. Public digital TV, HD radio, and satellite radio are good examples of this technique.

They are particularly useful for one-to-many data flows, and with encryption can enforce confidentiality when needed. See Figure 3-1.

Key Technical Point

EMI/RFI is a consideration with RF technologies. Modern equipment should be able to achieve effective unidirectional broadcast transmissions without undue risk of interference or unintended affects. Analysis will likely be required using current guidance documents. EPRI 30020000528, *Guidelines for Electromagnetic Compatibility Testing of Power Plant Equipment: Revision 4 to TR-102323*, is a good source for EMI/RFI requirements

Analog Interfaces

Analog interfaces are also an effective communications isolation technique due to the inherent physics of their construction. These interfaces have been used for many decades to communicate data values in industrial and equipment applications. Analog interfaces use a voltage or current level to represent a data parameter and transmit that from a primary source to one or more destinations. This is where the term "Instrument Transmitter" originates.

The most popular, widespread, and standardized analog interface is the 4-20ma. This interface takes advantage of the inherent physics of Ohms law that states the current (I) in an electrical circuit is equal to the voltage (V) divided by the resistance(R) or I=V/R. Physics also defines that this current is equal at all locations in a series resistive circuit. The 4-20ma interface takes advantage of this by forcing the current to be proportional to the sensed or selected data parameter while manipulating the voltage to adjust for resistance difference. The current is typically dropped across a 250 ohm resister to generate 1-5V DC to interface to connected equipment.

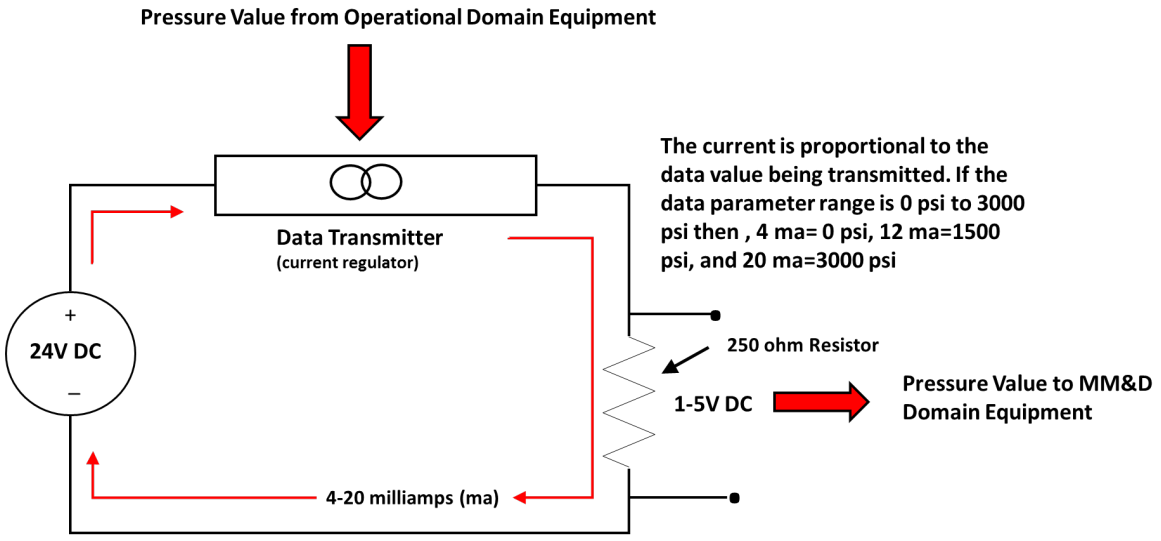


Figure 3-2
A Current loop Interface –How it Works

You will also occasionally see 10-50ma circuits and various voltage ranges in older equipment. These work the same way as 4-20ma loops. There are many other types of analog interface that do not use a current loop but in a similar fashion use proportional voltages to represent data values. This is common on interfaces used for moving machinery like vibration, shaft position, and RPM. Some of these interfaces, like vibration, generate a complete analog waveform for use by analytical equipment. Plant power bus monitoring equipment uses similar waveform techniques. These analog interfaces collectively can be used to get a data from the Operational Domain to the MM&D domain with high degrees of communication isolation. Analog interfaces can be used to interface the Operational Domain to the MM&D Domain for many data interfaces that have a relatively few data parameters. Some examples include:

Turbine Monitoring Systems

Turbine Monitoring Systems often need to provide data analytic software in the MM&D domain that are difficult or costly to transmit otherwise. By mirroring or "buffering" the native analog sensor interfaces to input hardware in the MM&D domain, this key operational data can be securely transferred. This includes waveform and proportional voltage sensor data. The buffer interfaces are unidirectional and have no data return path.

