Continuity of System Processing after Disasters

Usman Waheed, Mobeen Nazar, Mahawish, Misbah Perveen

Department of Software Engineering, Bahria University, Karachi Campus, Sindh, Pakistan
usmanwaheed.bukc@bahria.edu.pk , Mobeennazar.bukc@bahria.edu.pk, mahwishfatima.bukc@bahria.edu.pk

Abstract— In today's modern world, as our dependence on software systems increases more & more, the risks of catastrophic disasters that range from system failure to natural disasters also increases. These disasters threaten our most fundamental works because of our dependence on these systems. There we must have effective techniques regarding Continuity of System Processing so that if however, a disaster struck, we could continue our functions. This research is aimed at documenting the most common problems that can happen during and after disasters and their solutions to help these systems continue processing. The most common problem attached to most of the disasters is a disruption in service availability. Almost all systems face this risk after disasters. This Problem can also incur other problems such as losing system & database backups, unauthorized system takeover, no system restriction, and permanent data loss. In near future with the development of more complex systems, processes & business functions requirements, enterprises have to deploy a new set of techniques related to process continuity based on the complexity of requirements, processes & different increasing risks. These new measures along with the other enhanced systems will ensure lesser chances of process discontinuation.

Index Terms— Process Continuity; System Continuity; System Backup; System Restoration; Data Loss; Risk Assessment Plan; Reciprocal Arrangement; Manual System; Fault Tolerance; Event Reconstruction; Cascading failures; catastrophic failures.

1 Introduction

A disaster is an event that can cause by a single point failure that can cause system-wise malfunction and outage of the result. System failures include the disfunctioning of connected functionalities in the system that can include cascading failures or catastrophic failures [16]. Cascading failures successively weakens the system and can cause a catastrophic outcome in the form of blackouts in man-made infrastructure [17, 18].

"The ability to sustain processing in the event problems occur. Continuity of processing ensures that the necessary procedures and backup information are available to recover operations should integrity be lost [1]."

Continuity of Processing assures that "If a disaster has caused the system to stop its processing, the system must be able to restore to its previous state before that of the disaster to be able to perform its tasks." So, the function of continuity of processing is to assure that the user can easily perform all the required work on the system and the disaster doesn't cause the function interruption. This paper provides the main problems that can occur during when any disaster/ failure can occur on the system and all the possible solutions to solve these problems.

The main concern this paper provides is the solutions & strategies to continue operations uninterrupted despite the occurrence of a disaster [16].

2 Background

Many times, the critical systems availability problems arise due to negligence of process continuity planning. This could result in service disruption. No backups, unauthorized takeover, no system restoration & permanent losing data [2].

2.1 No Service Avaliability

The main problem after any disaster happens at the site of the system is the unavailability of systems services. As the severity of a system grows the importance of the availability of its service grows [3].

For example, a potential threat of fire just started at the business company's main headquarters where all business systems are located to process the services for its clients, the services will be stopped due to this disaster which results in user displeasure. Service unavailability is the main common reason for business system failure.

2.2 No System & Database Backups

The key staff doesn't have a system & its updated database backup. This is a severe problem. If the staff responsible for backing up the system's process & data doesn't have backup data information, they will not be able to re-continue the system processes [4].

For example: In the previous example where the system responsible for business processes was already in the implemented environment. When the disaster happens and the service stopped, the maintenance staff most likely will not have any system & database backup resources reserved for addressing this situation because this problem has not been addressing before. So this will delay the system restoration to a more extent which will eventually lead to more costly restoration.

2.3 Unauthorized System Takeover

Most of the unauthorized systems access likely happens when the systems are not secured or have already lost integrity due to any disaster [5].

For example: If the company's systems have been stopped from services by disabling firewalls, it is most likely that the hackers will try to access these systems because of no security which will lead to the disclosure of private data.

2.4 No System Restoration

If systems are processing important data transactions & a disaster occurs leading system to not respond within time, then

there are chances that the current transactions will lose its current state & will have to be restarted from the initial state [6].
For example: If a client is transferring his data to the system meanwhile system crashes due to any disaster, if there are no backups to support the process, the user will have to transfer his data again from the starting point when the system is restored after a disaster.

2.5 Permanent Data Loss

If there are no backups, all the systems are centered in one location & no contingency plan is established, we will lose our critical system data permanently due to the disaster.
For example: Since the company's all servers were directly hit by fire disaster and since there was no immediate backup reserved to resolve the problem, the company loosed more than half of its data permanently & were only able to recover half of it at a high staggering cost [7].

3 STRATEGIES

The problems that are previously described in this research paper can be resolve or can be controlled with the help of the following strategies.

3.1 Fault-Tolerant Systems

These systems are specially designed & developed around the special functional & nonfunctional requirements of the clients. These systems can continue working to a level of satisfaction even when the disaster has happened. These systems ensure that if any disaster happens, the critical process must run in any possible way [8].

