SANDIA REPORT
SAND2006-0650
Unlimited Release
Printed January 2006

Generic Attack Approaches for Industrial Control Systems

David P. Duggan
Sandia National Laboratories
PO Box 5800
Albuquerque, NM 87185

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Sandia National Laboratories

ABSTRACT

This report suggests a generic set of attack approaches that are expected to be used against Industrial Control Systems that have been built according to a specific reference model for control systems. The posed attack approaches are ordered by the most desirable, based upon the goal of an attacker. Each attack approach is then graded by the category of adversary that would be capable of utilizing that attack approach. The goal of this report is to identify necessary levels of security required to prevent certain types of attacks against Industrial Control Systems.

Special thanks to the following individuals for their participation in the brainstorm session and for their input to this document.

Michael Baca
John Clem
Johnny Giere
Bryan Richardson

Introduction

An Industrial Control System (ICS) is an important part of any business where real-time or near real-time control of some process or function is required. Also called Supervisory Control and Data Acquisition (SCADA) systems, these systems control physical processes that range from electric power generation and transmission, to control of chemical reactions, to control of manufacturing lines. These systems are not normal IT systems and their compromise can cause greater harm than that of a generic IT system. The locating of vulnerabilities and the mitigation of those vulnerabilities is extremely important for this type of system.

This paper contains information about generic attack approaches that can be used against the ICS and its components. First, we'll list cyber attack approaches that an adversary might take, in the order we believe they will be taken. Next, we will list the components of an ICS that we believe will be attacked, in the order an adversary will likely use. Finally, we list the attack approaches for each part of the ICS, in rank order, and assign an adversary[1] category to each attack approach for each ICS component.

The example system used for this research was created using the principles and guidelines found in previous works[2] of this organization. A sample functional view of the system is shown as ***Figure 1***, and a sample network view is shown as ***Figure 2***. Specification of the system is incomplete as there are no firewalls, extranets, access-control lists, or other hard or soft security features specified. Even though these items are recommended in the guides, we did not specify them. However, during the attack creation phase, we assumed that reasonable security features were in place, configured properly, and functioning.

The attack approaches and ordering of these approaches were developed against a system created using the guidelines taken from the reference model and best practices papers previously referenced. Actual attack approaches will be dependent upon the specific system developed and may include attacker goals that are different than those used in this paper.

