

Trustworthy Computing

Dependable and Trustworthy Enterprise System

YOUNGHO HAN

May 4, 2006

Table of Contents

OVERVIEW	3
Advent of Internet	
New Business Opportunities	
Requirements for Enterprise Systems	
Risks on Enterprise Systems	
Exemplification of Risks	
The Interruption of Business Systems	
The Impact of Unplanned Downtown	
Review of Key Concepts and Managerial Issues	6
Review of Applications and Practices	7
Disaster Recovery	
System Partitioning	
Security	
Examples and Cases	11
Reliable, Flexible and Cost-effective System in K Life Insurance Company	
Security Policy in Samsung Electronics	
Emerging Trends, Applications, and Issues	13
Fault tolerant system	
On-demand computing	
Conclusions and Findings	14
Annotated References	15
Appendix	16

Overview

Advent of Internet

Until about 20 years ago, client/server environment was a dominant concept with respect to designing enterprise systems. Almost all of business transactions were initiated, executed, and finished by internal employees at that time. In the meantime, a new concept in designing enterprise systems emerged. It was Internet. The impact of Internet was so tremendous that it has caused huge changes in business people's minds by showing them new types of business opportunities. With the advent of Internet, companies attracted by the merits of Internet began to introduce the web-based environment that allows for direct transaction involvement of customers in their enterprise systems, unlike the traditional client/server environment that used to be bounded internally.

New Business Opportunities

Since the web-based environment encouraged average customers to become more proactive and dynamic in buying patterns, companies acquired greater chances to get access to those customers to a great extent. Specifically, business transactions between companies and customers become more instantaneous, convenient, and ubiquitous. Consequently, Internet enabled companies to serve a greater number of customers, while it allowed customers to be more aware of companies through easy, fast, and open information.

Requirements for Enterprise Systems

As the web-based environment offers companies greater business opportunities, enterprise systems are required to have more and better attributes such as high reliability, availability, and security as well as high system performance and capacity. Coping with such attributes is

critical to companies' business success because missing those attributes can result in losing both current and future business.

Risks on Enterprise Systems

In the past when the client/server was the industry norm in designing enterprise systems, it was relatively easier for companies to handle contingencies and risks associated with their enterprise systems. Since most of their business transactions took place internally by their employees, relatively less uncertainties were involved in running their enterprise systems. However, unlike the traditional client/server environment, the Internet environment provides an enormous amount of business merits but, at the same time, considerable uncertainties and risks. Exhibit 1 shows regular customer demands trend over time.

Exemplification of Risks

To be considered a dependable and trustworthy computing system, addressing potential contingencies is essential. In particular, it is also important to prevent both potential problems and respond fast and effectively to them once they happened. Among a variety of cases of potential risks, several examples are described as follows.

Sudden increase in customer demands

An enterprise system can sometimes face abrupt soaring in customer demands. In this case, the system cannot handle the transactions requested from customers because the customer demand overwhelms the actual system capacity, possibly resulting in a system down and business loss due to the deficiency.

Unexpected system down and disaster recovery

There are myriads of factors that can cause a system failure. At many times, it is important how fast an enterprise system can recover from the disaster and resume its service to customers.

Data loss

As Internet prevails, the amount of data that companies handle increases virtually at every second. Also, business data increasingly contains private, confidential information, which is critical to the business. Thus, data protection and backup is necessary in running enterprise systems.

External attacks

After the advent of Internet, corporate information and system has been exposed to the public and under the fire of anonymous attacks such as from hackers. Increasing security and protecting systems from outside attacks is an aspect that needs to be paid attention to.

The Interruption of Business Systems

If a business system is interrupted, it will experience some serious financial losses, in many cases these can be fatal and these losses are no longer covered by insurance. Should any of the fundamental functions within a business be disrupted then inevitably the lack of cash flow will prevent the company from deploying capital to keep the business running. The ultimate risk is that credit ratings suffer, shares go down, the business is unable to fulfill the legal requirements of suppliers' contracts, customers lose faith and may never return, and significant costs can be associated with restoring servers and systems.

