assessment was the router configuration. There were a total of 426 different tests run on both the individual (IOS) routers and (CatOS) switches as well as the total network as a whole (the latter involving simulating traffic on the network to determine the viability of the routing configuration between routers and switches).

[redacted]

Figure 4-6. [redacted]

Of the 426 test that were run, no major errors were detected [redacted]

[redacted]

4.6 System Performance Monitoring

The team obtained information from interviewed employees of HEC, ITD, HFD, HPD, Greater Harris County 9-1-1 Emergency Network, and Northrop Grumman to discuss how the performance of the systems were monitored. [redacted] The team primarily focused on the monitoring capability for the HEC portions of the public safety system and the ITD networks. A similar analysis needs to occur for the HPD and HFD systems.

During interviews with ITD, MITRE was informed that the ITD may set up a Network Operations Center (NOC) to provide centralized network management functions for several organizations including HEC. The idea is still at early inception stage and the scope focuses only on detecting network outage alarms and providing centralized problem resolution in a timely manner. The NOC will also report uptime and downtime statistics. In other words, the function of the planned NOC is mainly to react to incidents when they occur. [redacted]

The Scope of Service identifies requirements for system performance monitoring. During interviews with HEC IT staff and Northrop Grumman, MITRE attempted to gain an understanding of what tools were in place and how they were used for monitoring and reporting system performance.

The interviews showed that the system is not being adequately monitored and reported. Basically, the HEC IT staff and Northrop Grumman have a process for system monitoring and reporting on an as needed basis. This process is put in place whenever an outage or significant lack of performance occurs. The process that is in place during normal operations is not clear.

The following paragraphs provide a brief description of possible network monitoring tools that could be used. Some of these capabilities exist in Northrop Grumman's existing configuration but are proprietary. The City of Houston should determine if these proprietary tools could provide the monitoring capabilities needed or if commercial tools are needed.

Performance monitoring and reporting tools fall into three broad categories that are applicable to the system:

- Client monitoring
- Network and server monitoring
- Application-level monitoring

The client monitoring tools gathers metrics about the end-user experience, such as response time for specific interactions in the application. It may be useful for measuring CAD Transaction Response, as defined in Section 15.10.3 of the Scope of Services. [redacted] However, these applications are data-intensive and should only be used as a tool to occasionally gauge the system load to aid in the decision on allocating resources.

Network and server monitoring tools monitor the performance of system infrastructure, connection status, and assist in error detection. They usually use SNMP and RMON agents with real-time event filtering for fault alerting and problem resolution. For non-SNMP equipment, a protocol mediation solution or a proxy agent can mediate standard alarm outputs from various types of equipment to SNMP. They can collect statistics and report throughput, uptime, data link utilization, CPU usage, packet loss, packet latency, etc. Some platforms may also be able to check on connections involved with any given application and provide information about the host server as well. Basic SNMP statistics collection, storage, exception reporting ("Top-N" lists, etc.) and historical trend graphing are built in to most of the major network monitoring platforms, and there are a number of commercial products focused specifically on performance. Concord Communications is one of those with the broadest coverage and largest customer base. HP OpenView series of solutions also provide comprehensive monitoring capabilities. There are also open source tools (MRTG is widely used). HEC is currently considering adopting a network performance monitoring tool.

It must be noted that generic tools used for monitoring network performance usually are not capable of detecting application-level problems. A better approach for application-level monitoring is application instrumentation, which involves writing specific code within an application to check key transaction performance indicators, such as message queue length, waiting time, and completeness of transaction. It may also report other measurements; e.g., response time, database connectivity, system load, etc. An application-monitoring tool may help avoid some of the incidents;, e.g., B4, B5, B6, B9, B10, and A2 from happening again.

A caveat application instrumentation is an invasive method that requires modifying the original application and may be too resource-intensive. The Application Response Measurement (ARM) and Application Instrumentation and Control (AIC) technical standards and APIs have been published by an industry consortium for some years and adopted by a number of leading providers of performance monitoring tools. The system managers can monitor transactions by using simple function calls embedded in the application code. An agent captures these calls and sends them to an ARM or AIC reporting application, such as the IBM Tivoli Management Environment platform. This popular platform is by far one of the best solutions in the industry to enable end-to-end management of all elements in a multi-vendor environment, from the network, to computers, to applications and databases, and to business management of IT services. Northrop Grumman has stated that the ARM tech suite is installed by default. The tool can monitor CPU performance by user and additional functions are available through all-on licenses.