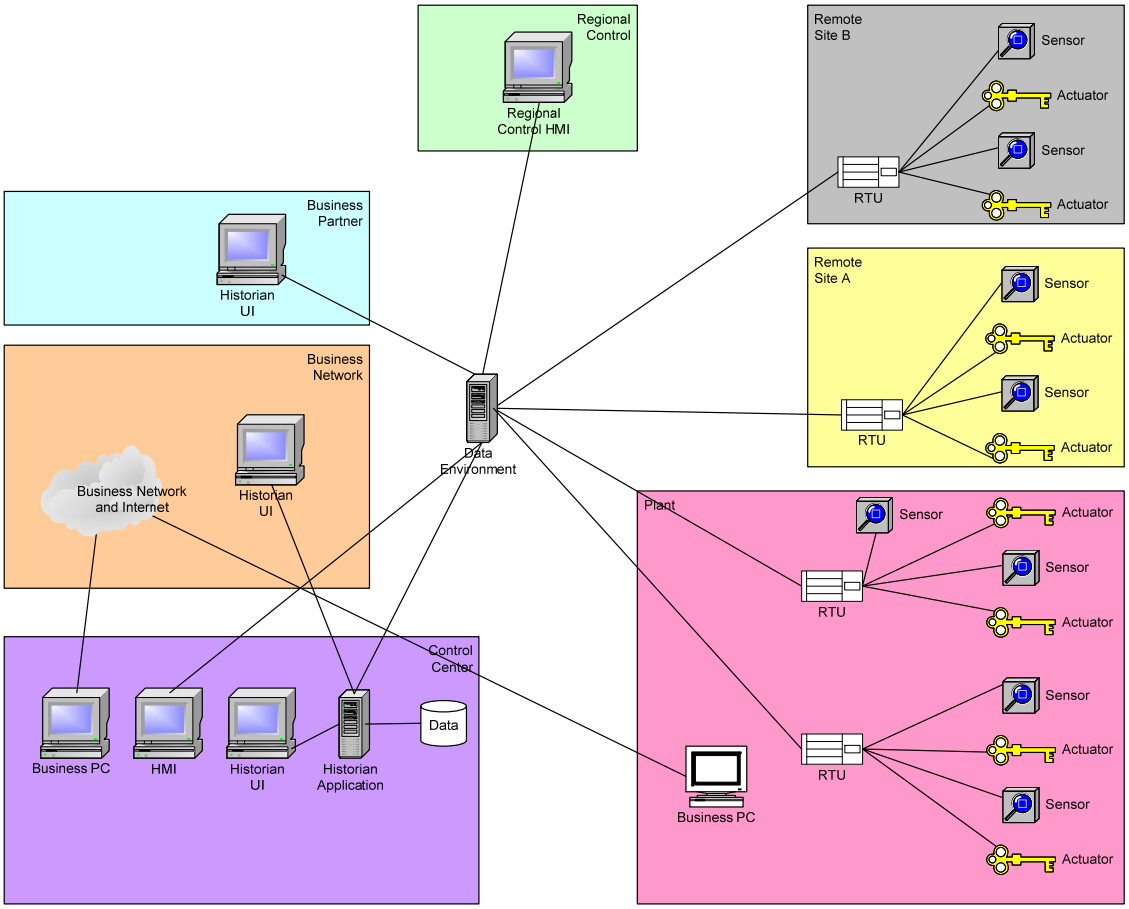

Figure 1 - Functional View

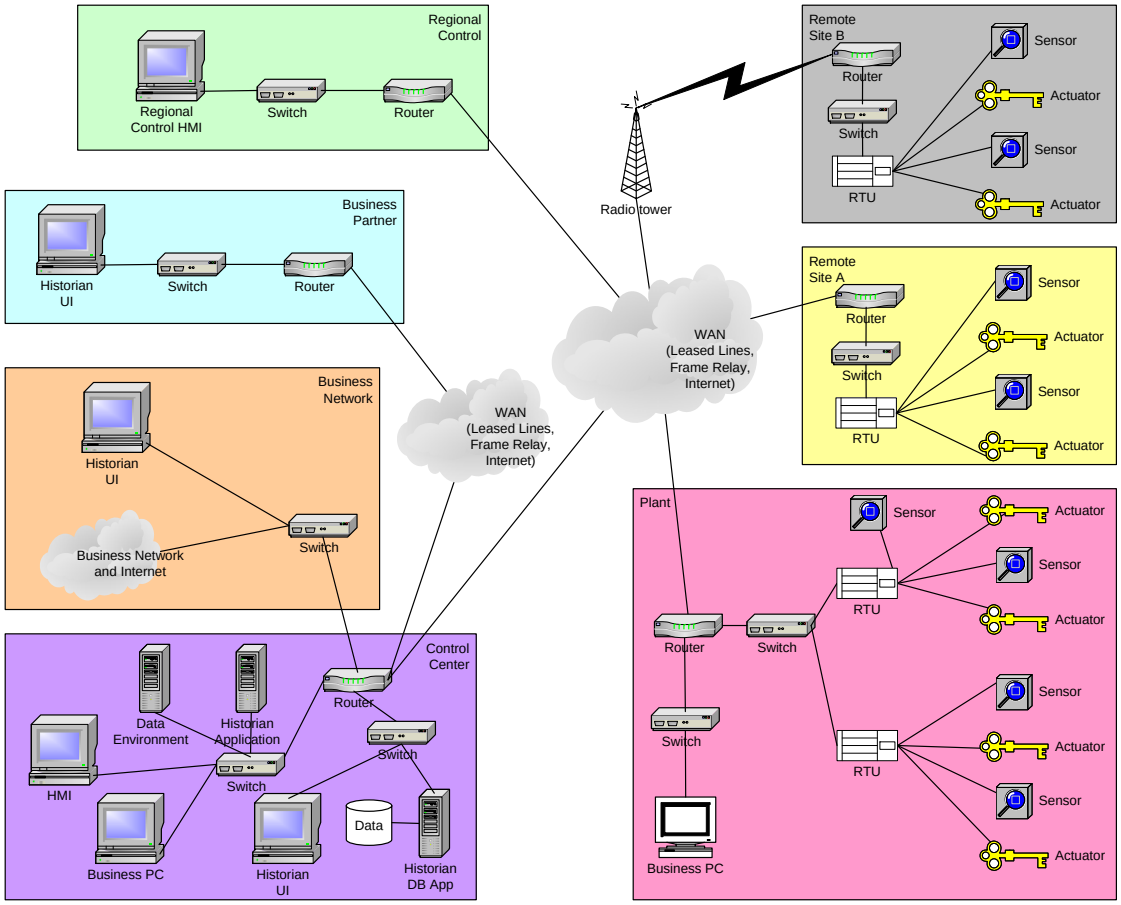

Figure 2 - Network View

Attack Approaches

When looking for vulnerabilities in a system, or component of a system, there are limited avenues to examine. Either the communications with the component, or the component itself can be attacked. The following lists of attack approaches are not intended to be exhaustive, but are expected to be the easiest for an attacker to implement or have the best chance for success.

When considering the communications portion of each component, we have identified the following unordered list of attack approaches. The list items are not fully independent and may have common actions across multiple items.

1. **Man-in-the-Middle** – Be in the communications channel and be able to see all communication. The ability to modify messages, create new messages, or delete messages will exist.
2. **Data Injection** – Be able to inject a message into the communications stream. It would not be necessary to see other messages.
3. **Overload Media** – Denial of service through any means available, such as jamming, cutting wires, overloading network equipment, etc…

4. **Replay** – Be able to capture a message for later injection into the communication channel.

During the course of this research, we determined that #3 was just a denial of service and would most likely be accomplished through other means, not cyber, and therefore was mostly ignored in the rest of the work.

There were more device attack approaches with merit than with the communications attack approaches above. The following list also contains a denial of service type of attack. It too was mostly ignored further as a cyber attack. Only the most likely approaches were developed further in this work.

