



CHEMICAL INDUSTRY DATA EXCHANGE

By the Industry....For the Industry

Cybersecurity Practices, Standards, and Technology

Cybersecurity Reference Model

Revision 1.0

August 2004

Copyright Notice

The Chemical Industry Data Exchange (“CIDX”) is a nonprofit corporation, incorporated in the State of New Jersey, which is exempt from federal taxation under Section 501(c)(6) of the Internal Revenue Code. The Cybersecurity Reference Model document has been developed in furtherance of CIDX’s nonprofit and tax exempt purposes in accordance with the CIDX Intellectual Property Policy, Antitrust Policy, and other relevant policies, and the document is owned by CIDX. CIDX has taken reasonable measures to develop the document in a fair, reasonable, open, unbiased, and objective manner for the purpose of providing a reference model to the chemical sector. However, the nature of appropriate practices, guidance, or methodologies is likely to change over time and with developments in technology. Therefore, inclusion of material in the document does not constitute a guarantee, warranty, or endorsement by CIDX regarding any guidance, methodologies, or preferences for conducting business, implementing any CIDX standards, or enhancing computer security. Further, neither CIDX nor its officers, directors, members, employees, or agents shall be liable for any loss, damage, or claim with respect to any such documents, work, or services; all such liabilities, including direct, special, indirect, or consequential damages, are expressly disclaimed. Information provided in the document is “as is” without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or freedom from infringement. The document is the sole and exclusive property of CIDX. Reproduction or redistribution of the document is prohibited without written permission of CIDX.

Copyright © 2004 Chemical Industry Data Exchange. All rights reserved.

Table of Contents

1.	Background.....	4
2.	Purpose.....	4
3.	Audience.....	4
4.	Needs-Based Analysis.....	5
5.	Cybersecurity Zone Definition.....	5
6.	Typical Chemical Sector Cybersecurity Zones.....	6
6.1.	Externally Facing Zones.....	7
6.1.1.	Business to Customer (B2C) Zone.....	7
6.1.2.	Business to Business (B2B) Customer and Supplier Zone.....	8
6.1.3.	Vendor Support Zone.....	8
6.1.4.	Collaborative Zone.....	8
6.1.5.	Business Alliance Zone.....	8
6.1.6.	External Employees Zone.....	9
6.1.7.	Outsourced Applications Zone.....	9
6.1.8.	E-mail Zone.....	9
6.1.9.	Internet Zone.....	9
6.2.	Internally Facing Zones.....	10
6.2.1.	Manufacturing Information Zone.....	10
6.2.2.	Process Control Zone.....	10
6.2.3.	Safety Systems Zone.....	10
6.2.4.	Intranet Zone.....	11
6.2.5.	Laboratory Environment Zone.....	11
7.	Applying the Model.....	11
7.1.	Characterization by Attributes.....	11
7.2.	Attribute Definitions.....	11
8.	Change Record.....	15

1. Background

When developing standards or directions, it is first necessary to establish the context, scope, and definitions that together provide a frame of reference for the more detailed information that follows. This frame of reference is commonly referred to as a “reference model,” a term that became popular with the success of the ISO “Seven Layer” model for Open Systems Interconnection. Of more direct relevance to manufacturing is the Purdue Reference Model for Computer Integrated Manufacturing¹, which in turn provided some of the basis for the ANS/ISA-95 standard.

The NASA Office of Standards and Technology (NOST) defines the term reference model as:

“A reference model is a framework for understanding significant relationships among the entities of some environment, and for the development of consistent standards or specifications supporting that environment. A reference model is based on a small number of unifying concepts and may be used as a basis for education and explaining standards to a non-specialist.”

Regardless of the exact definition used, the objective is to identify the requirements (such as content and latency) for information flow between areas and levels in organization so that it can address security issues with a common understanding of the framework and vocabulary.

To fully address this objective, a series of logical models may be required, each describing the overall scope from a different logical perspective. Examples include:

- A physical hierarchy model showing levels of systems and devices ranging from enterprise to control module
- A functional hierarchy model showing the relative positioning of various types of applications within the enterprise
- A security domain model that describes how different security requirements and constraints apply for various portions of the overall environment
- A system or network layer model that describes the hierarchy from physical infrastructure to applications

2. Purpose

The purpose of this document is to describe a security domain reference model that may be used to provide consistent context and terminology to aid cybersecurity efforts in the chemical sector. By design, this document uses references to existing zone definitions and lexicons rather than creating new ones. It is not a guidance document nor does it present a process for developing cybersecurity policies.