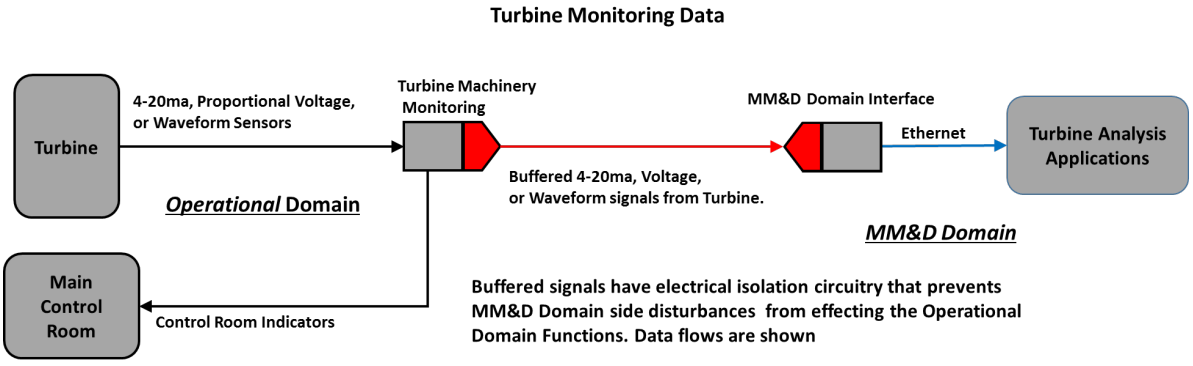


Figure 3-3
Turbine Monitoring Data [2]

Standalone PLC or Single Loop Controller

In legacy plants there are many installations of sub-systems or single loop controllers that are not connected to networks within the Operational Domain. This standalone equipment can have valuable monitoring and diagnostic data that could be used to improve plant operation. While the equipment could be added to the network, this can present integration and interface challenges, especially if only diagnostic data is being pursued. An alternate solution would be to use analog interfaces to transfer the seletced data parameters to the MM&D Domain. This will typically be 4-20 ma analog interfaces that then connect to the plant historian in the MM&D domain.

