Hurricane Katrina Control System Assistance

DHS recognizes many critical infrastructure control systems were shutdown, damaged, or destroyed as a result of Hurricane Katrina. This document provides assistance to owners and operators in rebuilding and securely restarting those sensitive control systems.

US-CERT
Informational Paper

September 16, 2005

Produced by:
United States Computer Emergency Readiness Team – Control Systems Security Center

Hurricane Katrina Control System Assistance

I. Overview

Hurricane Katrina, one of the worst natural disasters in U.S. History, devastated the Gulf Coast of the United States on 29 August 2005. A number of the critical infrastructures within the region were shutdown, damaged, or destroyed as a result of Hurricane Katrina. These critical infrastructures provide electricity generation, transmission and distribution; natural gas production and distribution; petroleum products refining; transportation systems monitoring and control; water supply; wastewater treatment; food production and processing; chemical processing; discrete manufacturing, and numerous other critical functions. These critical processes and functions are monitored and controlled by specialized systems called control systems. A control system is defined as the combination of computers, process control equipment, process interface systems and associated applications which work in concert to monitor and control variables of a technical process and manage the process of interest.

To assist control system owners, operators, vendors, and service providers in bringing control systems, and the sensitive processes and functions they monitor and manage, back into operation as safely and as securely as possible under the circumstances, the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) Control Systems Security Center (CSSC) compiled a set of items to consider when restarting and rebuilding control systems. Point of contact information for requesting assistance from the US-CERT CSSC is also provided in the last section of this document.

II. Control System Restart Issues

The US-CERT CSSC understands that the primary concern of critical infrastructure control system owners and operators during this time of recovery is bringing operations back online as quickly and safely as possible. In addition, DHS CSSC realizes that personnel are operating under difficult conditions and recognizes that systems, components, and associated communications may be operated in ways other than how they were utilized pre-Hurricane Katrina. Response actions taken as a result of Hurricane Katrina could result in short cuts or varying system configurations that could potentially leave systems vulnerable to cyber attacks and introduce other problems.

The loss of major critical infrastructures and associated control systems in the Gulf Coast Region has created cascading impacts across multiple critical infrastructure sectors. During the aftermath of this natural disaster, threat agents with malicious intent may attempt to exploit new vulnerabilities or take advantage of existing vulnerabilities as significant focus and resources are directed to those in need. It is important for the control systems community to be cognizant of threats that may attempt to take advantage of personnel and systems likely to be more vulnerable to both physical and

cyber attacks as a result of Hurricane Katrina. Threats may come from a threat agent who is targeting a specific system or may come from a virus, worm, Trojan or other malicious software that has become commonplace in today's connected world.

III. Putting Control Systems Back Into Operation Safely and Securely

To assist owners and operators in bringing critical control systems back into operation safely and securely, the US-CERT CSSC compiled a list of items for consideration. This list was produced through consolidation of input from a number of public and private control system security specialists.

These suggested items are not intended to replace a company's or facility's Disaster Recovery Plans (DRP) or Continuity of Operations Plans (COOP), which should already be in place and are likely already being executed in response to Hurricane Katrina. These items serve as reminders to ensure security is considered in a range of areas as control systems are placed back into operation. It is expected that some form of damage assessment has already been conducted to determine if control systems, associated components, and communications need to be restarted, repaired, or replaced (rebuilt).

Owners, operators, vendors, or service providers can contact the US-CERT CSSC via the contacts identified in the last section of this document for assistance with any of the items listed below.

Establish Physical Security

- Establish physical security at all sites, whether damaged or not, to prevent anyone from altering or vandalizing equipment.
- Determine which individuals require access to systems and components, including communications systems, and limit access to those individuals.
    - Establish a method to authorize access.
    - Ensure control system, associated components, and communications equipment accesses are logged and tracked.
        - E.g.: Logs should be reviewed several times a day during this recovery period as systems are being brought back into operation.

Establish Personnel Security

- Ensure individuals who will have access to control systems come from trusted and reputable sources.
- If the established personnel familiar with your local systems are not available, then seek the advice of operators in similarly configured facilities, retired staff members, contractors and other persons who may have knowledge of your site-specific conditions and procedures. The US-CERT CSSC can assist in locating

individuals and entities that can help owners and operators return control systems to operation securely.

Establish Configuration Control

- Maintain hardware and software configuration control and tracking to account for replaced or modified components. There may be a tendency, in the rush to get systems operational, to install parts that are not properly configured or patched (temporary fixes often become permanent solutions).
- Monitor disposition of computer equipment and file storage systems that will be removed. Ensure that hard-drives or data does not fall into hands where it may compromise either sensitive operational information or access information (user ID's/passwords).
- Ensure adequate policies and procedures are documented/implemented for secure disposal and destruction of damaged equipment or software.

Verify Hardware

- For replacement systems and components, utilize approved control devices acquired from authorized dealers where possible (avoid possibility of nefarious/covert capabilities being placed into system).
- Perform system/equipment validation and calibration tests on all sensors (as appropriate), devices, IED's, and controllers associated with the system under control prior to placing the system into operation. Repair, calibrate, reconfigure, or replace as necessary.
- Key components may have been looted, causing faulty operation of the overall system. Conduct a complete point-to-point checkout of the system to identify any missing or damaged components. Conduct point-to-point conductivity test, power, I/O, interconnection, cable runs, etc.
- Verify that power system is working adequately. If utilizing an uninterruptible power supply (UPS), attempt to get it working correctly before turning on anything else. If you have to by-pass the UPS, verify that circuits are adequate. Battery backup units could be exhausted; verify operability of backup power.
- Power systems may lock in an "on" state and not be able to be turned off due to hidden shorts. Test or inspect for proper operation.
- Ensure hardware has current firmware (with security updates) installed.
- Ensure systems are set to fail in a "safe" mode.
- Ensure hardware is configured in compliance with established security policies and procedures.
- If possible and where appropriate, manual operation of controlled equipment may be appropriate to identify operational problems before automatic operation is commenced.