3. Audience

The intended audience is as follows:

¹ [A Reference Model for Computer Integrated Manufacturing \(CIM\)](#), Copyright © 1989 Purdue Research Foundation, ISBN 1-55617-225-7

- CIDX cybersecurity teams
- Users of CIDX cybersecurity documents
- Those engaged in cybersecurity discussions or the development of cybersecurity policy in the chemical sector

4. Needs-Based Analysis

Cybersecurity policies, practices, and implementations may vary within a company depending on the functional needs of the computing assets under review. It is generally not appropriate to treat all computing assets in a similar fashion when developing cybersecurity policies. Assets may be segmented into cybersecurity zones consisting of components that share common functional use.

5. Cybersecurity Zone Definition

The information technology (IT) infrastructure of the typical chemical sector company can be described as a collection of zones, each with a specific set of characteristics and requirements that influence or dictate how elements in that zone should be acquired, operated, managed, and supported.

The following guidelines apply when describing a set of cybersecurity zones:

- A cybersecurity zone consists of a logical collection of IT components that share common functional requirements and cybersecurity policies, although the consistent implementation of a policy for all elements within a zone may be restricted by technical differences among the member components.
- There may be multiple instances of any particular zone within a company but consistent policies may still apply.
- Zones are typically interconnected but the usefulness of a zone during periods of temporary isolation from other zones should be a consideration when defining boundaries.
- A management of change policy should be a consideration when defining a zone and associated policies.
- Consistent trust relationships, user authentication, etc. should be a consideration when defining a zone.
- Cybersecurity policies should be considered for each zone and for interfaces between zones.
- Typically, each zone should have a single owner for cybersecurity policy.

6. Typical Chemical Sector Cybersecurity Zones

There are a number of ways in which various zones might be arranged. One of the simplest is to first consider two broad groups or categories. The first category includes those zones that by their nature have some degree of contact external to the enterprise. These are referred to as “externally facing zones.” Those zones remaining are by nature more focused on communications and interactions within the enterprise, and are referred to as “internally facing zones.” The following diagram (Figure 1) shows this arrangement and the specific types of zones in each category. The contents of each type are described in more detail in subsequent sections.

This arrangement represents typical chemical sector cybersecurity zones. Detailed zone definitions are likely to vary from one company to the next. It is more important to clearly define zones and boundaries as part of a cybersecurity effort than it is to adhere to any particular architecture.