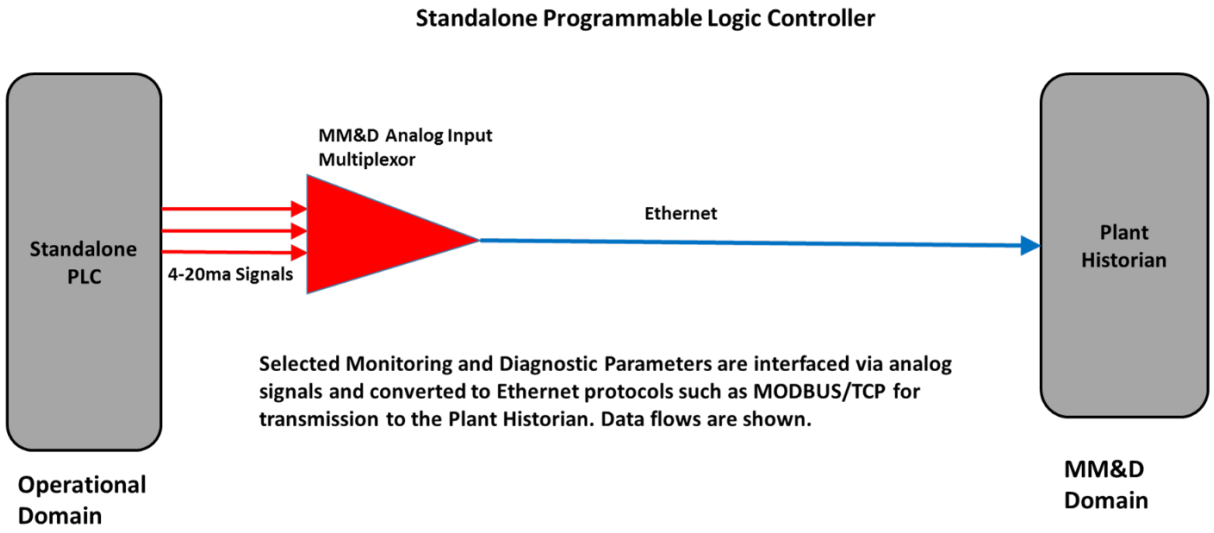


Figure 3-4
Data from a Standalone PLC

Highway Addressable Remote Transducer (HART) Protocol

Many modern implementations of the 4-20ma interface also include the HART protocol. The HART protocol has seen widespread use as configuration and monitoring protocol for industrial devices. It implements a Frequency Shift Keying (FSK) modulation which is electrically independent of the 4-20ma current loop. Because it is a bi-directional digital communications interface it cannot be used on the Operational Domain side in conjunction with an analog interface isolation scheme. If present, it must be permanently disabled or blocked with HART filters so that it does not leave the Operational Domain.

It may be used, however, with Functional Isolation along with other digital communications protocols as it is always on the MM&D Domain side in functional isolation schemes.

4
FUNCTIONAL ISOLATION

Functional Isolation employs a complete separation of equipment and data paths. Data is collected directly by sensors and equipment dedicated to the MM&D domain with no shared electronics or sensor elements. Isolation verification is simple and straight forward because there are no shared components nor interconnections with other digital components; there just is not much to evaluate.

Functional Isolation: Data is collected directly by sensors and equipment dedicated to the MM&D domain.

- Accomplished by using dedicated sensors and data sources for the MM&D domain
- No shared data sources
- Electrically and logically isolated
- No data connectivity
- No direct communications or organizational feedback loops exist that can effect Operational functions

With functional isolation, sensors are mounted directly on piping, equipment, and the sensors directly measure the variables. This usually results in some type of mechanical coupling. These sensors are mechanically attached to the equipment being monitored. They can be attached with various mechanical attachment methods including threaded wells or various flanges and bolts. For wireless sensors, magnetic attachment is also common. Each of these attachment methods provide isolation from the Operational Domain; the sensor resides in the MM&D Domain allowing the component to be monitored and diagnosed.

Dedicated vibration monitoring sensors, thermocouples, Resistance Temperature Detectors (RTD), and even dedicated instrument transmitters can be used for data acquisition. Sensor interfaces can be wired or wireless. In the case of wired sensors, the wiring is physically isolated from Operational Domain wiring and data functions. For sensors that use RF or optical communications, they communicate directly with the MM&D communications network and are physically and logically separated and from Operational Domain equipment.