The Impact of Unplanned Downtown

According to the findings Tatsunori Shibata of NEC Corporation from Contingency Planning Research, it is noted that the hourly cost of downtime ranged from US\$28,000 for companies in the manufacturing sector to \$6.5 million for the brokerage sector. This could explain why, in a recent study of US brokerage firms' web sites, the top five performing sites achieved 100 percent availability without a single instance of peak downtime during a month-long study by Keynote Systems, a web performance monitoring firm. Another famous example is eBay. In June, 1999, all bidding was suspended at eBay for about total 22 hours. eBay had to shut down its enterprise systems, rebuild the system disks, and transfer the data from the backup. The disaster caused about \$5 million revenue loss and, even worse, \$5 billion worth of corporate value loss due to deteriorated credit.

Review of Key Concepts and Managerial Issues

Key Concepts

Since the introduction of Internet, one of the new, 24x365 has entered the business field as one of the new, key concepts. This simple combination of numbers connotes the importance of continuous service for customers in various business situations by delivering 24 hours and 365 days service. Not to mention the greater business potential, the emergence of Internet and web-based business environment also enlightened companies on the requirements for enterprise systems that can satisfy the markets needs for continuous services. Furthermore, how to design and implement such continuous systems has been a challenge for business enterprises. When it comes to enterprise systems, high performance is now considered nothing but a necessary condition. To achieve the 24x365 concept in designing dependable and trustworthy enterprise systems, the enterprise systems need to be armed with high reliability, availability, flexibility,

and security. The requirements for the 24x365 environment stimulate IT companies to develop more advanced technologies that involve features and solutions such as fault tolerant components, disaster recovery, data backup, partitioning, and security policy.

Managerial Issues

While the requirements for enterprise systems increase to make them more dependable and trustworthy, managerial issues regarding such dependable and trustworthy enterprise systems become more challenging than ever. The first primary issue is cost. For instance, to make a server more fault-tolerant, many components of the server are designed and built in redundancy. Also, a backup network can be built in case that a primary network gets into failure. All these kinds of redundancy plans entail a significant amount of money at many cases. For this reason, it is no wonder that the management rigorously evaluates the potential outcome of its investment. Typically, the management would do risk analysis based on the potential impact associated with the cases of business system interruption. Another issue for the management is complication of its enterprise systems. Since Internet enabled end consumers to get closer to enterprise systems, the enterprise systems need to cope with a wider range of customers and more uncertainties that contribute to the complication of the enterprise systems from perspectives of both technology and operation. Lastly, another issue for the management is operational errors. In other words, although a company built a technologically perfect system, it could have failures due to employees' incaution or misconduct.

Review of Applications and Practices

To build a dependable and trustworthy computing system, enterprises make a wide range of efforts for virtually all functions of their IT environment from hardware to software to network.

The following technologies have been applied, selectively or widely, to enterprise systems.

Disaster Recovery

The degree to which enterprise systems handle mission critical applications has increased over time. Particularly, since the 9/11 disaster, the importance and interest in disaster recovery systems have become greater than ever. Under a business environment where 24x365 services to customers are critical, even a short period of system down can cause tremendous impact on the company's business performance. Therefore, the key concept on the disaster recovery solution is how fast and reliably one backup system can take over the primary system's applications to minimize the business impact. By capitalizing on disaster recovery solutions, companies can enhance their enterprise systems in terms of reliability, availability, and serviceability.

The Functions of Disaster Recovery Solution

Continuous heartbeat communication between systems either by IP heartbeat or by serial network heartbeat enables systems on a cluster to check the status of each other in real time. The causes of failures are normally found in such categories as system nodes, network adapters, and networks. (Exhibit 2)

Modes of Disaster Recovery Solution

- Mode 1: Hot Standby

A backup system is on standby. Once it recognizes any symptom of failure on the primary system, the backup system comes begins to run by taking over the applications and shared resources managed by the primary system. The backup system will serve until the primary

system comes back on the cluster.

- Mode 2: Mutual Takeover

The way one system takes over the other system is virtually as same as the hot standby mode. However, the difference is that in this setting, one of the two systems is defined as neither primary nor backup system. Instead, each two system runs its own applications. Once one system falls down, the other system takes over the applications of the system going down. This mode setting is normally used for the case in which both systems run their own critical applications or both of them can afford the workload of the other system.