Computer Associates' Unicenter monitoring environment also has a built-in functionality that can provide application-level monitoring. The AIC standard was based on Unicenter's TNG management software. The Insight Integration for CA Unicenter can integrate HP hardware monitoring and event notification functions into Unicenter. Together they provide an integrated platform for managing and monitoring systems and business applications. As stated at the HP web site:

> "This comprehensive, scalable solution builds upon the core elements of Insight Management to complement and extend Unicenter, and to maximize existing IT investments. Network environments that implement Unicenter as the preferred enterprise management platform can use the Insight Integration to help streamline administration and increase systems availability."

Since HEC has already chosen HP System Insight Manager as part of the server management strategy, the combination of Unicenter and Insight Manager seems a suitable candidate and is recommended.

There is a 3-page document called HEC System Monitoring Policy, Draft V1, with the following purpose:

> "The purpose of the Security Monitoring Policy is to ensure that Information Resource security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measuring, Limiting Liability, and Capacity Planning."

This policy focuses on security monitoring. It requests that automated tools be used to perform real-time monitoring of Internet traffic, email traffic, LAN traffic, and operating system security parameters. It also requests that some logs and records "be checked for signs of wrongdoings and vulnerability exploitation at a frequency determined by risk." Although Performance Measuring is listed as one of other benefits, there is no specific procedure or data requirement defined.

The policy also states:

> "Currently, all security monitoring is conducted [redacted]

The Altaris® CAD System Manager's Guide prepared for HEC by Northrop Grumman describes eight categories of daily and weekly tasks for monitoring the system performance:

[redacted]. Some of these commands can also be organized in scripts associated with UNIX cron processes to facilitate scheduled monitoring. However, the current guides and practices do not show the employment of automated problem alerting. Without on-site 7x24 support, the collected information cannot be interpreted in time either. It is agreeable that all these tasks are useful; without them, other incidents may have occurred. Nevertheless, some problems slipped through and caused substantial outages. To reduce the hit or miss situations, the following strategy should be considered:

- Perform more frequent checking.[9]
- Provide adequate analysis and interpretation of the collected information, e.g., trending and correlation with historical events. Some (but not all) application-level problems may be reflected upon system performance data. To discover this causal relationship requires collecting and interpreting data collected over a long period of time.

---

[9]There has been a concern that more frequent monitoring might cause degradation of the system performance. The concern is legitimate; however, it should not deter adequate monitoring. The HEC system computing power and network bandwidth are designed to handle above the current workload. It is unlikely that they cannot accommodate the resource requirements for monitoring. On the other hand, a proper planning for capacity should take monitoring requirements into consideration.

- Use automated monitoring tools with comprehensive coverage and robust performance. The automation is not just for automating data collection; it should also do automated event identification and filtering using the relationships obtained from the analysis above.

The Altaris CAD System Manager's Guide also provides a comprehensive list of troubleshooting steps for problem identification and resolution after a problem has occurred.

4.7 Security

[redacted]

5 Process Analysis

In addition to assessing the technical performance of the system, MITRE evaluated the engineering process that were or should be in place to support the overall end-to-end system performance. This analysis is applicable to the overall public safety data and radio systems. As explained in this section, the HEC processes are primarily analyzed but the outcome and recommendations apply to all City of Houston departments public safety data and radio systems. Some of the processes assessed included the following:

- Configuration management to monitor and control the system baseline.
- Risk management to identify areas that may negatively impact system performance, raise these levels to appropriate management level, and plan budget.
- Change management to prepare staff and employees for new methods of doing business and systems operations.
- Requirements management to ensure users have method to identify requirements; system is designed and tested to satisfy requirements.

Our analysis showed that from an end-to-end perspective, the City of Houston engineering processes are fragmented and very few processes are documented. Informal processes do exist in some areas but the effectiveness of these undocumented processes is very hard to evaluate. This section identifies the informal critical processes that are in place at the HEC and then suggest two critical processes that need to be established, risk management and configuration management. This section also discusses two other important items that need to be addressed: training and testing. The criticality of establishing processes can first be shown through the analysis of the outages that occurred.

5.1 Outage Cause Summary

A summarization of the type of problems resulting in the system outages and relevant processes and practices are presented in Table 5-1. This table shows MITRE's analysis of whether the lack of formal processes and practices may have contributed to the outage. The "Relevant Processes" column identifies applicable processes while the "Relevant Practices" column shows applicable practices. The notations in the "Relevant Processes" and "Relevant Practices" columns in Table 5-1 indicate that these processes and controls are relevant to the type of problem encountered. They do not indicate that there was a deficiency in the indicated process or practice, but indicate focus on that process or practice could prevent or minimize similar problems in the future.

