**Overview**

Control system security is the practice of using security methods to prevent intentional or unintentional interference with the operation of industrial automation and control systems. These control systems manage the production or use of electricity, petroleum, water, transportation, and many other services. This Industrial Control System (ICS) contains a few underlying technologies and approaches, all of which function and report information in different ways–and over different geographic distances. Decades before the micro-controller was invented, and subsets of ICS did not exist, process control systems used mechanical pneumatics for logic, discrete control systems used relays, and related systems used transistors and radios. As a result, there were significant differences in the underlying system technologies, their functionality, and the roles of anyone tasked with handling them.

When the micro-controller finally came along, field experts realized that the same hardware could feasibly be used to do everything, making the process and its terminology much simpler. Without ICS technologies, processes and machines in the industrial world would not be able to function beyond mere mechanization. If a leak opened up in a pipeline, the system would not know how to gather information and report it. But with ICS systems, overall quality and flexibility in manufacturing, automation, productivity, quality, accuracy, and safety of important fields like health and the environment is possible. Through their reliance on computers, networks, OSes, applications, and programmable controllers, ICSes have come to serve a powerful role in the modern industrial world. And as such, they demand a high degree of overall security and forensic process.

**Types of ICS Architecture**

ICS systems are generally recognized as having a few different levels—from enterprise to process to control—each of which represent a different part of the critical infrastructure hierarchy. The enterprise sits at the top, above process and control, and is the general IT network of an organization where systems are connected as such. Whether they are overseeing a power plant, a public facility, or some other kind of industrial operation, ICS systems must work together to offer effective protection. One single security product, technology, or solution is simply not enough. Instead, a multiple layer strategy involving two or more overlapping security mechanisms—also known as defense-in-depth—must be in place to minimize failure on any one part of the system. This type of security architecture strategy includes the use of demilitarized zones, firewall, and intrusion detections features along with strong security policies, training programs, incident response, and physical boundaries. It also demands a thorough understanding of possible attack vectors on an ICS, like database attacks, spoofing, or backdoor breaches. It is important to note, however, that this evolving technological environment has exposed ICSes to new risks and challenged their ability to handle them.

**SCADA**

These days, the term Supervisory Control and Data Acquisition (SCADA) is well-recognized by most and generally refers to control systems that cover large geographic areas. This includes industrial automations like power transmission, gas pipelines, or water distribution systems—anything that handles the use of control systems like computers, robots, or information technologies. In a SCADA network, the control level functions sit at the center and send coded information to coordinating components of the ICS and the industrial machinery itself. This system is what connects sensors to the broader network and carries data through both wired and wireless networks. Depending on whether its connected to the internet, the information carried by the ICS should be firewalled to prevent against any kind of cyberattack. At least half of SCADA’s job is to monitor remote events (using remote gear) and report valid findings to users. In this way, a SCADA system is event driven and can be effectively used to monitor and control the transport of chemicals and other physical processes that are further away.

**DCS**

A Distributed Control System (DCS) is used to handle production with the same geographic area and is particularly useful in industries like oil refineries and wastewater treatment plants where process control systems function in one facility. As an a piece of a larger control architecture, DCSs supervise the functions of multiple, integrated subsystems that are responsible for control the activities of what is localized. They use centralized supervisory control loops to mediate a group of local controllers with the same basic tasks and help them carry out the production process. To achieve this end, specific process controllers, or powerhouse PLCs, are employed in the field and tuned to provide the correct tolerance of rate of self-correction. In short, a DCS reduces the impact of a single fault on the overall system and can provide businesses a better view of production when interfaced with the corporate network. Local operations are also sometimes controlled by “field devices” that receive supervisory commands from remote stations.

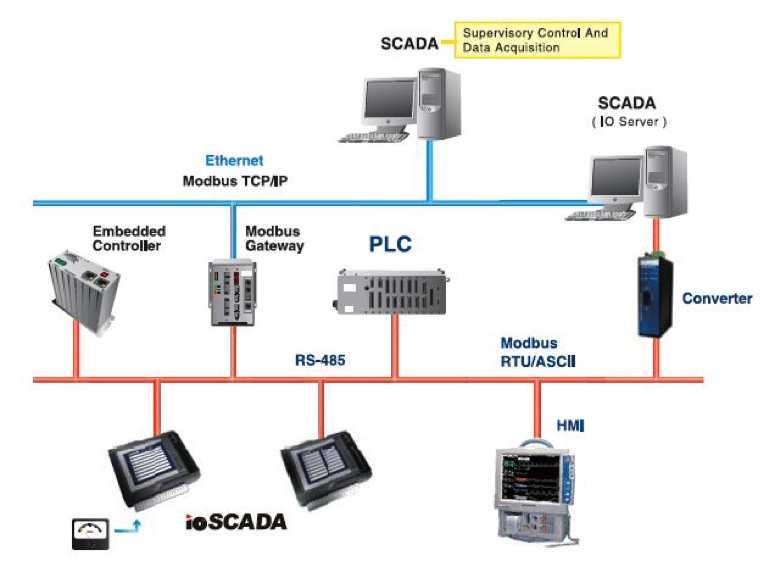
Computer network used to have very little bandwidth, which is why SCADA systems were the top-level controller for many lower-level players. It just didn’t make sense to to have one system controlling every tiny part of a system. As a result, Distributed Control Systems (DCS) hardware did most of the local detail work and simply took orders from (and reported to) the SCADA system. But today, computer networks are much faster, so quick in fact that there’s no practical reason why SCADA and DCS systems need to be separate. So, they have essentially blended themselves to create a single monitoring and control systems which largely depends on what is needed from users.