Process of Takeover and Recovery

- Sever Problems

Sever B takes over the disks that used to belong to Server A with problems.

Server B activates the secondary network interface and takes over the A's IP address.

Server B serves for the clients of Server A.

- Network Adapters Problems

IP address is transferred to the standby network adapter from the primary one.

The primary network adapter takes over its role back from the standby adapter after being repaired.

- Network Problems

The network adapters in the backup network will be activated with new IP address.

The whole of a backup network will take over the primary network.

System Partitioning

Thanks to the advent of Internet, the number of customers who would cause the transactions load on enterprise systems varies substantially. In reality, varying demand can affect the utilization of business systems. If a system is underutilized due to a smaller number of transactions, the system can handle all the transactions with no problem but can make the management concerned about cost efficiency. On the other hand, if the system confronts too much demand beyond its capacity, it may not handle all the transactions, leaving a high possibility of system down. Partitioning is one technological concept that can offer enterprise systems greater flexibility and cost efficiency.

The Functions of Partitioning

Instead of having one type of operating system in one server, a company can implement multiple operating systems and applications in one sever by drawing on the partitioning solution. Then, the server can change allocation of application capacity, depending on situations. Small unit of system components such as processor, memory, disk, and adapter can be assigned to each partition that virtually works as an independent system.

Security

Since the business world became more open and connected, the security issues become more important. Along with the increasing importance and alert to security issues, companies have increased their protection level and structure in their enterprise systems. Besides the enhancement in the system level including operating system and more protective firewalls, companies also strive to enact stricter security policy, since human errors are considered one of the major causes for security problems. Thus, the enterprise systems reflect security policy in

its functions.

Examples and Cases

The continuous efforts for a dependable and trustworthy enterprise system have made by many business enterprises in the real world.

Reliable, Flexible and Cost-effective System in K Life Insurance Company

In 2004, K Life Insurance launched a server consolidation project in which the company would consolidate ten scattered, independent servers into two IBM high-end servers. Before the project was launched, each of ten servers had run different applications ranging from a small-scale like web application to a large-scale like CRM application. CRM were underutilized for most of time except for the few times a year. Meanwhile, web servers were overwhelmed by an extreme number of incoming transactions from consumers who wanted to get a quotation or product information, whenever K Insurance introduced a new production promotion. With the completion of the project, all the ten applications were transferred into the two high-end servers that are connected by IBM HACMP, a disaster recovery solution with the mutual takeover mode. Beside the implementation of the disaster recovery solution, the two servers were equipped with logical partitioning technology that enabled the two servers to change each application capacity along with situations. For instance, during the period of a new product promotion, the system extended the capacity of web applications to accommodate a greater number of transactions and simultaneously reduced the capacity of CRM application that was not much in use. Additionally, the system allocated roughly 1GB memory and 20GB hard disk for the development of a new, in-house application on a next-version operating system. After the new application development was finished, a new partition for the new application service was allocated in the

system. The consolidated systems with two solutions dramatically reliability, availability, and flexibility as well as better performance due to higher-performing processors and cost effectiveness due to lower system maintenance costs.

Security Policy in Samsung Electronics

When it comes to security policy, it is recommended to follow the industry standard where a company belongs. Also, the company can customize security policy along with their interests and preferences. Depending on each company's focus, a security policy can be either preventive or reactive or both in its characteristics. Samsung Electronics is a company of which security policy has more of preventive characteristics than reactive. The company is very meticulous and strict especially regarding its employees' communication activities such as email and commercial messenger programs usages. Some exemplary provisions in the IT policy are as follows.

1. No file attachment on any outgoing messages without approval from the management
2. Random inspection on employees' email
3. No USB outlets or recordable drives on any personal computers issued from the company
4. No messenger programs allowed to use and blocked by the system

According to US Patent and Trademark Office, as of 2005, Samsung Electronics ranks as the number 5 private organization with the most number of patents. It may be interpreted that the internal knowledge and information is considered so critical that the company applies a rigorous policy to any kind of outgoing communication vehicles. This specific policy is reflected on the enterprise system design and implementation. For instance, the email server checks each outgoing emails automatically and keeps the log of its transactions for further investigation.

