Working Document of the NPC Study
Dynamic Delivery –
America's Evolving Oil and Natural Gas Transportation Infrastructure
Made Available December 12, 2019

Topic Paper #4-14

PURDUE MODEL FRAMEWORK FOR INDUSTRIAL CONTROL SYSTEMS & CYBERSECURITY SEGMENTATION

Prepared for the

Technology Advancement and Deployment Task Group

On December 12, 2019 the National Petroleum Council (NPC) in approving its report, *Dynamic Delivery – America's Evolving Oil and Natural Gas Transportation Infrastructure*, also approved the making available of certain materials used in the study process, including detailed, specific subject matter papers prepared or used by the study's Permitting, Siting, and Community Engagement for Infrastructure Development Task Group. These Topic Papers were working documents that were part of the analyses that led to development of the summary results presented in the report's Executive Summary and Chapters.

These Topic Papers represent the views and conclusions of the authors. The National Petroleum Council has not endorsed or approved the statements and conclusions contained in these documents, but approved the publication of these materials as part of the study process.

The NPC believes that these papers will be of interest to the readers of the report and will help them better understand the results. These materials are being made available in the interest of transparency.

The attached paper is one of 26 such working documents used in the study analyses. Appendix C of the final NPC report provides a complete list of the 26 Topic Papers. The full papers can be viewed and downloaded from the report section of the NPC website (www.npc.org).

This page is intentionally left blank.

Topic Paper

(Prepared for the National Petroleum Council Study on Oil and Natural Gas Transportation Infrastructure)

4-14	**Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation**
Author(s)	**David Garton (Plains All American Pipeline)**
Reviewers	**Alfred Lindseth (Plains All American Pipeline)** **Wesley Malaby (Phillips 66 Company)** **Doug Sauer (Phillips 66 Company)** **Jay Churchill (Phillips 66 Company)**
Date: November 12, 2019	**Revision:** Final

SUMMARY

The Purdue Enterprise Reference Architecture is based upon the commonly used architectural reference model authored in the 1990s for control systems. The Purdue model provides a framework for segmenting industrial control system networks from corporate enterprise networks and the internet. The model is used as a baseline architecture for all industrial control system frameworks such as API 1164 and NIST 800-82. To understand the complexity of the OT environment, the Extended Purdue model was developed which is derived from the generic ICS model and applies specific risk layers and security zones. A conceptual visualization is displayed at the end of this topic paper to assist in applying these zones theories for practical consumption.

Purdue Model Description: Overview

The Purdue Enterprise Reference Architecture is based upon the commonly used architectural reference model authored in the 1990s for control systems. The Purdue model provided a framework for segmenting industrial control system networks from corporate enterprise networks and the internet. The model is used as a baseline architecture for all industrial control system frameworks such as API 1164 and NIST 800-82. According to Li (1994), the Purdue Enterprise Reference Architecture (PERA) and associated methodology were developed by the Purdue Laboratory for Applied Industrial Control (PLAIC) of Purdue University. PERA was first developed by PLAIC in December 1990 and published one year later. PERA was defined as “an informally described means for leading a user’s application

group through all of the phases of an enterprise integration program from initial concept through use to final plan obsolescence (Li, p. 26, 1994). The most important contribution of Purdue Architecture is the level of detail and practical proposal to assimilate and integrate enterprises within standard industrial processes, manufacturing and services industries. These layers represent interconnections between electronic or mechanical, which permit two or more physical (human, organizational, or both) mechanisms to accomplish specific functions. An interface to the interconnections is a shared boundary between two entities. These interconnections, while not an exhaustive list, consists of an engineer or programmer to computer, plant worker or operator to computer, and computer to computer. Within the energy sector, information data flow, material and energy flow, and physical systems are all controlled throughout the various interconnected interfaces. Protocols are designed in order to provide a common language throughout these interconnections. These protocols consist of some standard Information Technology protocols, but Operations Technology contains protocols not consumed by conventional IT. While the delta is not considerable, the small difference in protocols must be accurately represented when describing, identifying, and securing OT (NIST 800-82, p. 29, 2015). NIST 800-82 further proclaims a cross-functional team of control engineers, control system operators, and IT security professionals need to work closely to understand the possible implications of the installation, operation, and maintenance of security solutions in conjunction with control system operation. IT professionals working with ICS need to understand the reliability impacts of information security technologies before deployment. Some of the OSs and applications running on ICS may not operate correctly with commercial-off-the-shelf (COTS) IT cybersecurity solutions because of specialized ICS environment architectures. To understand the

complexity of the OT environment, the Extended Purdue model was developed which is derived from the generic ICS model and applies specific layers defined within Table 1.

