Securing Batch Control Systems

Pamela Mars
Batch Product Manager
Honeywell
2500 West Union Hills Drive
Phoenix, AZ 85027
USA
602-313-3252
Pamela.mars@honeywell.com

KEY WORDS
Security, Batch, Process Control

ABSTRACT

As batch control systems have grown from proprietary to open systems networked both within the plant and with expanded links throughout the enterprise, the ability to share information and access data across platforms has reached levels that were never possible before. With this flexibility has come the increased need to secure systems and ensure only authorized individuals have access to operations. Attempts at unauthorized access can come from outside the process area through viruses and external attacks. Additionally, internal security is critical to ensuring only trained and authorized personnel are controlling the process. These security requirements may come from internal business rules or external regulatory agencies that work to ensure product quality and process safety. This paper explores several key security concerns in batch control system architectures and methods for addressing these issues.
Overview

Batch process control security is becoming a critical concern for the process control domain, IT technology infrastructure and the business enterprise. Over the past several years, increasing focus is being placed on security as the affects of improperly secured systems across industries are realized. The evolution of batch control systems from proprietary to open systems has provided immense flexibility for connectivity, hardware options and application interfaces. However, since these systems are designed using open technologies networked together and leveraging off the shelf operating systems that allow data to flow outside of the control domain, they are inherently less secure. Steps need to be taken to proactively address security before failure modes are realized. The effects of such security breaches can range from an improperly trained individual performing a control action to a virus attack affecting a process control network and causing system failures, or a hacker infiltrating your system. A security problem may also involve a user with inappropriate access rights accidentally deleting system files and rendering a control node unusable or result in a loss of important information. These attacks or inadvertent security breaches can come from an outside source or from within the organization. Security has become higher profile as Homeland Security moves to the spotlight with a focus on cyber security. Standards bodies such as ISA are also looking at addressing security issues through the SP99 working committee, but industry cannot wait to begin addressing security until standards are completed. Security standards development is a lengthy process, which may require technology development and networking infrastructure enhancements.

The first step is to evaluate your security risks today and ensure a plan is in place to address security needs both today and as your needs evolve. There are methods to evaluate security risk and improve security by leveraging existing technologies and infrastructures. Security needs should be identified by building a security risk and mitigation plan. This plan helps define how to move your systems and networks forward to reduce the risk of security incidents. This plan will likely result in leveraging a combination of features within the control platform, features typically used in the IT domain and building control infrastructure. This paper explores several aspects of batch control system security and methods to address these issues. There are multiple layers of security and a combination of these layers can be used to reduce the risk of system harm. The main aspects of security covered in this paper can be broken into the following categories: Control Centric Security, Network Centric Security and Homeland Security as related to the batch control system.

Control Centric Security

Control Centric Security focuses on enforcing industry and user specific business rules within the control platform. Business rules are often dependent on the industry and may involve issues related to regulatory compliance such as 21 CFR Part 11 and predicate rules in FDA regulated industries. Additionally, business rules in non-regulated industries may be developed to ensure product quality and safety by enforcing user authorization to perform control actions. The key is to ensure the solution you are using or plan to use supports flexible security capabilities that can grow as your security needs expand. This includes evaluating potential security risks and maintenance problems created when
multiple applications are integrated together and each carries their own security model verses leveraging a common infrastructure such as domain security. There are three primary modes of Control Centric Security as follows: Build Time Security, Run-Time Security and Reporting Security. Each of these security modes may have different requirements based on the end-user specifications and risk evaluation/analysis.

Starting with build time security, there is a growing trend toward flexible security and tracking capabilities that allow the end-user to determine the level of security required. The base system requirement is to provide system support for limiting access based on the logged in user by providing them the minimum privileges to effectively perform their job. This may be built into the application software, or it may be implemented using operating system level capabilities such as file permissions. This prevents access to critical files by unauthorized personnel. The second level of security adds version control capabilities. This includes user authentication and tracking who made any changes to a configuration, what those changes are and when the changes occurred. However, it may not manage review, testing and authorization to install a modified configuration. The third level is management of change, which includes full life-cycle management where business rules are enforced on any change including approvals, testing and installation. This allows for an approval process where a single user cannot modify and install a control strategy without at least one other person approving the change. This reduces the risk of an unauthorized change on the system. Management of change may also include the ability to roll-back to a prior version as needed.

The next security mode is the Run-Time Security structure. Some companies have a philosophy of having a station based security model where a general login is used by all operators. This strategy assumes there are other safeguards in place to ensure all operators are properly trained and any operator may need to respond to alarms across systems/stations and normal scope of responsibility in emergency situations. This station based mode of operation is starting to lose favor as more companies want to have better tracking of individual operator actions and tighter access control. More extensive forms of security leverage individual operator logins with full traceability on who logged into the system, who performed an action and when. Full printed names may also be required in support of industry regulations. Additionally, there may be control actions that require both primary and secondary signatures before completing to ensure correct information is entered or proper security is enforced to perform critical functions.