Also, a communication server has the information of certain commercial messenger services such as MSN Messenger, so that it blocks all the communication relevant to those programs.

Emerging Trends, Applications, and Issues

Fault tolerant system

While the goal of high availability configurations is to help firms recover quickly from a crash, that is not good enough for fault tolerance or for continuous availability, which seeks to eliminate the recovery time completely. For the complete fault tolerant system, it is essential to build a system with full redundancy in all types of hardware and with complete contingency scripts in software. Companies – especially those in the financial services and telecom industries – have used fault tolerant configurations to protect some of their most vital and core applications for several years now. But ecommerce and globalization have now upped the ante, driving demands for continuous levels of service availability across a wide spectrum of enterprises. However, in spite of such high reliability, completely fault tolerant systems are forecast to be adopted by a limited number of customers who would not allow for even 30-second system down because achieving full redundancy requires an enormous amount of money for companies.

On-demand computing

Business enterprises increasingly confront uncertainties on a daily basis. In order to let themselves to respond to unexpected changes and risks with flexibility, companies are advised to modify their business model from the traditional way to the on-demand way. In the traditional business model, the increase of their IT capacity was lumpy due to ineffective demand forecast and inefficient system operations. Thus, it was natural to have imbalance between actual

customer demand and enterprise systems' capacity: sometimes too little or too much. (Exhibit 3 – A) For the past few years, the concept of on-demand computing has prevailed and it is considered to offer a greater degree of flexibility that enables enterprise systems to cope with abrupt increase of demand. (Exhibit 3 – B) This new way of designing and managing IT systems enables the enterprise systems to minimize the reserved capacity, so that it can provide the management with an advantage of cost reduction. Eventually, customers can pay as they use, which implies that they can save a great amount of money for IT systems. However, the issues regarding the on-demand computing is a lack of references. More reference cases will provide greater trust in the new technology for potential buyers and further encourage them to willingly invest in the on-demand computing systems. Additionally, Exhibits 4 shows how flexibly an on-demand system can handle different system resources usage by different applications.

Conclusions and Findings

As the business environment becomes more open, companies and their enterprise systems need to handle a greater number of customers and thus plenty of uncertainties and potential risks. Plus, enterprise systems increasingly deal with mission critical applications with no stop. In this sense, the importance of reliability and uptime as well as performance is an essential part of enterprise systems. Since a short period of system down can cause a tremendous negative impact on a company image as well as on its financial structure, business enterprises strive to make their system more reliable, flexible, and protective. At the same time, companies also search for technology that can present them not only more dependable and trustworthy systems but also cost-effective systems.