These layered attributes consist of

- **Level:** Overall section where network segments reside within a company's overall enterprise network.
- **SCADA/ICS Description:** General description of assets within each layer.
- **Risk/Material Profile:** Risk rating and material impact of each layer.
- **Functional Layer:** coordination of industrial control and business systems are deployed
- **Standards:** Common standards that assist in governance within each layer.

Table 1: Extended Purdue Model Attributes

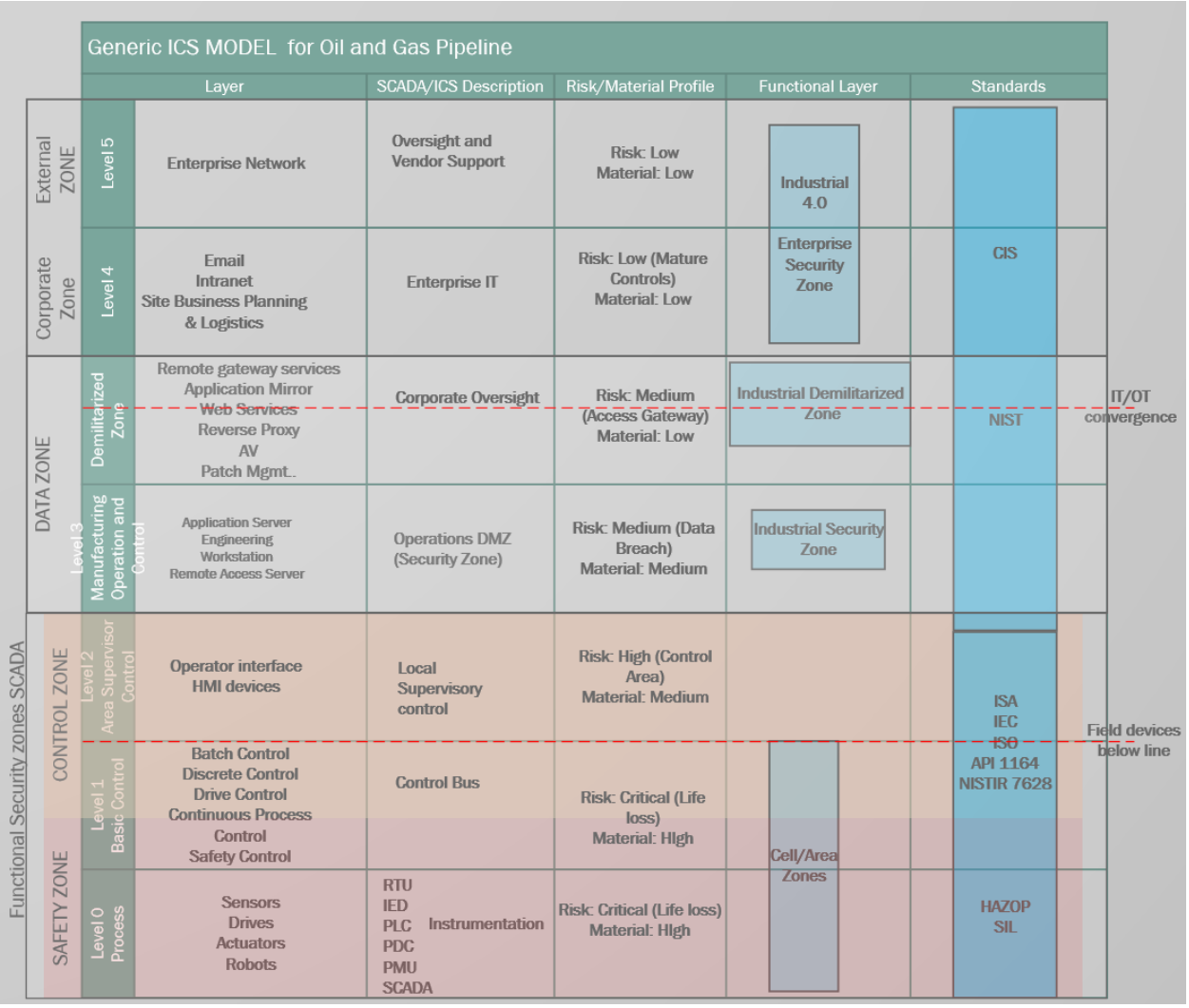
Level	SCADA/ICS Description	Risk Material Profile	Functional Layer	Standards
Level 5	External/ Vendor Support/ Cloud Access	Level 5 is considered low because of the IT controls that are in place. Material Impact is considered Low.	Industrial 4.0	CIS
Level 4	Business Logistics systems/ Enterprise IT- This is corporate IT.	Level 4 is considered Low because of the Maturity of IT controls. Material Impact is considered Low.	Enterprise Security Zone	
Level 3.5	Demilitarized Zone This level was not designed initially within the Purdue model; however, with the continual convergence of OT and IT this abstract layer is essential to ensure separation of communications.	Level 3.5 is medium but a crucial layer. This is the access gateway that provides IT access for governance function and vendor support. Material Impact is considered Low.		NIST