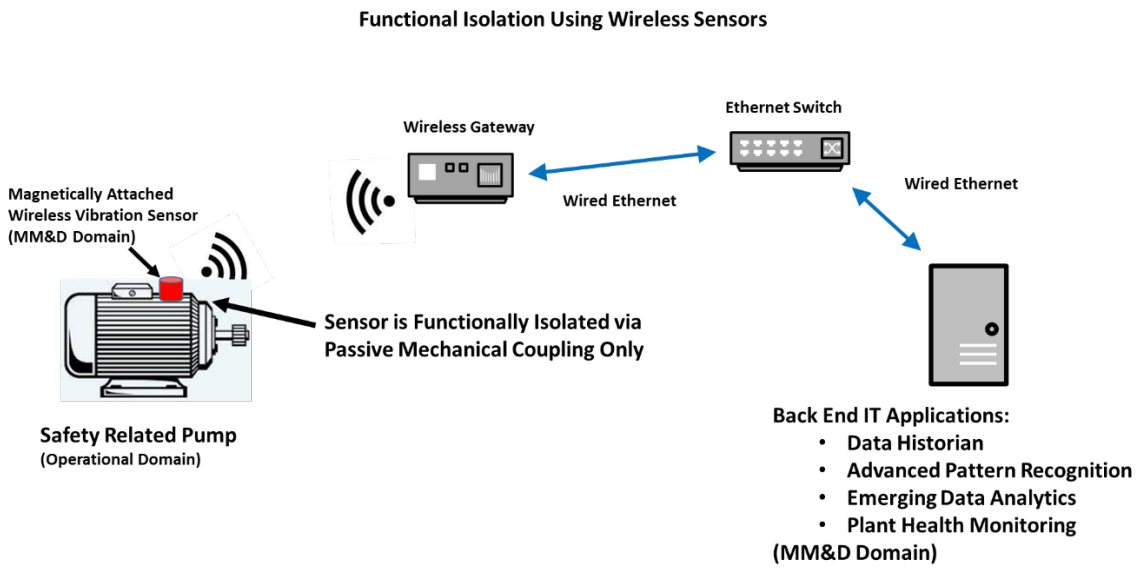


Figure 4-1
Vibration Monitoring (Wireless configuration shown)

An example that applies to both wired and wireless scenarios is vibration monitoring (see Figure 4-1). A vibration sensor attached to the target component interfaces via a wired or wireless connection to the MM&D Domain. This dedicated MM&D Domain specific sensor is functionally isolated from any control, communications, or electrical aspects of the critical component (the pump motor) which remain undisturbed. This example shows functional isolation.

The choice of wired or wireless will depend on many local variables such as sampling frequency, data type and quantity being sampled, and availability of local power sources. This architecture can be applied to a wide variety of MM&D data acquisition scenarios.

Advantages of Functional Isolation

As nuclear facilities seek to expand their monitoring capability, functional isolation provides a means to reduce the stress and analysis associated with assessing cyber security vulnerabilities to meet regulatory and generation risk. By having a direct link to the MM&D Domain, the cyber security risks and mitigation can be evaluated consistent with the utility's business network security policies.

Encapsulation for Functional Isolation

Encapsulation can provide efficiencies in plant implementations by allowing systems and physical infrastructures to host less critical data sources within a more critical data path. This is accomplished by some form of channelization or other isolation method within the systems structure. This technique can lead to very high efficiencies in plant optical cabling and can be a key enabler in the expansion of senor networks and monitoring strategies within existing plants.

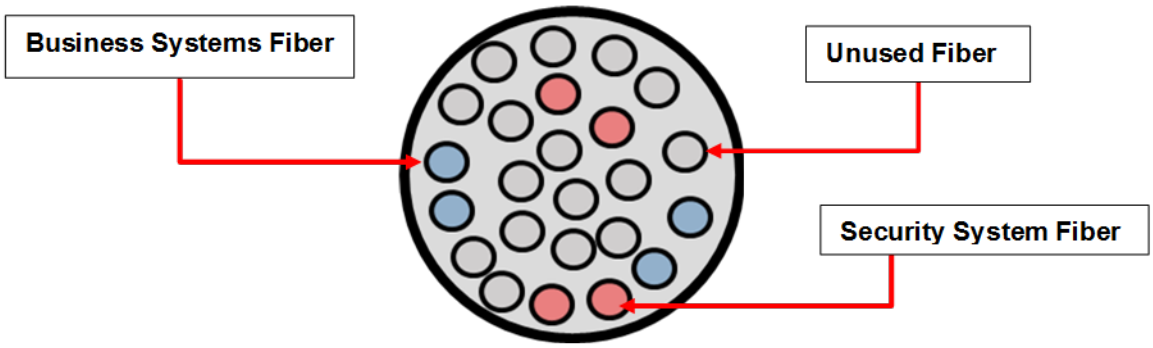


Figure 4-2
Fiber Optic Cable Profile

A good example of encapsulation is in the efficient optimization of existing site fiber optic cabling and the use or installation of multi-use fiber optic backbones. Such installations typically use multiple single core fiber cable with each having its own buffer or sheath within a single multi-fiber cable that can be only 8 to 12mm in diameter.

Each fiber in these multi-fiber cables are electrically and optically isolated from one another other by the cladding and sheath material. The cables are designed for such isolation as each fiber is intended to carry optical communications independent from any other fiber in the multi-fiber cable. The example shown in Figure 4-2 illustrates how business fiber on the MM&D domain can be mixed in the same multi-fiber cable as fiber to support the security functions in the Operational Domain while still remaining isolated from each other.

