Table 3-1. [redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

While the CAD system is the core system used by the call takers and dispatchers, there are many other systems (applications) required to be available and functioning in an optimal manner in order to efficiently and effectively enable communications between the call takers, dispatchers, and HPD/HFD response personnel when responding to 911 emergency incidents.

Other key components comprising the City of Houston's public safety system are shown in Table 3-2:

Table 3-2. [redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

The above list highlights those device components also required to be operational in order for all data to be successfully transmitted to and from the CAD system. In the event that any one of the above device components is not properly functioning, back-up procedures are activated in order for HPD/HFD emergency response personnel to continue responding to 911 emergency incidents.

[redacted] Table 3-3:

Table 3-3. [redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

The Tables depict the various groups involved in the end-to-end delivery of the HEC IT portfolio. Figure 3-1 illustrates the complexity of the operations and support for the public safety system. Root cause analysis of a perceived system problem may require multiple organizations to become involved in order to validate and verify that their particular scope of supported component is not the root cause of the problem or issue being experienced. Finally, outages to the system may be prolonged due to differences in service levels from the various groups identified below. While some groups and organizations provide 7x24 support for their components, other groups are only responsible for delivering support during regular business hours Monday through Friday.

As is the case with the device components and subsystems, public safety system performance may become degraded or unavailable to all or portions of the public safety system users when any of the above systems are not properly functioning. While back-up/contingency processes and procedures are instantly activated in order to eliminate disruptions to 911 emergency operations, unavailability of any of these components may have a performance impact to the CAD system.

The architecture was evaluated for possible single points of failure. This analysis primarily focused on the CAD, RMS, MSS, SAN, and network and did not address the possible failure of the radio, EAS, or PBX systems. For purposes of this assessment, single point failure analysis explored the impact of the majority of users being denied access to computer resources necessary to carrying out their mission. Based on the design of the HEC infrastructure, key systems such as CAD and RMS have been redundantly maintained [redacted] In addition, alternative systems to support voice via radio interface can function without the need for CAD or RMS and still permit the dispatch of resources (while somewhat less efficient than if CAD were available). Therefore, if CAD were to shut down, the ability to use Orbacom in conjunction with the call taking front end still permits the emergency dispatch function to occur. The following is a list of potential single points of failure that should be further studied and remedied:

- [redacted]
- Data Interfacing to MDT and RMS-HPD system from/to CAD.
- SAN Architecture.
- Integrated Database – Integrating CAD and RMS-Fire.
- [redacted]

3.2.1 [redacted]

[redacted]

3.2.2 RMS-HPD System From/To CAD

The next single point of failure addresses loss of services within 61 Riesner even when network services are available. While the CAD at HEC has a redundant design for both Fire/EMS and HPD, HEC only supports a redundantly configured RMS for Fire/EMS. A corresponding RMS-HPD exists at 61 Riesner that is not redundantly configured – implying a server failure (RMS-HPD) will result in down time with no failover option (as exists for the RMS-Fire/EMS at HEC).

The team was concerned that a past CAD outage resulted in problems at RMS-HPD [redacted] causing CAD to "hang" due to large queue backlogs that were unanswered. This problem has been resolved through upgrades to memory and processor functions.

3.2.3 Storage Area Network Architecture

The primary disk storage supporting the [redacted] was designed to support a high degree of redundancy from a RAID design as well as provide mirror imaging to another system (connected via a SAN) that could be used for recovery in the event of catastrophic failure of the primary RAID system. However, the implementation of the storage environment does not provide for real-time dynamic failover (it was neither specified in any requirements nor tested during acceptance). The intent of the components that are used in the design is primarily for disaster recovery. [redacted] In the event the primary RAID fails, the secondary system (which is basically a mirror image of the primary) is "resurrected" and becomes the primary system (until manually switched back to the backup role). This resurrection process is manual and can take many minutes depending on the disk configuration. [redacted] Network storage systems do exist that can provide real time dynamic failover but the current implementation does not provide that level of support.

3.2.4 Integrated Database – Integrating CAD and RMS-Fire

The database failover capability is primarily oriented at ensuring that when the primary system fails the system fails over to the backup system. This capability supports redundancy but does not adequately address other critical areas that need to be planned for to prevent database failures from causing outages. As noted in the review of the outages, one or more of the longer outages related to human error associated with the CAD/RMS databases. While disk mirroring can protect against catastrophic equipment failure, human error that erases the database is instantly "mirrored" to the backup disks. At that point, reconstruction of some type will be necessary to have an operational system. The best protection against this type of failure is to prevent it through better process management (configuration control practices). Other database improved performance measures can include:

- Database management tools exist that can create checkpoint rollbacks for certain types of transactions.
- Database replication with properly configured delays to remedy human error.

- Other database tools that can analyze the impact of a change prior to that change. Further analysis would need to be conducted to determine the best tools and techniques to mitigate this type of potential failure.

[redacted]

The team also noted that the current database version used in the system is Oracle 8. Oracle 8 is not fully supported by Oracle Corporation. Several security vulnerabilities have been identified with Oracle 8 and patches are not being provided to remedy these vulnerabilities. Oracle 9i can improve the reliability, security, maintainability, and performance of the system. For example, Oracle Real Application Cluster (RAC) is provided with Oracle 9i and it has distinct advantages over Oracle Parallel Server (OPS) used by Oracle 8.

RAC, introduced with Oracle 9i, is an advanced version of OPS with many additional self-tuning, management, and data warehousing features.

Oracle 9i introduced many new features to help the database administrator such as the ability to change database configuration "on the fly," enhanced availability, automatic performance and configuration tuning, and enhanced manageability. Given the nature of how past database administrator activities have led to system outages, the additional functionality reduces the risk of making a wrong decision that impacts the overall operations.