Hurricane Katrina Control System Assistance

Verify Software

- Loss of power (and battery backup power) can cause some control systems to revert to a manufacturer default state, including insecure default settings and passwords. Check to ensure appropriate versions of programs are in place and that all passwords are sufficiently secure.
- Prior to restart, verify all firewall and router access lists are in effect.
    - Review settings to ensure unnecessary communications are not permitted on networks (corporate networks or control system networks).
- Take advantage of this period of time while systems are off-line to ensure all software (and hardware) upgrades, patches, and anti-virus programs are in place and operating correctly (particularly security upgrades and patches).
    - Patch and test existing systems.
    - Patch and test any new systems or components that will be installed.
    - Test that anti-virus software will not impact control system performance.
- Ensure systems are set to fail in a “safe” mode.
- Ensure software (applications and programs) are configured in compliance with established security policies and procedures.
- Systems should be secured before being attached to a network. Software downloads should be performed from systems “trusted” to be secure.

Secure Remote Support

- Analyze need for remote support from vendors, integrators, and others who assist with equipment installs, repairs, or maintenance.
    - If remote access is required, ensure is it is implemented securely (including secure identification/authentication, authorization, and encryption) and logs are maintained and monitored.
    - Allow authorized remote support connections to occur only for specified periods of time from specified system/locations.
    - Intrusion Prevention Systems (IPS) and/or Intrusion Detection Systems (IDS) are recommended to monitor these remote connections.

Secure Communication Paths

- Secure external communications to/from control systems.
    - Protect/segregate control networks from Internet and corporate networks to the extent possible.
    - The control system and any associated networks should initially have no, or very limited, external communications before restart.
    - Identify each external connection requirement, analyze, and gain appropriate approval.
    - Develop and implement mechanisms for secure external communication.

  - Ensure all external communications are securely filtered through a firewall or some equivalent device.
  - Monitor external communications with an IPS and/or IDS and review logs on regular basis.
  - Assess business, vendor, and regulatory connections; they may have been compromised or affected by events and could potentially contain malicious code that could spread to your system.
- Secure all telephone/modem connections to control system networks and equipment.
  - Allow authorized, securely configured, modem connections to occur only for specified periods of time from specified systems/locations.
- Secure wireless connections.
  - If wireless systems are going to be implemented to replace or augment hard-wired connectivity for control systems and components, ensure appropriate wireless cyber security measures are implemented.
- If backup communications paths are being utilized instead of "normal" operations communications paths (e.g. backup T1 connection which does not pass through a firewall and was never secured), ensure appropriate security controls are implemented.
- Secure control network internal communications.
  - Ensure communications equipment (routers, switches, firewalls, VPN devices, etc.) and control systems and associated components are secured in accordance with established security policies.

Safely and Securely Start Control Processes

- Ensure for all systems and components repaired or replaced (control systems, actuators, sensors, routers, firewalls, etc.) that an individual was assigned responsibility and implemented appropriate security measures.
- Ensure safety systems are in place and operating properly before attempting to restart control process.
- Equipment grounding and grounding protection equipment should be inspected, tested, and repaired as necessary. This is critical for equipment and hardware torn loose from high winds or flood water debris, or exposed to excessive moisture, chemicals, or toxins which could corrode or degrade their ability to handle short circuit faults.
- If emergency power supplies or generators are utilized to supply temporary power to components of the control system, ensure proper emergency shutdown protection and interlocks are enabled.
- Restart process.
  - Put extra eyes on watching safety and control system displays during restart.
  - Watch for any indication of out-of-the-ordinary performance.

    - If out-of the-ordinary conditions arise, stop safely, retest, reconfigure, and re-build as necessary.
- After everything "checks-out" OK, establish necessary external communications securely as described in section on "Secure Communication Paths."

Taking notes during the recovery process can prove valuable for lessons learned initiatives and for updating relevant DRP, COOP, policy, guidance, and procedure documents. It is recommended that a risk assessment, which includes a vulnerability assessment, be conducted to identify any vulnerabilities which may have arisen as a result of changes made to the control system and surrounding environment.

IV. Control System Assistance Points of Contacts

The DHS US-CERT CCSSC was established to bring together control system owners, operators, Information Sharing and Analysis Centers (ISACs), vendors, industry associations, and subject matter experts to address control systems cyber vulnerabilities and to develop and implement programs aimed at reducing the likelihood of success and severity of impact of a cyber attack against a critical infrastructure. The US-CERT CSSC works to enhance the cyber security of the Nation's critical infrastructure by coordinating government and industry activities and has relationships with relevant federal agencies, National Laboratories, private sector control system entities and subject matter experts to ensure the best available facilities and minds are addressing the critical task of protecting our Nation's control systems used in critical infrastructure.

The US-CERT CSSC would like owners and operators to work with their Sector Specific Agencies (SSA's), Sector Coordinating Councils, and sector ISACs to provide status and share information, lessons learned, and data that can be utilized to develop timely situational awareness on the health of critical infrastructure sectors in the areas impacted by Hurricane Katrina.

DHS would like to inform the control system community that the US-CERT CSSC can provide assistance in ensuring control systems are brought back into operation in a safe and secure manner. The US-CERT CSSC can assist in locating individuals and entities that can help owners and operators return systems to operation and can assist owners and operators with cyber security issues. Requests for assistance from the US-CERT CSSC can be made by contacting the US-CERT via telephone at (888) 282-0870 or by sending an email to soc@us-cert.gov. Information about the US-CERT can be found on its web site (http://www.us-cert.gov).