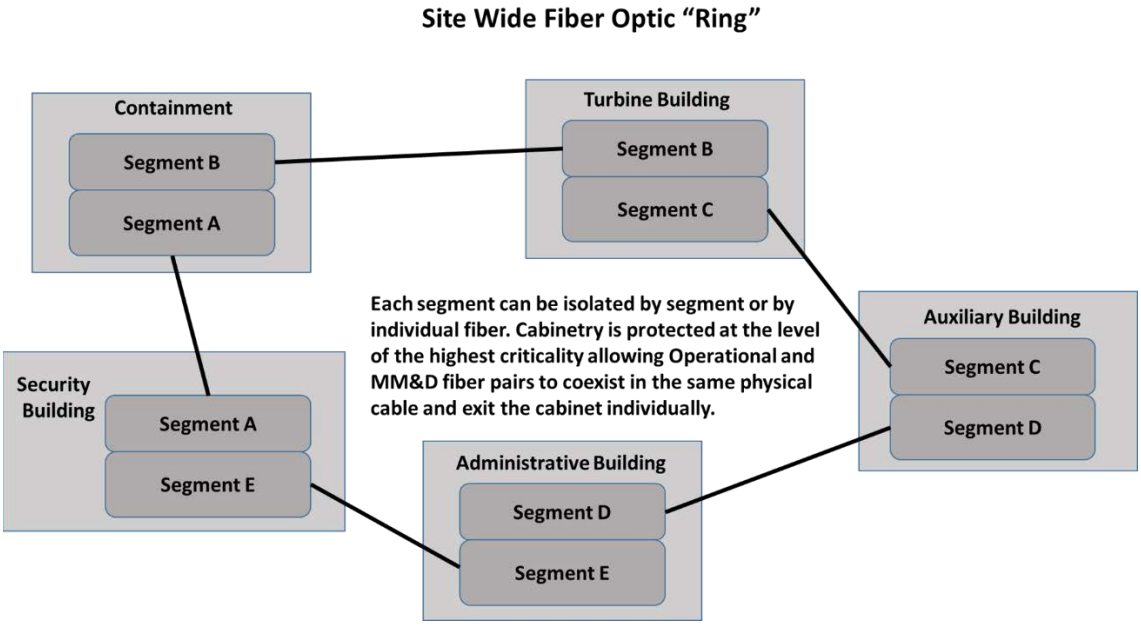


Figure 4-3
Fiber Backbone Segment Arrangements

Functional Isolation

The key technique in implementing optical cable encapsulation is to ensure a secure and isolated exit from the cable infrastructure for each fiber depending on the targeted domain. This is done by extending lower criticality (MM&D Domain) fiber through a high criticality cabinet (Operational Domain) so that it can be interconnected to MM&D equipment while remaining isolated from the Operational Domain.

Another example of encapsulation to achieve Functional Isolation is an analog Distributed Antenna System (DAS). In this example, the DAS carries various RF frequencies and they are being distributed through both optical and metallic RF cables. Every RF signal is at a different frequency and isolation is achieved by a frequency separation that is wide enough to avoid interference and eavesdropping between frequency bands. This makes the isolation equivalent to RF in open air.

For the optical segments, the RF frequencies are used to modulate the optical signal such that there is an optical frequency for each RF frequency. This provides frequency based separation and isolation equivalent to the source RF frequencies in open air.

For the metallic cable segments, the RF frequencies are transmitted using RF independent modules. This provides frequency based separation and isolation equivalent to the source RF frequencies in open air.

Most DAS technologies, including those that use analog modulation techniques, have a software based subsystem that is used to configure the system and perform diagnostics. The DAS software based configuration and health monitoring functions would be protected at the level of the highest criticality while the lower criticality signals would be hosted by the DAS and enter and exit the system without effecting the security of the higher criticality signals.