1. **Break Authentication** – This approach covers many specific attack approaches and includes such things as finding passwords that were written down, breaking weak password encryption, finding a way around the authentication system, etc….
2. **Change Configs** – Modification of any of the configuration files, such as access-control lists, user roles, or ICS configuration will cause the system to lose its security integrity.
3. **Busy Device/Power off** – This is just a denial of service and may be created many different ways.
4. **Social Engineering** – Using social contact to gain, either directly or indirectly, information that will allow the exploitation of the ICS.
5. **Destroy Files –** The destruction of files will allow the changing of authorization, the collection of historical data, and other control functions.
6. **Lifecycle Maintenance –** Through the lifecycle process, files, procedures, access-control lists, and other security significant functions can be affected.
7. **Malware –** Through the use of targeted malware, control of the ICS can be gained.
8. **Change Data –** Some systems use historical operations data to affect the control of processes within the ICS. This feedback type of system can be gamed to change the processing to the detriment of the system owner.
9. **Attack Timing –** Time in an ICS is extremely important. In some systems, incorrect timing of process steps can cause critical problems.

After determining this list, there ended up being an attack approach that was not really an attack, but a method by which quite a number of other approaches could be enabled. That approach is #4, social engineering, and we excluded it from further development in this work.

Likely Targets

Using the terminology found in the Reference Model paper, the targets are listed below in the order of importance to an adversary. This list will be combined with attack approaches and put into a table in the next section.