While SCADA is the preferred technology for monitoring processes spread out over a vast area—primarily because it has distributed intelligence and allows control to continue even when communication to the central hub has been lost—DCS does not have the ability to operate in such geo-diverse scenario. It relies too heavily on local events and has no ability to endure communication outages, even temporarily. In short, DCS is process oriented, while a SCADA system is focused on data-gathering. And while SCADA monitors and controls, a DCS uses a network and certain protocols to interconnect various sensors through communication and process.

It is more integrated than SCADA and can complete higher-end tasks, albeit with far less flexibility and range. However, DCS systems are also used to control industrial processes in areas like agriculture, food processing, and nuclear power power plants, increasing their safety, cost-effectiveness, and overall reliability.

**Non-Centralized Systems**

Some of these control systems do not need central management, as a logic controller can feasibly be configured as part of a larger control system. This type approach is typically found in manufacturing processes.

[](https://mk0resourcesinfm536w.kinstacdn.com/wp-content/uploads/1-137.png)

**What are the Components of ICS?**

In order to respond effectively to incidents of varying degrees, it’s essential for private businesses and government agencies to coordinate their efforts when formulating the right response. This type of formalized management structure is supported by different components of ICS and fosters increased efficiency, knowledge, and direction during times of confusion or difficulty. If a problematic situation is not properly stabilized, it can mean the loss of property, systems, and even lives. Therefore, the control loops, human interfaces, maintenance tools, and remote diagnostics associated with ICS must use an array of network protocols on layered architectures to be successful.

**Sensors and Actuators**

“Smart” sensors are devices used to measure some aspect of physical property before sending findings as controlled variables to the controller. The signal is then interpreted by the controller, variables are manipulated, and control algorithms and target set points are created to transmit data to actuators like control valves, breakers, switches, and motors. This bits of hardware are used to directly manipulate the controlled process based on commands and protocols.

**PLC**

Some general purpose computers such as laptops, desktops, and workstations can participate in the control process, and other times something more serious is needed. A rugged, industrial digital computer adapted to control manufacturing processes is known as a Programmable Logic Controller (PLC), and it plays a major role in things like assembly lines, robotic devices, and any other activity that demands high reliability control, simplified programming, and fault diagnosis. First created in the age of the automobile, PLCs replaced timers and sequencers with a highly reliable form of automated control, capable of standing up to harsh environments and real-time demands. As hardware, they can be designed and arranged to deal effectively with factors like temperature, electrical noise, intense vibration, and even physical impact. Their operations programs are usually stored in battery-backed or nonvolatile memory.

**RTU**

A Remote Telemetry Unit (RTU) can be visualized as a communication hub located near the devices it serves. It is known component of a SCADA system and is used as both a remote hub for collecting information and a relay point for control commands.

**ICS Environment**

Control systems often function in harsh environments like busy factories, electrical substations, or loud control rooms, which means only certain devices will suffice. From vibration to contaminates to humidity, these systems must operate well under less than ideal circumstances. They also operate in real-time which means their security can be so beefy as to limit the efficacy of a security response. Compared to IT systems, they have unusually high uptime requirements and must have a window of scheduled downtime to complete actions like patching. Such a window can take months and force processes to adjust in inconvenient ways. And of course, all of these realities help shape the forensic responses to attack and system issues, as they must take all factors into account.

## What is the Need for ISC Forensics?

So, why would an attacker target an ICS anyway? Turns out, threat actors have a lot to gain from messing with ICSs. In today’s global market, the reliance on natural resources for economic development have led to the creation of some valuable commodities. And with fluctuating geopolitical climates, these industries have become big prizes for cyber criminals who want to disrupt systems, create chaos, and reap personal benefits in the process. Often times these attacks are really more like coordinated campaigns, geared towards achieving certain goals for interest groups, terrorists, hacking groups, competitors looking to gain an advantage in a market-driven global economy, or simply in retaliation to a perceived injustice.

## What Approach Should Be Taken to ISC Forensics?

Forensic considerations must be made when a control systems fails to function properly to ensure a hacker is not involved. If a hostile act is detected through forensic process, actions must be taken to identify the source and harden the control system against similar or future attacks. Although this effort should include a concentration on the central server of a DCS or SCADA system, it is not the only place where forensic technique is needed. Other field devices like PLC or RTU should also be involved in the investigation. In general attacks on a controlled system occur through the configuration workstation, and through both the Ethernet and non-Ethernet networks. Attacks on the workstation can be addressed by applying forensics techniques to the workstation itself, while non-Ethernet attacks are much harder for investigators to conduct without specialized equipment.