Annotated References

IBM, <http://www.ibm.com>

IBM, Introduction of HACMP, 2003

IBM, Comparison of LPAR Technology, 2004

IBM, pSeries On-Demand, 2004

IBM, pSeries References

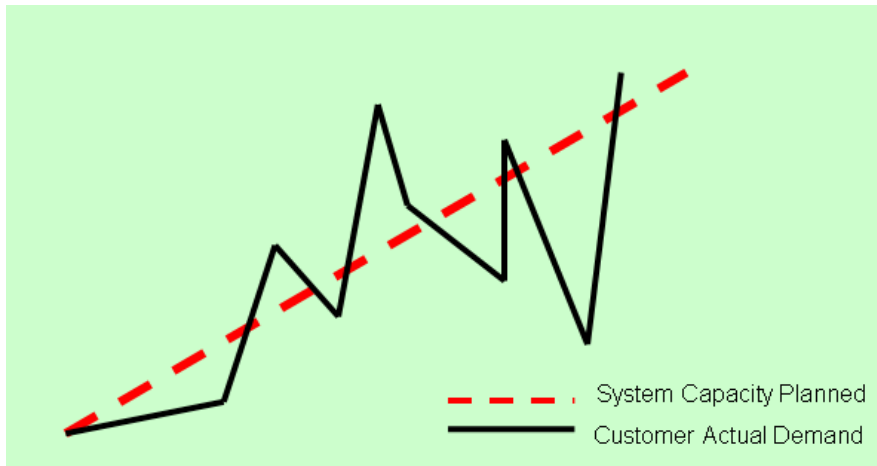
AME Info, <http://www.ameinfo.com/>

Computerworld, <http://www.computerworld.com.sg/>

US Patent and Trademark Office, <http://www.uspto.gov/>

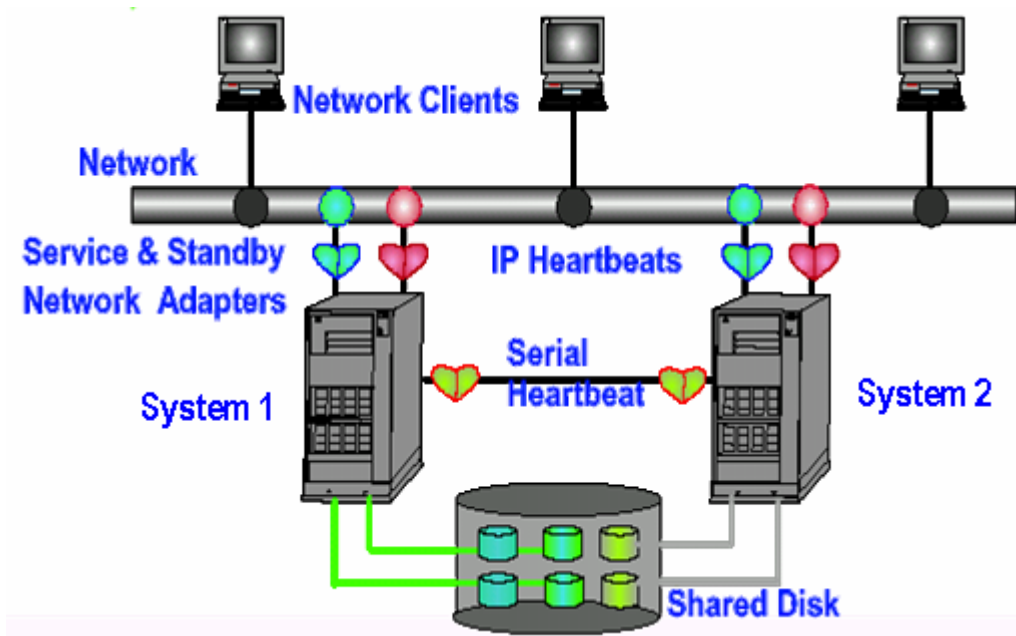
Appendix

Exhibit 1 Customer Demand VS System Capacity in Regular Situations