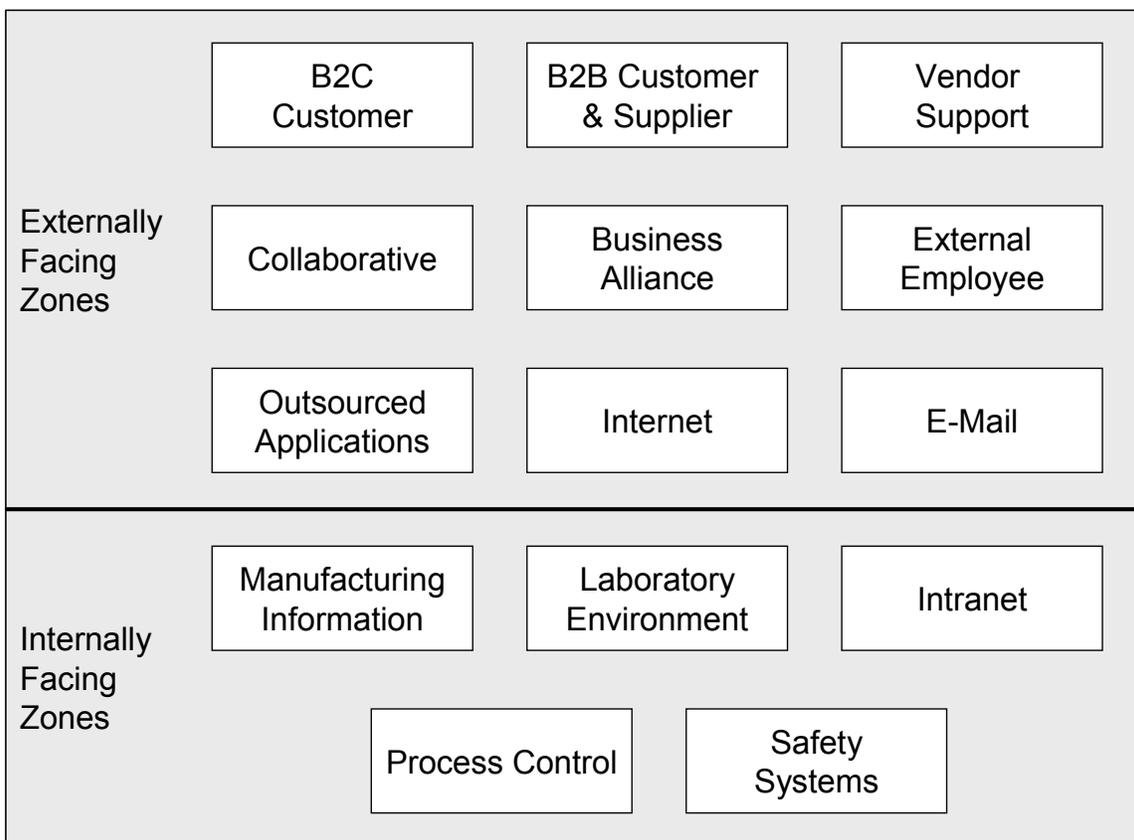


Figure 1 – Zones by Type

6.1. Externally Facing Zones

Externally facing zones by nature consist of some part that exists outside of the main business facilities or connects to external systems. For manufacturers, the main business facilities may include corporate headquarters and production sites, company owned warehouses and storage facilities, logistics systems, and others.

Many businesses have local area networks (LANs) that may be accessed externally with a broad range of applications sitting on these LANs. For our purposes, only those systems that are intended to directly interact with external systems are included; others are considered internally facing.

This section addresses only those systems that are considered enterprise; consideration for production systems, including those connected externally are considered within production zones.

Specific zones in this category are:

- Business to Customer (B2C) – Direct sales and support for customers
- Business to Business (B2B) – Customer and Supplier – typical e-business functionality
- Vendor Support – direct access from outside for vendor support of hardware and software
- External Employee – employee remote access
- Collaborative – external partners, consultants, and service providers through exchange of information and routine communications
- Business Alliance – supporting business relationships, such as joint ventures, providing limited, bi-directional information exchange
- Outsourced Applications – services that are hosted outside the business facilities
- E-mail – e-mail entering the enterprise from the Internet
- Internet – is provided primarily for completeness

6.1.1. Business to Customer (B2C) Zone

Support for customers who may initially log onto a corporate web site (store) to browse and select products for purchase are considered separate from B2B, because of the nature of the interactions. B2C customers may be initially anonymous, may have no permanent arrangement or connections, and probably use unsecured Internet communications.

A similar situation may exist for some suppliers that have little or no e-commerce capability and minimal IT staffing.

Both customer and supplier situations may also be provided with support through self service portals, with provisions for direct communications.

6.1.2. Business to Business (B2B) Customer and Supplier Zone

Many businesses establish secure connections with suppliers and customers for the purpose of conducting electronic commerce. B2B zones typically involve automated connections between systems perhaps for the purpose of exchanging purchase orders, executing release for shipment, issuing advanced shipment notices (ASN), notification of goods received, issuing invoices, and settling payment. It may also include exchange of product, catalogue, pricing and availability information depending on the relationship.

Relationships with customers and suppliers are of course opposite roles to the business, but involve similar integrations and exchanges such as Electronic Data Interchange (EDI).

B2B zones may also support collaborative relationships between companies such as collaborative planning, forecasting, and replenishment.

Depending on the arrangement, connections to services that support B2B interactions, such as product item data synchronizations (for example, Uniform Code Council (UCC) net) may be considered part of a B2B zone or considered a separate zone.

6.1.3. Vendor Support Zone

Many manufacturing organizations rely on vendor support for manufacturing equipment. In some cases the equipment includes diagnostic and health status ports that are designed for remote access when connected to the internet or perhaps telephone lines.