The final security mode is the reporting security structure. Reporting is a topic that crosses domains of responsibility as there may be a set of reports and data that are control centric and another set that must have accessibility to the business domain. If historical data is stored as files, signatures may be needed which allow modified records to be easily identified and/or the proper operating system file security to prevent unauthorized access. If the data is stored in a database, audit trails and security may need to be configured to manage or prevent modification of data. Securing history also encompasses limiting view access to authorized personnel. As more functions are outsourced, and expanded access is provided to the business domain, providing a secure connection with specified viewing access is also necessary. Role based security can be implemented to limit data access based on functional roles. The linkages between the business layer and the process control layer will be discussed in more detail in the section on Network Centric Security.
Network Centric Security

Network Centric Security focuses on the network infrastructure and operating system configurations that can be leveraged to provide a more secure basis for execution. Whereas process centric security was focused on ensuring the right individual is performing approved actions on the control system and enforcing business rules, Network Centric Security is focused on ensuring the base operating system and process control environment is secure and the network is protected from unauthorized users who may cause malicious or accidental damage. Unauthorized users may be within the business intranet or outside users attempting to remotely gain access to the control environment. The section focuses on network topologies and operating system configurations that support expanding security requirements.

Network Configurations

There are several key issues that arise when looking at Control Network Centric Security as indicated below:

1. Performance is critical on process control systems and can impact safety, quality and throughput – security cannot cause degraded process control
2. Deterministic and predictable operations are critical to insure correct execution – application of security software, hardware and configurations cannot result in unpredictable operations
3. Support for interoperability with business systems is being leveraged across industries – proper security needs to address the compatibility of these networks
4. System must be manageable or it will not be effective in a control environment – 50 nodes that must be individually configured and maintained creates a maintenance nightmare and can lead to inconsistently applied configurations
5. COTS (commercial off the shelf) technologies are prevalent in process control and need to be addressed – COTS software can provide cost effective, open solutions, but if not properly configured can introduce security risks.

These issues delineate some of the unique aspects of control networks around determinism and performance but also some of the similarities with traditional IT infrastructures around COTS technology and integration with the business domain. The three networks primarily involved in a batch process control system are the Controller Network/Control Network, Application Network and Business Network (reference figure 1).
Over the past 10 years there has been a shift from leveraging proprietary networks towards using open Ethernet communications initially at the business layer, then at the application networks and now that shift is also occurring at the control/controller networks. Communications within the control domain must be highly reliable and secure to ensure process activities are not compromised. There are several steps that can be taken to improve the security on these networks by leveraging capabilities from switches and routers to operating system functions such as domains.

Switches can be leveraged to provide fast and secure connectivity, but they only provide support as defined in their configuration. A poorly configured switch can provide little security from unauthorized access, which can lead to denial of service problems, virus intrusion, etc. There are different types of switches available, with managed switches providing several key capabilities that can improve network security by limiting access and minimizing the effects of some security breaches. Switches can prioritize traffic for packets originating on the local network versus packets initiated from an upper level system. An example would be application traffic would have priority over business traffic on the application network. Additionally, providing a redundant link assists if a communication problem occurs on a primary path. Switches may also support the ability to configure detection of packet storms and specify system responses. Packet storms are floods of packets sent on the network that can disrupt normal operations and are often generated maliciously, but can also be caused by faulty equipment. Switch configuration capabilities may support disabling the port where the storm is initiated and re-enabling when normal conditions are restored. Port filtering can also be leveraged to ensure only selected traffic passes from one network to the next. Access can be further restricted using access control lists (ACL) that specify the permitted source nodes and destination nodes.
The greatest risk of a security problem arises from the business domain where users are readily accessing e-mail, internet applications or transferring files. Many viruses are transmitted using e-mail and the receiving of e-mail should be disabled on process control nodes to minimize the risk of viruses finding routes onto the control network. The business network also has the widest user access and poses the greatest security risk. For communications between the Application Network and the Business Network, expanded security measures are required to ensure the control network is not compromised. These include leveraging an additional router and firewall. If a modem is placed on a control node for business or other specific access, this can also provide an entry point that is bypassing many of the network security layers. A router can be used as the single point of connectivity between the Business Network and the Control Network. Only a single point of connectivity should be used as more entry points result in increased vulnerability. Features within the router can isolate the Business Network traffic from the Control Network while enabling connectivity between the networks. A firewall further protects the network by supporting the following features:

1. Setting a restrictive security policy that denies access to all nodes unless explicitly specified
2. Enable source and destination filtering including specification of which nodes on the business network can connect to specified nodes on the control network
3. Port filtering can additionally be used to only allow specific ports to communicate through the router.

Similar to switch configuration, firewalls and routers can only provide the protection they are configured to support and an improperly configured firewall and router provides minimal security. But a properly configured system of switches, routers and firewalls can immensely improve network security.