1. **Data Environment** – This target is the system, communication channel, or other components that contain or pass the current values for sensors and actuators in the system. These are also known as communication processor, front-end processor, I/O controller, etc….
2. **Human-Machine Interface (HMI)** – This component is the interface that system operators use to interact with the Data Environment.
3. **Remote-Telemetry Unit (RTU)** – This component of the system is the part that interacts directly with sensors and actuators. It can have other names, such as Programmable Logic Controller (PLC) or Intelligent Electronic Device (IED).
4. **Historian** – This target is where historical data is collected and stored for use by all parts of the business.
5. **Applications** – This is a class of targets that contains other applications that are unique to each different business, but control some portion of the processing environment.

The intent of an adversary is to gain some measure of control over the system. With the exception of the Historian, the intent we studied was for the adversary to gain direct or indirect control over the system and its functions. The adversary intent against the Historian was to establish a bogus baseline or to change billing data.

Attacks and Adversary Levels

Table 1, in this section, is a combination of information from previous sections, with information about attack approaches and adversary levels added. For some targets, there is more than one "intent" listed and will have different attack approaches listed as well. For each attack approach in the table, there is a list of adversary categories we believe have sufficient capability and resources to successfully perform the attack. In this table, the ranked approach will be prefixed with either a "C" for a communications attack or with a "D" for a device or component attack. Since a category I adversary is the highest level adversary, an adversary level denoted as "(≥ IV)" means adversaries of level I, II, III, or IV are capable of this attack. The "≥" is in reference to the capability of the adversary, not the numerical value of the category.

Table 1 - Correlated Attack Approaches Table

Target	Intent	Ranked Approaches
1. Data Environment	Direct control of ICS	A. D1: (≥ V) B. D7: (≥ IV) C. C1: (≥ IV)
1. Data Environment	Indirect control of ICS	A. D2: (≥ V) B. D8: (≥ V) C. D7: (IV, I) D. C2: (≥ IV) E. C4: (≥ IV)
2. HMI	Direct control of ICS	A. D1: (≥ IV) B. C1: (≥ IV) C. D7: (≥ III)
3. RTU	Direct control of ICS	A. D1: (≥ V) B. C4: (≥ V) C. C1: (≥ IV)
4. Historian	Establish bogus baseline	A. D1: (≥ III) B. D8: (≥ IV) C. C2: (≥ IV)
4. Historian	"Fix" billing data	A. D1: (≥ III)[A] A. D1: (≥ V)[B] B. D8: (≥ IV) C. D5: (≥ V)
5. Applications	Direct control of ICS	A. D1: (≥ III) B. D7: (≥ III) C. C1: (≥ III)
5. Applications	Indirect control of ICS	A. D7: (≥ III) B. C2: (≥ III)

One trend to note from this table is that in general, attacks become harder (requiring a better equipped adversary) as you move from the more desirable targets to less desirable targets and as you move from the more desirable attack approaches to a lesser ones against the same target. This shows consistency from the brainstorm process and was not identified until after the table was put together here.

This table should be used by a system designer and by the system maintainers to identify attack approaches that an adversary is likely to use against their system. They should identify the level of adversary that is of concern to their operation and ensure that additional controls are put in place to mitigate actions taken by that level of adversary. According to the table, if the system has been designed and built according to the specifications in the reference model and best practices paper[3], then it should be able to

[A] This attack is rated for this level of adversary, if the attack is to modify the historian database.
[B] This attack is rated for this level of adversary, if the attack is to modify the information on the business network only.

withstand attacks from a category VI adversary. Additional controls and security mechanisms must be designed and installed if a higher-level adversary is the concern.

Summary

For ICS that are built using the reference model and according to the best practices outlined in the referenced papers, we have postulated a set of generic attack approaches that various adversaries will use to compromise the ICS. It is incumbent on the ICS designer and maintainer to consult this work and ensure that security controls placed within the system are sufficient to mitigate the attacks for adversaries of concern for that ICS.

[1] "Generic Threat Profiles", David P. Duggan, June 27, 2005.
[2] "A Reference Model for Control and Automation Systems in Electric Power", Michael Berg, Jason Stamp, 2005.
[3] "Security Best Practices for Control and Automation Systems in Electric Power Systems", Jason Stamp, Michael Berg, 2005.