The capability and implementation of these interfaces vary widely. Accordingly, these access points require special analysis and control to provide adequate security. They seldom can be grouped with other connection categories and require a separate zone.

6.1.4. Collaborative Zone

Some partner, supplier, customer and other communications is designed specifically for the purpose of collaborations. This is typically centered on document exchanges, and associated business processes, and may include other collaboration tools such as remote desktop sharing, instant messaging, and work portals - either privately or publicly hosted.

6.1.5. Business Alliance Zone

Business alliances may take many forms, perhaps including shared facilities and information systems. Furthermore, they may require differing types of communications, and may include a relatively large variety. There may even be a need to have multiple business alliance zones, corresponding to the types described in other sections of this document.

Even when communications are technically similar to B2B, for example, special controls are usually required to protect confidentiality and limit access to certain information.

6.1.6. External Employees Zone

A growing number of employees are being set up to work from places other than the manufacturing facilities or corporate offices. This includes working from home, while traveling on company business, at a partner's site, or any number of other locations.

They are often described as mobile or remote workers and may be using either a company owned and controlled computer, a privately owned computer, or a borrowed computer owned by someone else, creating a large variety of situations for security considerations.

Company-owned and controlled computers may be connected to corporate systems with secure communications (such as a virtual private network [VPN]), creating a different trust relationship, which may lead to treatment of this sort of situation as a separate zone from other situations.

6.1.7. Outsourced Applications Zone

In some cases businesses make arrangements with an external service organization to run applications in the service organization's computers. The applications are accessed from the business through various means. Outsourced hosting typically requires special security arrangement to assure protection of the business information, to assure quality of service, and to make other arrangements.

Often outsourcing may offer the cost benefit when the service provider is able to load balance across multiple customers, and this may require special security arrangement such as logical and physical separation and protection of applications.

The service providers' security practices are an important part of the businesses security program.

6.1.8. E-mail Zone

E-mail entering the enterprise from the Internet needs additional security controls because of the problems associated with e-mail distributed viruses and worms, spam, phishing, etc. The content filtering, attachment blocking, virus checking and spam blocking e-mail coming from or going to the Internet would be included in this zone.

6.1.9. Internet Zone

The Internet zone is provided primarily for completeness. The firewalls that allow employees on the internal network to access the Internet would be part of this zone. Activities with security policies that are substantially the same as those for employees surfing the net could be included in this zone. Activities with substantially different policies should be put in a different zone.

6.2. Internally Facing Zones

Specific zones in this category are:

- Manufacturing and Control Systems – manufacturing IT systems that have quality, safety, regulatory compliance or reliability roles
- Manufacturing Information – the transition between the manufacturing zone and other zones
- Safety System – special equipment or software to ensure the safe shutdown of a process
- Intranet – PCs, network, and server not included in other zones.
- Laboratory Environment – (research, quality assurance, pilot scale, etc.) – devices, network components, computers, etc. that are connected directly to equipment in the laboratory environment.

6.2.1. Manufacturing Information Zone

The manufacturing information zone typically serves as the transition between the manufacturing zone and other zones. Non-manufacturing zones often need data from manufacturing but do not have the need to access other systems within the manufacturing zone. Issues such as authentication, trust and isolation should be considered when defining this zone. Manufacturing information systems often have functional requirements that are quite different than those for components of the process control zone so separating them in order to simplify routine system maintenance may be appropriate.

6.2.2. Process Control Zone

Modern process monitoring and control systems, Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control System (DCS), etc. often rely on IT assets that must be considered when developing cybersecurity policies. Often, the policies for these systems are different than those for general purpose computing due to the nature of the manufacturing environment.

The need for deterministic response in a control system could preclude the use of certain tools, methods or policies in the manufacturing and control systems zone.

Typically, process control systems are defined as those that have quality, safety, regulatory compliance or reliability roles, and must be able to function even if isolated from other zones.

6.2.3. Safety Systems Zone

Although shown in Figure 1 as a separate zone, safety systems are typically connected very tightly to basic process control systems (BPCS). This zone may be separated from the process control zone if it is desirable to implement a cybersecurity policy separate from the process control zone. The components of the safety system zone, however, are typically critical components on which the process control zone components rely. In those situations where a Safety Instrumented System (SIS) is required to ensure the safe shutdown of a process, special equipment is used that may have correspondingly specialized security requirements. More detailed information on these requirements is available in the international standards IEC-61508 and IEC-61511.