Operating System (OS) Domain Security

Much as the network configuration can be adjusted to increase security, there are also configurations of the base operating system that can impact administering an effective security policy. Domain based security is a key operating system capability that provides a centralized location for managing user security across the process control network. As systems grow from a few workstations to complex networks, the need for centralized security becomes paramount and a dedicated domain server for process control can be used to centrally manage security and enforce group polices/user administration. Group Policies can restrict application access, configuration capabilities and even desktop and start menu access to authorized personnel only. Additional centralized management includes specifying password policies, disabling guest access accounts, managing current users and disabling unused accounts. The domain server can then be configured with trust relationships as necessary to support communication between the Business Network and the Process Network. Security Auditing should also be implemented to track both successful and failed log-in attempts as they can be indicative of an impending problem. These features can be leveraged to ensure centralized management and enforced security policies across the process control network in efforts to prevent unauthorized access.
Anti-Virus Protection

But what happens if a virus manages to reach a process control node? Anti-Virus software can be installed on process nodes to detect and in some cases remove viruses in the event the hacker penetrates the security infrastructure or an infected file is inadvertently placed on a control node. The virus software is only as good as the version installed and old anti-virus protection provides minimal security. Before installing any anti-virus software on a process node, confirmation should be obtained from the control vendors on supported versions and configurations. Anti-virus software can interfere with processing if not qualified and correctly configured. Configurations such as enabling full scanning or anti-virus software that does not include CPU limits can degrade performance and must be considered before installing on a control node. Anti-virus software can provide a final line of defense if a virus has penetrated your system.

Operating System (OS) Security Hotfixes

Some security problems may be inherent in the base operating system software and OS vendors may release security hotfixes to address these security gaps. These security patches are updated by OS vendors regularly and control system suppliers need to provide appropriate qualification of critical hotfixes. Each hotfix needs to be individually evaluated and should not be installed without first contacting the process control supplier as these hotfixes may inadvertently affect control operations and process performance. Firewalls can also limit exposure when security fixes have not yet been installed.

Homeland Security

Security related to preventing terrorist attacks has received unparalleled attention since recent assaults in the United States and the government establishment of the Office of Homeland Security. Could a compromise of your systems by a terrorist assault result in life safety issues, critical loss of information, explosions, chemical releases, etc? Many companies are working with security experts to evaluate their risk of a terrorist attack including what vulnerabilities exist in their current systems. These studies often evaluate what vulnerabilities are present at a facility that could be leveraged in a direct terrorist assault or a cyber-assault. The security features outlined above can assist in some areas related to cyber security. But what safeguards are in place to address an unauthorized physical entry into a process area where an exothermic reaction is taking place, ensuring key proprietary information and cell banks are safeguarded or preventing unauthorized users changing process variables from a remote location? There are many aspects of risk and vulnerability, but this section will only focus on the areas of building management and its integration with the batch process control environment. Additionally, many of these same principals can be applied to internal system monitoring and tracking to address business rules from a control centric view of security.

Some components are typically present in batch process control facilities including fire/smoke detections systems and appropriate HVAC controls. However, some capabilities are not as common, but can assist in detection, prevention and ensuring appropriate actions are taken in the event of access violations. One such feature is an integrated access control and monitoring system. Access control can limit access to specific process areas and track operator locations throughout the process. An example
of how tightly integrated building controls and process control can address specific security concerns is outlined below:

*If an unauthorized operator attempts to enter a restricted area, they are given an authorization error and that error is reported on the process control system. From the batch process control system, the operator can be alerted to a possible security problem. Once a problem is observed through the activation of a process alarm or access control error, digital video monitoring can begin recording any events that occur in a specified location and the production supervisor can be paged. Additionally, the alarm triggers a set of procedures to give the operator guidance on what to do in this situation. The batch control operator can then monitor the video/alarms and determine if they need to take specific actions to address the access violation.*

This example illustrates how a tight integration between the process control and building security infrastructure can assist in reducing security risks and enabling the operator to better respond to potential problems. It also illustrates the concept of having evaluated emergency situations in advance and building guidance into the system to ensure the operator has the best information possible to address the problem. The importance of an integrated building management and process system can also be applied when monitoring moveable assets and ensuring they are not moved without the necessary authorization.

**Summary**

The impact of security breaches on a batch process control system can result in business losses and life/safety issues. Having a security plan based on a risk analysis and mitigation strategies can ensure you are proactively reducing security risks today while regularly updating the plan as security needs evolve. There are features present in both the process control domain and the network infrastructure that can assist in addressing security concerns related to enforcing business rules and limiting cyber access to critical control systems. Additionally, a tightly integrated building management system with features such as access control and video monitoring can assist in detecting and preventing unauthorized access to critical areas, restricted information, etc. The key is to evaluate your security risk and vulnerabilities and ensure you are proactively addressing issues before a critical problem occurs.
Bibliography

References