Level 3	Manufacturing operations systems — Managing production workflow to produce the desired products. Batch management; manufacturing execution/operations management systems (MES/MOMS); laboratory, maintenance, and plant performance management systems; data	Level 3 is considered Medium because personnel safety is low; however, Data breach is an issue. Material loss profile is considered Medium		
Level 2	Control systems- Supervising, monitoring, and controlling the physical process. Real-time controls, HMI (Human-machine interface) SCADA (supervisory and data acquisition)	Level 2 is considered High because of access to SCADA. The material loss profile is considered Medium.		ISA IEC ISO

Level 1	Intelligent devices- Sensing and manipulating the physical process. Safety is considered the highest priority function in ICS within the safety zone. Zones 0-1 is where safety systems have been utilized even before attacks on critical infrastructure existed. These embedded safety systems provide some mitigation against cyber-attacks; however, a new variance of malware that attacks CSS (Cyber Safety Systems).	Level 0-1 is considered critical because of safety concerns. A mix of standards, guidelines, and regulations assist cybersecurity defensibility as well as safety depicted under standards. The material loss profile is considered High.		API 1164 NISTIR 7628
Level 0	The physical process – Defines the actual physical processes			HAZOP SIL

Figure 1 attempts to take the overlaying attributes and provide insightful boundaries within these interconnected devices.

Figure 1: Extended Purdue Model with overlaying attributes defined in Table 1



To further enhance cybersecurity NIST 800-82r2 defines specific zones. A conceptual understanding must be stated and defined. The next section will describe these zones outlined within NIST 800-82r2. A conceptual visualization is displayed at the end to assist in applying these zones theories for practical consumption. Please refer to NIST 800.82r2 stated within the references section for more detailed information.

Network Security Zones

Network security zones are logical areas within a company's networks, and each zone has basic and unique security requirements. Networks should be demarcated by network security zones.

- **Network Boundary Protection**

Network security zones should have clearly defined boundaries. At a minimum, network boundary defense requirements should ensure that all:

- Devices attached to a zone are authorized
- Interfaces with other zones are authorized
- Entry points are defined
- Boundary devices are hardened against attack
- Network traffic is filtered at entry points
- Network traffic is monitored at entry points
- Encrypted Network traffic is inspected for malware, phishing attacks, and other security considerations at entry points
- Authorized user-authentication techniques are employed
- Privileged access is managed and monitored
- Authorized change control processes are aligned with change management standards

- **Network Traffic Control**

Network traffic between zones should be controlled to ensure that:

- Only authorized traffic is allowed to pass between zones
- Malicious traffic is identified and filtered wherever possible
- Authorized traffic is directed to specified resources
- Outgoing traffic does not expose the zone to additional risks
- Wireless traffic is terminated in the public access zone

- **General Zone Controls**

General zone controls apply to all zones within each functional layer. At a minimum, these controls should ensure that:

- Routable network/segments:
  - Exist in every zone
  - Are entirely within a single zone, i.e., two nodes with the same network address should not be indifferent zones
- Servers and clients should not be accessible in more than one zone
- Zones connect through approved entry points
- Documentation and technical drawings for all zones should be maintained and appropriately secured.

Authorized Zones Authorized security zones should include:

- **Public Access Zone (PAZ):**

The PAZ is the only zone that can connect to the public Internet and facilitates access between the company's online services and the Internet.

Companies should configure the PAZ to:

i. Interface company's on-line services
ii. Set-up proxy services to allow access to:
iii. Internet-based applications
iv. External email
v. Remote access
vi. Implement extranet gateways
vii. Include the Demilitarized Zone (DMZ) as a component

- **Operation Zone (OZ)**

The OZ is the standard environment for general business corporate operations, and most end-user systems and workgroup servers are installed in the OZ.

A company should configure the OZ to:

i. Route traffic to originate internally or from external sources via the PAZ, e.g., external traffic sources include remote access, mobile access, and extranets
ii. Separate sub-zones for clients and servers as components
iii. Exclude large repositories of sensitive data or critical applications
iv. Process sensitive information with appropriate security controls at the client level

- **Restricted Zone (RZ)**

The RZ is intended for services and systems having reliability requirements where compromise of the IT services would cause a business disruption.

A company should configure the RZ to:

i. Connect to the PAZ, OZ, and ICRZ through approved entry points
ii. Separate sub-zones for client and servers as components
iii. Harden servers and clients in the zone
iv. Include large repositories of sensitive data or critical applications

- **Industrial Control Restricted Zone (ICRZ)**

The ICRZ provides a controlled network environment. This zone is suitable for Industrial Control Systems (ICS), where compromise of those systems may endanger human health, safety or the environment.