6.2.4. Intranet Zone

The Intranet Zone or the general purpose computing zone includes all terminals, workstations, PCs, servers, networks and mainframes used to support the operations of an enterprise except those systems identified to be in another zone. Applications that might run in the enterprise zone include, but are not limited to financial applications like general ledger and accounts payable, CAD/CAM applications, simulations and modeling, personal productivity tools, database systems, human resource systems, and enterprise resource planning (ERP) systems.

6.2.5. Laboratory Environment Zone

Research, quality assurance, pilot scale environments, etc. often rely on devices, network components, computers, etc. that are connected directly to equipment in the laboratory environment for the purpose of automation. Cybersecurity policies may be quite similar to those of the process control zone but the software and hardware may be quite different. In addition, responsibility for the policy likely falls to a different organization.

7. Applying the Model

The set of zone definitions described in the previous section are to be the basis for additional documents generated by CIDX. However, they can also be used as an example that can be adjusted to meet specific company requirements. In determining the exact set of zones for a particular situation, it is important to have a method for determining whether gaps or overlaps exist.

7.1. Characterization by Attributes

One such method is to identify a list of attributes that may be used to describe each zone. If the set of attributes chosen adequately cover the most important functional characteristics, then it becomes a fairly simple exercise to compare zones based on these attributes. If two zones have essentially the same description with respect to all of the attributes, then it is likely that they can be consolidated, reducing the total number of zones to be considered. On the other hand, marked differences between zones with respect to selected attributes help in determining differences in how the zones should be designed and operated.

7.2. Attribute Definitions

There are many potential attributes that could be used for the characterization exercise. The following are suggested.

Remote Access – Is any type of remote access to devices or systems in the zone a requirement? If so, what is the nature of this access in terms of the technology used, the purpose of access, etc.?

Authentication Rules – What are the “rules” that are applied when authenticating users or automated systems? Are they more or less stringent than the norm for the rest of the network?

Authorization Rules – What are the “rules” that are applied when authorizing access by users or automated systems? Are they more or less stringent than the norm for the rest of the network?

Data Protection Methods – What (if any) methods are required in this zone to protect data, over and above the norm? For example, is special or additional encryption required?

Physical Security – Are there any special or additional needs for physical security in this zone? An example would be the requirement for limited access to the control room in a plant.

Audit Requirements – What are the audit requirements? Are they more or less than what is typical for other zones?

Non-Repudiation Methods – Are any special methods required for the zone?

Operational Procedures – Does the nature of the zone dictate any special operational tasks or procedures? This could include an assessment of whether tasks could be outsourced.

Maintenance Procedures – Does the nature of the zone dictate any special maintenance tasks or procedures? This could include an assessment of whether tasks could be outsourced.

Management of Change – Are there any unusual or unique requirements for Management of Change?

Availability – Are the availability requirements more or less stringent than the norm? If so, what are the relevant business drivers?

Policy Responsibility – What group, function or role is responsible for determining security policy for this zone?

Answering the above questions for each zone should result in a fairly comprehensive understanding of what makes each zone different from the others. The answers also contribute to a better understanding of what additional or special focus may be required for selected zones.

This exercise can be completed fairly quickly by using a simple table, with the zones listed in rows and the attributes in columns. Short comments or summaries on the application of attributes to each of the zones help to gain an understanding of similarities and differences.

The following tables show the results of the exercise for the zones identified in this document.