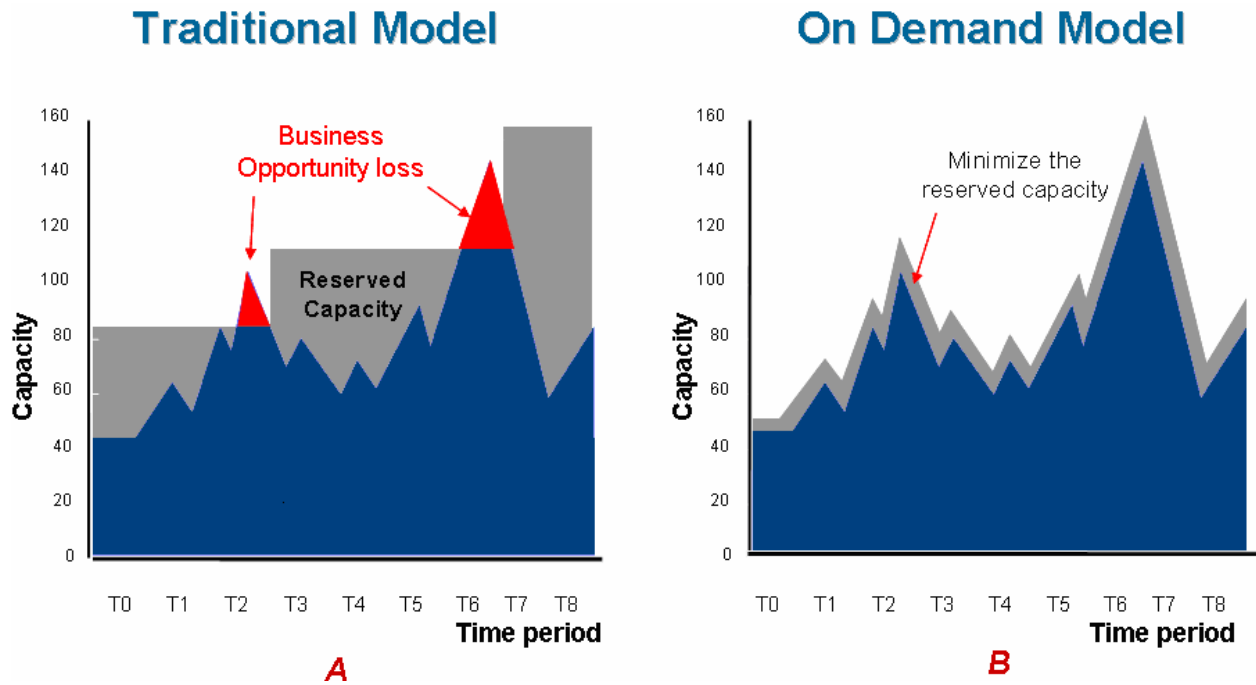
Source: IBM, pSeries On-demand, 2004

Exhibit 2 Brief Configuration of a Disaster Recovery System



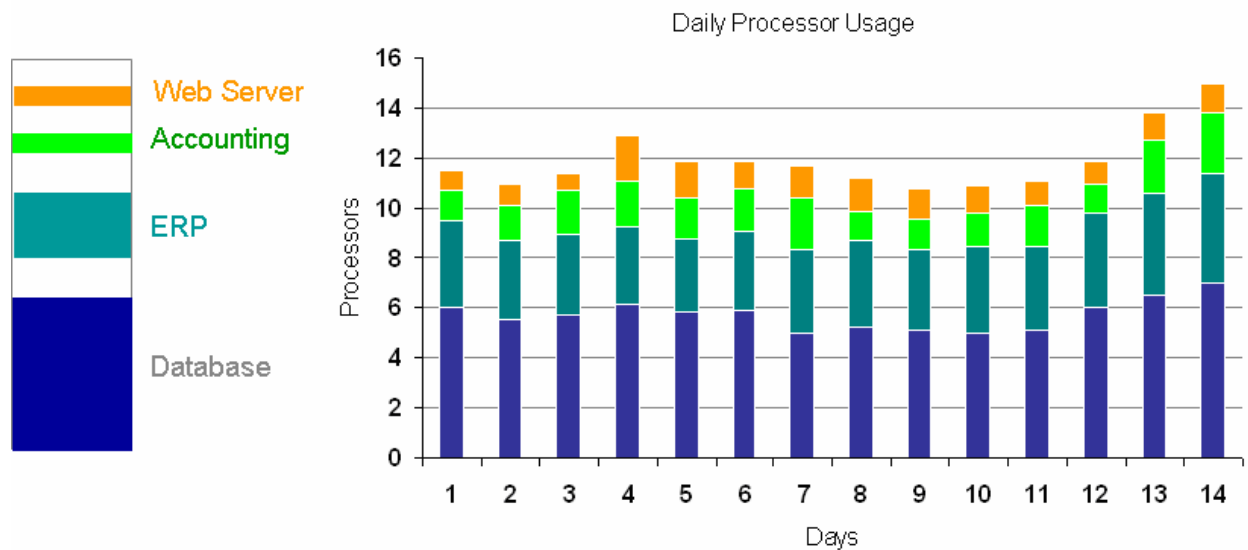
Source: IBM pSeries HACMP Solution

Exhibit 3 Comparison of On-Demand Model to Traditional Model



Source: IBM pSeries, On-Demand Business, 2004

Exhibit 4 Different Application Usage and On-Demand



Source: IBM pSeries, On-Demand Business, 2004