3.3 Systems Operations and Support

The public safety operations includes call takers from HEC, and dispatchers from the Houston Fire Department and the Houston Police Department. The primary roles are:

- Neutral 911 Call Taker
- HEC Call Taker (Fire/EMS)
- HFD Dispatcher
- HEC Call Taker (Police)
- HPD Dispatcher
- Supervisor HEC Call takers (Fire/EMS)
- Supervisor HEC Call takers (Police)
- Supervisor HPD Dispatch
- Supervisor HFD Dispatch

Appendix B provides a description of the call takers and dispatchers functions and how they operate the system.

4 Performance Analysis

This section analyzes the performance of the public safety data system. The analysis includes investigation of past records, interview results, and recently captured data traffic to determine whether the system performs in accordance with the scope of services and if it meets normal service level requirements. The analysis also assesses on other factors which provide past and current measurements of success performance. Specifically, this section discusses the following:

- Analysis of system outages that occurred from the period September 2003 through December 2004.
- Estimates of operational and inherent availability.
- Workload statistics.
- Scope of services performance analysis.
- Reliability assessment.
- Network configuration analysis.
- System performance monitoring.

4.1 Analysis of Outages and Errors

The scope of incidents considered in this report is based on the "HEC Outage Status" Excel spreadsheet and the "CAD System Availability From September 23, 2003, through December 16, 2004." The outages documented in the spreadsheet caused system-wide downtimes. Downtime is defined as a period of time when the system was unavailable to the call takers and dispatchers).[3] In all but two outage incidents,[4] the system was completely at the down state, and all users had to use some other means to get their jobs done. Isolated problems are identified in another report called the Software Incident Report Tracking (SIRT) and are analyzed separately.

The total assessment period for the HEC availability covers from September 23, 2003, 04:00, when the live operation of the upgraded system commenced, till January 31, 2005, 23:59. The upgraded system was accepted on January 2, 2004. In Section 4.2, two sets of availability calculations are provided, one for the total assessment period starting from the live operation commencement date, and the other for the shorter assessment period starting from the acceptance date.

[3] See Section J of Scope of Services: *CAD & RMS Acceptance Test Plans*, Page 11.

[4] For two outages CAD was able to operate partially. But, during these two incidents, either new logons could not be established or new emergency events could not be recorded. For incident # B10, all systems eventually had to be shut down.

Seventeen outages have occurred since the system went live. Table 4-1 shows a short summary of these outages. Ten of them occurred before system acceptance in a period less than 3 ½ months, and are labeled B1 through B10. After the acceptance, the frequency of outages has been significantly reduced, with only seven outages occurring over a period of almost 12 months, but their recovery times were generally longer. These outages are labeled A1 through A7. Each downtime period of an outage consisted of corrective downtime, preventive downtime, and/or delay time (for lack of logistic or administrative support). The last two outages were scheduled repairs and hence considered as preventive downtimes.

Table 4-1. HEC System Outages

Incident #	Date	Start Time	Total Time (hours)	Corrective downtime (hours)	Preventive downtime (hours)	Delay time (hours)	Problem	Cause	Device (Location)
(System went live and the acceptance test period started on 23 Sep 2003. This period had 10 outages: B1 – B10.)									
B1	9/24/2003	?	0.23	0.23			Incompatible software upgrade (for MDC sign-on) and human error	The down time was caused by an attempt by Northrop Grumman to install a software upgrade relating to MDC unit sign-on	CAD
B2	9/30/2003	16:00	0.08	0.08			Software bug		CAD
B3	10/2/2003	21:50	0.28	0.28			External interface and human error	Root cause was a network problem at 61 Riesner. The network problem was diagnosed to	CAD and SNA gateway @ Riesner

Incident #	Date	Start Time	Total Time (hours)	Corrective downtime (hours)	Preventive downtime (hours)	Delay time (hours)	Problem	Cause	Device (Location)
								be caused by the backup SNA gateway computer	
B4	10/8/2003	21:58	0.45	0.45			Software bug (system deadlock)		CAD
B5	11/5/2003	12:15	0.25	0.25			Software and client-server communication	Root cause was a network problem at 61 Riesner	CAD and workstation @ Riesner
B6	11/7/2003	17:21	0.12	0.12			Software and client-server communication	Root cause was a network problem at 61 Riesner	CAD and workstation @ Riesner
B7	11/10/2003		0.62	0.62			Software bug (archive logging)		CAD
B8	11/16/2003	22:08	0.25	0.25			Hardware failure (memory module)		CAD
B9	11/28/2003	8:30	4.38	4.38			Software bug (database lock) and procedure error		RMS and CAD
B10	12/3/2003	14:05	0.98	0.98			Hardware failure (RMS memory module) and software bug (database lock		RMS and CAD

Incident #	Date	Start Time	Total Time (hours)	Corrective downtime (hours)	Preventive downtime (hours)	Delay time (hours)	Problem	Cause	Device (Location)
(System was accepted on 1/2/2004)									
A1	4/10/2004	0:30	3.18	2.18		1.00	Database configuration mistake and human error (Northrop Grumman DBA)	Problems with expansion of the data table	CAD
A2	4/25/2004	16:26	0.90	0.90			Software bug (memory leak)		CAD
A3	5/10/2004	15:10	12.00	12.00			Human error (system admin to backup database)	Programmer issued a command at the Operating System (UNIX TRU64) level that caused the problem	CAD
A4	8/8/2004	12:10	5.00	5.00			Hardware failure (SAN disk array controller) and human error (HP)	Error on the HP technician part on loading a previous version of the firmware	SAN
A5	12/1/2004	7:30	8.00	8.00			Hardware failure (SAN disk array controller) and human error (HP)	Bad disk controller	SAN