Cybersecurity Reference Model

Externally Facing Zones	Business to Customer	Business to Business (Customer and Supplier)	Vendor Support	External Employee Zone	Collaborative Zone	Business Alliance Zone	Outsource Application Zone	E-mail Zone	Internet Zone
Nature of Remote Access (if required)	Browser to Internet	Electronic	Remote access outside the company firewall is common, VPN, can be client/server rather than web browser, PCAnywhere, CarbonCopy, etc. VERY limited access is desirable. Vendor is getting well within the company's IT infrastructure, but accessing limited	Dial-up, SSL/VPN, IPSEC VPN - VPN services are typically outsourced	IM, Internet Browser, other tools	Browser-based, seldom SSL VPN	If remote SSL VPN	SMTP based	
Authentication Rules	May begin with anonymous logon	Never anonymous logon, typically protected by SSL	VPN and internal network	Strong authentication required	Tool dependent	User ID and Password or Client Certificates	User ID and password, SecureID or Secure Token respectively	none normally required - occasionally people use X.509 certificates for non repudiation.	Outbound authentication required if variable blocking of sites or for some types of audit trails
Authorization Rules	Typical	Typical	Lots of negotiation and legal agreements	Typical	ACL based	yes	yes	Typical	Typical
Methods for data protection (encryption)	Privacy driven, e.g. for storing credit information	Typical	Nondisclosure agreement typical	Typical	Tool dependent	SSL	Typical	S-mime or PGP occasionally used for authentication	SSL
Physical security	Typical	Typical	Typical	Typical	Typical	Typical	Typical	Typical	Typical
Audit requirements	Order entry focused, typically application audit rather than system audit	Typical	Highly audited	Needs an audit trail	Can be low	medium	high	Message headers or entire message may be retained as audit trail	organization specific requirements
Non-repudiation methods used	Typically just password, not tokens	Typical	Digital certificates might be required for audit	Typical	Tool dependent	Typical	Typical	X.509 certificates	Typical
Operational procedures	Dedicated e-biz group or could be outsourced	Dedicated e-biz group or could be outsourced	Typical	Dedicated IT Admins	Dedicated IT Admins	dedicated IT personnel	dedicated IT personnel	Typical	Typical
Maintenance procedures	Dedicated e-biz group or could be outsourced	Dedicated e-biz group or could be outsourced	Typical	Dedicated IT Admins	Dedicated IT Admins	dedicated IT personnel	dedicated IT personnel	Typical	Typical
MOC procedures (patches, etc.)	Rigorous due to exposure to Internet	Rigorous due to exposure to Internet	Vendor typically applies changes and typically follows vendor procedures	More important than internal because they are outside the firewall	Exposed to internet so rigorous, tools like WebEx can be from outside provider so MOC may not apply	Typical	Typical	Typical	Typical
Availability requirements (redundancy, etc.)	Highly available	Highly available	Could be at any time of day, typically driven by system availability requirements	High availability but typically not mandatory	Standard	high availability is desired but not mandatory	high availability crucial	Typical	typically high
Security policy responsibility	Involvement by Legal department, data privacy, European Signature Law apply	Involvement by Legal department, data privacy, European Signature Law apply	Typically an exception to every security policy	Normal corporate policy	Standard				involves legal and HR to establish appropriate use standards

Table 1 – Externally Facing Zones

Internally Facing Zones	Process Control Zone	Manufacturing Information Zone	Manufacturing Safety System Zone	Internet Zone	Laboratory Environment Zone
Nature of Remote Access (if required)	Restricted (people and tasks), must be pre-approved by operating staff	Open	Prohibited	Typical	Restricted (people and tasks), must be pre-approved by operating staff
Authentication Rules		Typical	Typical	Typical	Typical
Authorization Rules	By role	Typical	By user	Typical	By role
Methods for data protection (encryption)	Typical	Typical	Typical	Typical	Typical
Physical security	Control room access rules	No special requirements	Locked	Typical	Lab access rules
Audit requirements	Typical	Typical	Typical	Typical	Typical
Non-repudiation methods used	Typical	Typical	Typical	Typical	Typical
Operational procedures	Typical	Typical	Typical	Typical	Typical
Maintenance procedures	Maintenance must be scheduled with operating staff, updates push or pull	No special requirements, updates push	Only during plant outages, updates pull	Typical	Maintenance must be scheduled with lab staff, updates push or pull
MOC procedures (patches, etc.)	Same as other control system components	Typical IT MOC	HAZOP	Typical	Same as other lab components
Availability requirements (redundancy, etc.)	24/7	Occasional maintenance outages okay	24/7	Typical	24/7 with acceptable, scheduled outages
Security policy responsibility					

Table 2 – Internally Facing Zones

8. Change Record

The following is a record of significant changes made to this document:

Revision	Date	Description of Changes
1	August 2004	First general release