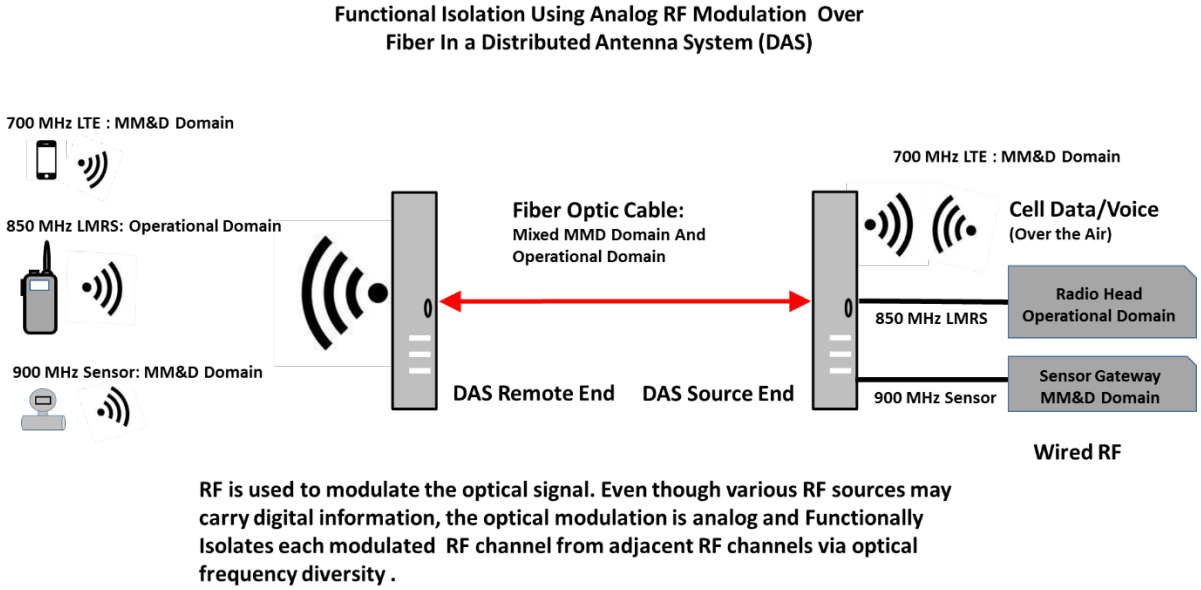


Figure 4-4
DAS Isolation Techniques

5
ORGANIZATIONAL ISOLATION

The last isolation technique is Organizational Isolation. Organizational Isolation is based on long standing concepts in Human Factors and Organizational engineering that include task and functional allocations of duties. Task and functional allocation allows a person to evaluate the type and quality of data (inputs) required and execute an allocated task or function. Think of it as a process to design human activities that support specific organizational or system functions. Allocations can be thought of as Human vs. Machine, Machine vs. Machine, or Human vs. Human. The Operational Domain allocates certain tasks and functions that depend on having data and control mechanisms that meet specific criteria such as latency, accuracy, integrity, and completeness (scope). Organizational Isolation techniques separate data into domains with different levels of integrity, accuracy, and assurance as required by the organizational requirements of the consumer.

The nuclear industry has an established safety culture that implements the concept of separation by criticality. Safety critical components are isolated from less critical components to ensure that equipment qualified to a lesser degree of rigor do not impact the safety critical function. Organizational Isolation follows this same concept. Data which has originated from the MM&D Domain via functional isolation is prevented from being used for Operational Domain decisions. In the context of cyber security, this is necessary to prevent a feedback loop where an MM&D data source could have less assurance of cyber security protection or detection is compromised through malicious attack and then used for an Operation Domain function.

Key Human Performance Point

Data from the MM&D Domain must be reviewed/analyzed/or processed and integrity ensured by qualified engineering personnel before it can be used for Operational Domain decision making.

An example would be the pump motor vibration monitoring system illustrated in Figure 4-1. In this scenario, data is acquired directly from the vibration monitor in a manner to optimize for cost and ease of installation and maintainability. Because of that, the data values obtained directly from the sensors may have periods of missing or inaccurate data. The missing and inaccurate data is analyzed, normalized, and evaluated by qualified personnel before the data is used for plant decision making which makes any undesired data characteristics manageable.

If this vibration data on the MM&D Domain were used directly for Operational Domain decisions without review and analysis by qualified personnel, undesired or unsafe plant operations could potentially result.