A company should configure the ICRZ to:

i. Prohibit direct connection to the PAZ
ii. Connect to the OZ and RZ through approved entry points
iii. Separate sub-zones for client and servers as components
iv. Ensure servers and clients in this zone must be appropriately hardened
v. Include large repositories of sensitive data or critical applications

- **ICRZ Subzones**

ICS units may create Subzones within the ICRZ for their respective areas.

Subzones should not connect to the PAZ.

Subzones can connect to the OZ and RZ through approved entry points (conduits)

External partner connections for SCADA support should be through the TPZ or ICS level 2 network subzones through approved entry points (conduits)

ICS units deploying Subzones must create and maintain Subzones documentation that includes:

i. Technical drawings
ii. Definition of the subzones
iii. Controls associated within each subzone
iv. Traffic Control requirements
v. Boundary Protection requirements
vi. Reference to this standard

- **Trusted Partner Zone (TPZ)**

A TPZ supports directly connected services with highly trusted partners. This Zone can be viewed as a logical extension of internal Zones to organizations external to the company.

A company should configure the TPZ to:

i. Prohibit connection to the ICRZ and RZ
ii. Connect to the OZ through approved entry points

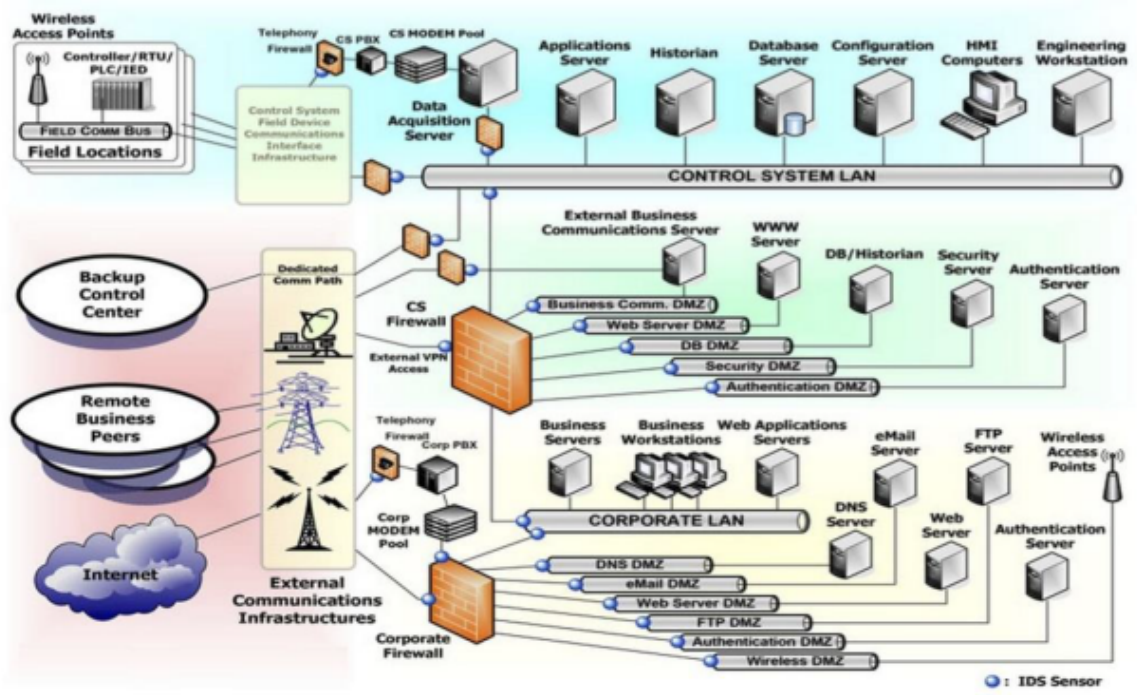
Requirements for the TPZ should be developed on a case-by-case basis and enforced by agreements with trusted partners.

Possible examples of TPZs include:

i. Integration with financial institutions
ii. Integration with trusted suppliers
iii. Outsourced IT environments
iv. Interfaces to independent subsidiaries and affiliates

The figure below taken from NIST 800-82 depicts these boundaries at a functional level.

Figure 2: NIST 800.82 Example (NIST 800-82, p. 62, 2015)



References

I, H. (1994). *A formalization and extension of the Purdue enterprise reference architecture and the Purdue methodology* (Order No. 9523390). Available from ProQuest Dissertations & Theses Global. (304140676). Retrieved from https://pdfs.semanticscholar.org/9fb4/61f114253007097706e387fa2f68257635e2.pdf

K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn, *Guide to Industrial Control System (ICS) Security, Revision 2 Final Public Draft* (NIST SP 800-82), February 2015. Retrieved from: https://doi.org/10.6028/NIST.SP.800-82r2