Table 5-1. Processes and Practices Relevant to the Outage Problems

Legend: D - Directly control; I - Indirectly control

Time Line		Requirements Management	Configuration Management	Deficiency Reporting	Risk Management	Test & Evaluation	Continuity Management	Release Management	Continuous Process Improvement	Integrating Vision	Acceptance Testing	Involving Stakeholders	Documentation	Usability	on-going support	Maintainabity	Checklists	Training
		Relevant Processes								**Relevant Practices**								
Sep-03																		
	9/24/2003	D	I		I								I	I	D	I	D	D
	9/30/2003	D									I				D	I		D
Oct-03																		
	10/2/2003				I		I						D				D	D
	10/8/2003				I	I	I											
Nov-03																		
	11/5/2003				I		I											
	11/7/2003				I		I											
	11/10/2003					D												
	11/16/2003				I		I											
	11/28/2003				I		D										D	D
Dec-03																		
	12/3/2003				I		D										D	D
End of Acceptance Testing																		
Jan-04																		
Feb-04																		
Mar-04																		
Apr-04																		
	4/10/2004				I		I								D			D
	4/25/2004				I		I								D			D
May-04																		
	5/10/2004				I		I									I	D	D
Jun-04																		
Jul-04																		
Aug-04																		
	8/8/2004		D		I		I								D	D	D	I
Sep-04																		
Oct-04																		
Nov-04																		
Dec-04																		
	12/1/2004		D	I	I		I											D
	12/7/2004																	
	12/14/2004				I	I	I											

A look at the outage data (Table 4-2, 4-3, and 5-1) shows that many of the problems encountered in the outages are the result of insufficient training or human error. In fact, as explained in Section 4.2, the majority of outage time can be contributed to insufficient training or human error.

Only two of the outages were the result of requirements. In both cases, human error caused the wrong requirement to be provided. Thus, MITRE concludes that the requirement management process used has been sufficient. However, there were two incidents where the lack of adequate configuration control had a major impact. In a couple of these instances, the problem causing an outage was repeated later. This reoccurrence indicates that the problem resolution process may not be adequate since the actual cause of the first outage was not resolved sufficiently to prevent it from reoccurring a second time.

Table 5-1 shows that institution of risk management and continuity management would be beneficial in the likelihood of decreasing the outages occurring. A risk management process could have identified potential problems before they became outages. A risk management process will make the City of Houston more proactive in assessing and improving the performance of the overall system. The purpose of a risk management process is to identify risks and prioritize them so that limited funds can be spent where they will have the most beneficial impact on the program.

Table 5-1 also shows that a continuity management process could have a beneficial role in most of the outages. The continuity management process is not only responsible for the contingency plan in the event of an outage, but also evaluates other changes that could minimize the chance of an outage in the event of the type of problems seen. MITRE noted that the City of Houston has an effective process for continuing operations during system outages. The "paper" process adequately maintains the degree of call taking and dispatching operations needed for emergency services. The chart was primarily focused on continuity of operations for the CAD system and should not be misunderstood to indicate there is no continuity management.

5.2 Critical Processes

MITRE assessed and evaluated processes applicable to all departments and those within the HEC. The major process or strategic planning activity that relates to the scope of this assessment was the City of Houston Executive Order "Policy to Direct and Monitor Technology Efforts." As stated, the purpose of the Executive Order is to establish and communicate the City's technology strategic direction. The Technology Steering Committee, or a committee of equivalent scope, could provide a forum to oversee and pursue the recommendations made in this report.

The team was unable to find documented engineering processes that were applicable to and being used by all departments. Thus, MITRE recommends that the City of Houston identify and adopt policies and procedures that implement critical engineering processes such as problem resolution, risk management and configuration management. Next, the MITRE team reviewed HEC policies and interviewed HEC staff to identify processes in place at the HEC. Table 5-2 contains a list of the process, the applicable policy and general status information.

Table 5-2. HEC Processes

Process	Applicable Policy	HEC Process Status
Risk Management		No formal process
Requirements Development & Management		Uses a system of functional design and detailed work packages to manage requirements.
Configuration Management		Informal process in place for change control.
Enterprise Integration		No formal process.
Integrated Testing		Internal testing process. Individuals test requirements using a loose test plan that tests all functionality.
Capacity Management		No formal process.
Continuity Management		No formal process.
Incident Management	Software Incident Report Tracking (SIRT) Form	On a "by exception" basis.
Change Management	HEC Change Management Policy draft	As implemented, a change control process not change management.
Change Control		Informal exists.
Release Management		No formal process.
Service Management	Maintenance Agreement	No formal process.
Problem Resolution		Informal process exists.
System Enhancement		Informal process exists.