

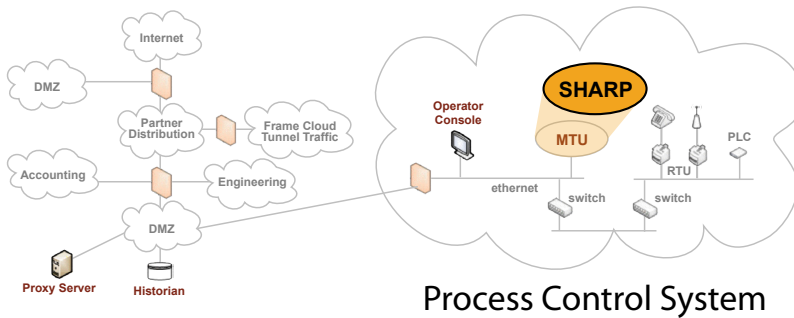
## SHARP

Security-Hardened Attack Resistant Platform  
*Hardening security for existing PCS networks*

Institute for Information  
 Infrastructure Protection

### Overview

The Security-Hardened Attack Resistant Platform (SHARP) provides a vendor with an infrastructure-independent, high-security environment for networked process control systems. The SHARP is designed to be a drop-in component, thus current process control investments are preserved. This architecture is designed to limit access to sensitive data, increase the difficulty of a successful attack and reduce interruption to operations in the event of a successful attack.



SHARP Protects High-value Assets on a Process Control Network

### Key Features and Benefits

The SHARP provides secure remote and local access for operators, integrators, administrators and managers of commercial control system applications and platforms. It incorporates the following features:

- **Enhanced ability to continue operations during an active attack**
- **Control and monitoring of local fixed and removable data storage**
- **User authentication and privilege escalation protection** – unauthorized physical or network access by malicious users or software are detected and blocked.
- **Enhanced tamper resistance**
- **Scalable as needed** –It will scale from one PCS component to many.
- **Encryption** – Includes a cryptographically enforced security-layering model, allowing authorized users or software to perform authorized functions.
- **New approach to security** –provides a fundamentally new architectural approach to PCS security that can serve as the foundation for a trusted computing environment.
- **Can be integrated with other security tools** – For example, can be used with EMERALD (an intrusion detection and alert correlation tool).

### Why are legacy systems hard to protect?

On legacy systems, such as Standard MTU implementations, DCS Controllers, or graphical user consoles, the operating system may provide all the required services. An adversary who successfully gains access to such a system may be able to exploit an application to modify the operating system, stored data, and other applications. Malware may be able to persist despite reboots or system updates. Even when detected there is an increased risk of interrupted operations because the compromised components must be rebuilt from scratch.

### What is Privilege Escalation?

Privilege escalation is the exploitation of a security flaw in a running program in order to gain access to system resources that would normally be of a higher security context than would be otherwise allowed. This bypasses the standard user authentication which is intended to identify users and provide or deny them access to resources. With sufficient privilege an adversary can make their presence permanent and/or alter the system in any manner they choose.

### Combining available technologies for higher security

Technology / Features	SHARP	User Authentication	Linux iptables	Firewall	Audit logs	Boot from CD/DVD with storage encryption	System partitioning
Monitors own integrity	Yes	No	No	No	Poor	No	No
Physical access modification deterrent	Yes	No	No	No	No	Yes	Yes
Availability during attack	Yes	No	Partial	Partial	No	No	No
Prevents attacks	Yes	Yes	Yes	Yes	No	Partial	Partial
Privilege escalation deterrent	Yes	Partial	No	No	No	No	Partial

## Functional Description

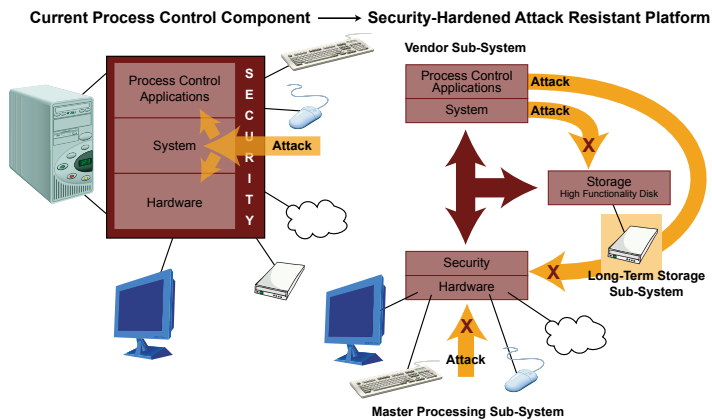
**The Master Processor Sub-System (MPS)** separates the external network from the active Vendor Sub-system. It runs without user interaction to mitigate vulnerabilities and protect against external and internal threats.

- Provides self validation (detects successful attacks)
- Boots from read-only media, any detected coercion is remedied by restart/checkpoint from known good state / restart.
- Validates the other system components
- Provides cryptographic functions to reduce insider and outsider threats

**The Long Term Storage Sub-System (LSS)** provides storage for the SHARP. It runs separately from the other system components

- Secured by limited access using only required protocols
- Can provide encrypted storage to reduce insider threat (this feature is not yet implemented in the current version of SHARP)

**The Vendor Sub-System (VS)** is the high value asset that is protected by SHARP. It can be a legacy MTU, DCS controller or graphical user console. The VS runs as usual with the added protection of the MPS, and the high reliability and security of the LSS.



### SHARP fights attacks to Hardware, System Software and Process Control Applications

- Provides legacy services and capabilities
- Access is restricted to authorized personnel and services via MPS
- Protected from subversion

SHARP employs a File Monitor, Network Monitor, and Memory Monitor. The File Monitor looks for policy violations in VSS-LSS communications and responds accordingly (e.g., by interrupting or reversing the activity, alerting operations). The Network Monitor looks at ingress and egress sides of the MPS network stack and uses a policy-based decision engine to adaptively respond to network based denial of service attacks. The Memory Monitor looks for unexpected changes in MPS memory process images. The system can respond by restarting the process from an image stored on CDROM.

## Technical Description

The SHARP secures the process control network using standard commercial computing platforms and other technologies that securely monitor and control data input/output and storage. The SHARP does the following whenever possible:

- Use minimized operating systems to reduce complexity thus reducing the number of attack vectors.
- Partition – place high value, harder to secure systems behind high performance (low latency) systems to enhance security and monitoring.
- Harden the environment of each system.
- Separate the access privileges of each system. For example, the system administrator for the low-security partition can be a different person than the administrator of the high security partition.

## Summary of Costs

	Low	Medium	High
<b>Component</b>	<\$1,000	\$1,000-\$10,000	>\$10,000
<b>Engineering</b>	Drop-in	Moderate modification	Complete System Design Lifecycle
<b>Bandwidth/Network Burden</b>	None-Passive Only	Moderate Traffic, Medium Overhead	Heavy Traffic, Large Overhead
<b>Training</b>	No training required	Moderate training	Intensive training. Additional staffing may be required.
<b>Maintenance and Operation</b>	< 1 hour per week	< 5 hours per week	> 5 hours per week

**Technology Transfer and Readiness:** Bench-tested.

For more information about the Survivability and Recovery of Process Control Systems project, visit:

<http://www.thei3p.org/projects/pcs07overview.html>

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.



The I3P is managed by Dartmouth College.