Generalized Security Objectives

derived from

Meeting with Chemical Sector (16 Jan 2003)

- **Communications Objectives**

  Integrity

  a. A secure channel between communicating devices will be established prior to any information being passed.

  b. The secure channel will be established as follows:
     1) each endpoint of the communication will authenticate the other endpoint
     2) information flow between the authenticated endpoints will be conducted in accordance with specific rules defined for that secure channel, addressing:
        i. data content type
        ii. data content values
        iii. flow direction

  c. The secure channel will be maintained as follows:
     1) Each endpoint will only accept information received from an authenticated endpoint
     2) Loss of connectivity will result in attempts to reestablish the secure channel
     3) For each received transmission, endpoints will detect incorrectly formed and erroneous data and will institute recovery action

  Application Note:

  Serial connections using leased line, dial-up or wireless connections are not subject to this integrity criteria. Independent criteria to address serial line communication will be independently developed.

  The integrity criteria apply to all other communication over the control system network infrastructure. The criteria apply regardless of communication media.

  The use of wireless technology in process controls, at a minimum, falls into the following two categories:

  - Wireless technology is integrated into control system devices as a replacement for wired communication medium. The wireless technology is used to support the normal process control functions.

- Wireless technology is integrated into control system devices to support the operations and maintenance activity of a “roving operator”.

The integrity criteria apply to communication over the control system network that is implemented through the following technology:

- Remote access:
- Dial-up connections
- Cable modem
- DSL

- **Identification & Authentication Objectives**

Endpoint Device Authentication

a. The endpoint device will authenticate the claimed identity of an individual prior to that individual being able to initially invoke security relevant actions or initially accessing security relevant information on that device.

   Application Note:
   Security relevant actions include computer system actions such startup, shutdown, backup, recovery, device configuration, s/w or firmware upgrade, etc.
   Security relevant actions also include control system actions such as calibration, set-point adjustment, information download, or maintenance activities.

b. The authentication will be conducted in accordance with the defined rules for authentication, which may include:
   i. Single factor authentication (e.g., password)
   ii. Two factor authentication (e.g., PIN or token with password)

   Application Note:
   Endpoint devices include operator consoles, maintenance consoles, and field devices.

c. Re-authentication of the individual will be required prior to the individual being allowed to invoke a limited set of functions.

d. Re-authentication of the individual will be required prior to the individual being allowed to access a limited set of information.

Boundary Device Authentication

a. The boundary device will authenticate the claimed identity of an individual prior to that individual being able to initially access other devices within the scope of protection of that boundary device.

b. The authentication will be conducted in accordance with the defined rules for authentication, which may include:
   i. Single factor authentication (e.g., password)
   ii. Two factor authentication (e.g., PIN or token with password)

   Application Note:
   Boundary devices include firewalls, routers, bridges, gateways.

c. Re-authentication of the individual will be required prior to the individual being allowed subsequent access to a limited set of devices within the scope of protection of that boundary device.

- **Access Mediation Objectives**

  Roles and Responsibilities

a. Each individual authenticated by the control system will be associated with a defined role.

b. The functions that the authenticated individual may invoke will be restricted based upon the role definition.

c. Each function will have restricted default capabilities enabled.

   Application Note:
   As an example, a firewall would have ports defaulted to “off” or “disabled”.

d. The information that the authenticated individual may access will be restricted based upon the role definition.

e. Each accessible information set will have restricted default access permissions that limit access and subsequent use of the information set.

f. Each role will have restricted default capabilities established for an individual assigned to that role. Restricted defaults include:
   i. Default passwords that expire on first login to that role
   ii. Default assignment to no role or at maximum one role.

g. An individual is restricted to having only one (1) role active at any time.

h. Special roles will be defined for those individuals that perform system administrative, operations and maintenance functions.

   Application Note:

In this context, maintenance refers to the computer system maintenance, not control system maintenance.

Application Note:

Consideration should be given to establishing criteria to enable a “security override capability” that allows operation outside the bounds of the defined policy. Any such criteria would include strict auditing and perhaps a limited time during which the override capability is enabled and then reverting back to normal operations.

- **Audit and Accountability Objectives**

Event Recording

a. Security relevant events will be recorded to enable subsequent analysis of system activity.

b. Each recorded event will include the following:
   - i. Date and time of the event
   - ii. Description of event
   - iii. Verdict depicting result of the event (e.g., success, failure, shutdown)
   - iv. Identity of device, individual, role, etc, involved in the event
   - v. Event-specific explanatory information

Event Processing and Alarms

a. Semi-automated or fully automated processes will review the event audit trial and for identification of potential security policy violations

b. Semi-automated or fully automated processes will provide an alarm notification for each potential security violation as follows:

   - i. For a set of security violations, the alarm will be immediate
   - ii. For a set of security violations, the alarm must be verified prior to the notification being made