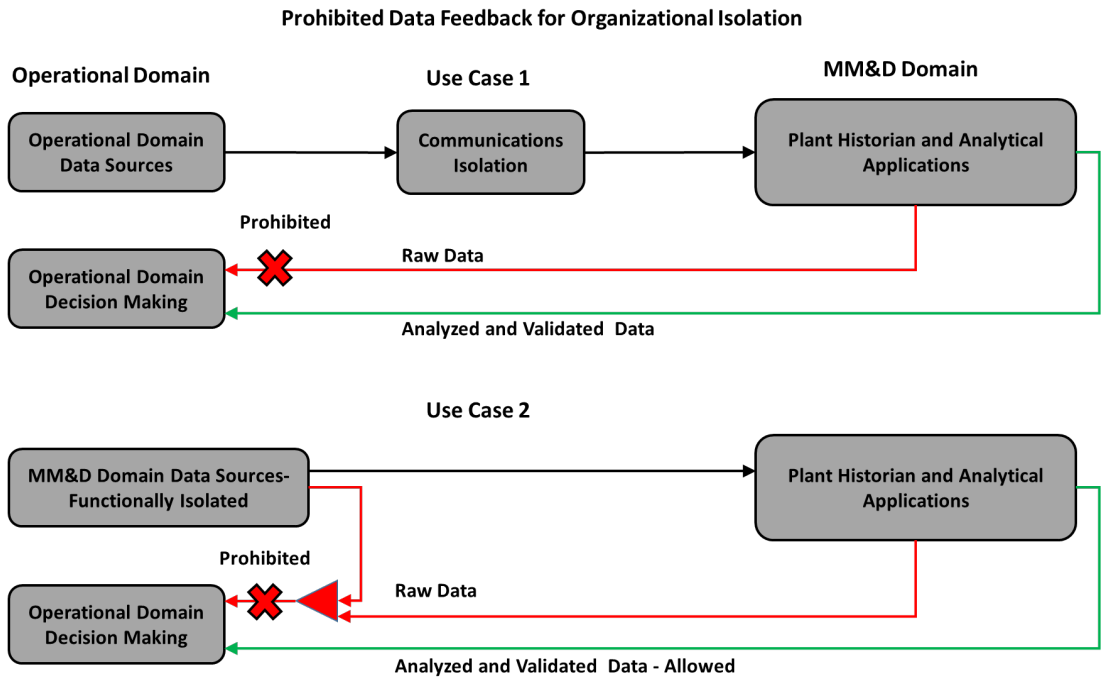


Figure 5-1
Organizational Isolation Use Cases

Use Case 1 in Figure 5-1 illustrates the issues with using data that, while originating in the Operational Domain, has been modified or processed in the MM&D Domain but not analyzed or validated. Any time data passes through the MM&D Domain, analysis and validation methods must be applied before the results can be used in the Operational Domain. Otherwise the data could now have reduced accuracy or integrity depending on the traits of propagation applied to the data. Raw Data is prohibited from being fed back into the Operational Domain for decision making in this circumstance. An example is the use of Human Machine Interface (HMI) displays on the Plant Data Historian in the MM&D Domain. This would be a case in which the data originated in the Operational Domain but was processed and displayed with a lesser degree of integrity and assurance than is expected in the Operational Domain. It would be inappropriate for these HMI displays to be used for real-time decision making in the Operational Domain by Plant Operators. Plant System Engineers could use these displays and input to perform further analysis that established the integrity and accuracy of the data displayed.

Use Case 2 in Figure 5-1 describes the prohibition of data sourced directly from the MM&D Domain from being fed into the Operational Domain. This prohibition is necessary to prevent inappropriate use of the MM&D Domain data. This could occur if sensors intended for MM&D Domain use were also connected directly to an Operational Domain system without additional analysis and assurance methods being applied.

6
REFERENCES

References

1. Antonin Scalia, "Separation of Functions: Obscurity Preserved," 34 Administrative Law Review [v] (1982).
2. GE Measurement and Control, *3500 Series Machinery Protection Systems*, GE Measurement and Control, Minden, NV 2015
3. “Network Segmentation and Segregation.” Department of Defense-Intelligence and Security, Australian Government , *Protect* September : 2012 ed.
4. *Security Guideline for the Electricity Sector: Physical Security*. NERC, Atlanta, GA: 2012.

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 members represent 90% of the electric utility revenue in the United States with international participation in 35 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

Programs:

Nuclear Power

Instrumentation and Control

3002008206

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