- This strategy will help in reducing the chances of No Services Availability when the system is struck by a disaster such as a system failure.
- In a fault-tolerant computer system, programs that are considered robust are designed to continue operation despite an error, exception, or invalid input, instead of crashing completely; resilient networks continue to transmit data despite the failure of some links or nodes.
- A fault-tolerant design enables a system to continue its intended operation, possibly at a reduced level, rather than failing, when some part of the system fails.

3.2 Hot Start

This is perhaps the most common & expensive method to be used in the event of any disaster & is also called "immediate recovery". This option is used for special critical services in software systems that cannot be tolerated without response for a length of time. A hot start option provides immediate restoration of system services [11].

- This strategy is useful for solving the No Service Availability problem. In this strategy, there should be a backup system or server. In short, it will be a copy of the original server, or whenever a system stops working then immediately copy server will continue the ongoing process.

3.3 Reciprocal Arrangement

This strategy involves forming any type of arrangement with another System that has a similar purpose & process. For example, if the system services become unavailable then the other same system which performs some other processes can provide services to a customer in the time of disaster for some time [9].

- This strategy will reduce the problem, of no service availability because in this strategy duplication of the system is done. There are some ways of duplication like the warm site, cold site, hot site, etc.
- The organization will simply use their uncritical system in the replacement of the critical system. Hence the system continues to work until the problem with the critical system is not resolved. Also, this strategy solves the problem of permanent data loss. In this, Organization keeps their same data as in the original one so when they lose data in the critical systems, this system helps them get back data in shot possible time.

3.4 Event Reconstruction

The event log is a record of all processes of the system including alerts and notifications. This Event log is analyzed by the specialists to understand & solve the possible reasons for the discontinuation of the system process. We can detect the culprit behind the discontinuation of the system process if we reconstruct the sequence of events in which the disaster happened which will help us in avoiding this problem in the future [12].

- This strategy can help understand & resolve problems & issues related to unauthorized access. In this scenario, experts see what are the steps that can be taken to get unauthorized access to the system.
- This strategy will reconstruct the events that led to the disaster happening. They analyze the digital footprints left behind in several ways. Once the main reason of disaster is identified, the patch is used to cover the loophole.

3.5 Contingency Plan

There have never before been more prevalent, persistent risks to our systems and data. Today the need for drawing up contingency plans emerges from the thorough analysis of these risks. A contingency plan is a plan devised for an outcome other than in the usual (expected) plan .It is often used for risk management when an exceptional risk that. Though unlikely, would have catastrophic consequences [10].

- Contingency planning is useful for reducing the chances of having No System & database backups. It describes how an organization will deal with potential disasters when they happen. It's also useful in thinking about other ways like what happens when 'PlanA' doesn't work as expected? Sometimes Plan A simply means 'Business as usual'. PlanA is your first response to deal with an identified risk – and when PlanA doesn't work, you use PlanB.

3.6 Manual Systems

The Manual system strategy is that to run similar processes besides the main system process. So, if the main system goes down or unexpectedly any disaster comes resulting in an unresponsive system and

gets data lost with no backup to respond, the manual system can help [13].

- The manual system is useful when the system & its data is completely lost. It helps to resolve the situation created by permanent data loss. In this manual system is rum besides the computer system and whenever a disaster occurs company can restore their data from the manual system.

3.7 Proper Documentation

Formulating detailed recovery process documentation is the main aim of the entire IT disaster recovery planning project. It is in this documentation that you will set out the detailed steps needed to recover your IT systems to a state in which they can support the business after a disaster. Proper documentation will help your IT staff to recover systems easily within less time [14].

- This strategy helps in understanding the system & its functions making it useful for the staff to understand how the system could be accessed unauthorized.
- Also helpful in resolving no system & database backups. If proper documentation is exists, then IT staff can work with the help of documentation in order to recover system by following the documentation which describes that what are the steps taken previous.
- It also solves permanent data loss. All data that lost will also be maintained in the manual or documentation so through which that can be restored.

4 PROBLEMS AND SOLUTIONS

Table 01 shows the problems discussed above with strategies that have been discussed to solve these problems. This table includes the problems which are described on the left side of the table and their respective solutions on the right on the top of table 01.
Table 1 describes that No service availability can be solved by fault-tolerant systems [8]. Hot starts & Reciprocal Arrangements [11]. No system Backup Problem can be solved by adopting a contingency plan & paper documentation techniques [10, 14]. Unauthorized access can be stopped by Event reconstruction & paper documentation [12, 14]. System restoration can also be achieved by event reconstruction [12]. Permanent data loss can be neglected by using Reciprocal arrangements, manual system & proper documentation [9, 13, 14].

5 CONCLUSION

The paper described the details, problems & strategies that could be implemented to preserve process continuity in modern systems. The biggest risks arise due to fault occurrence, system failure, and others. Process continuity in systems is achieved by the mentioned techniques that keep the system working after any disaster. Proper documentation is the technique through which most of the problems can be solved so this research paper recommends that a company should have proper documentation to protect their systems from permanent Data loss, unauthorized access, and no system & database backups.

Table 1: TABLE 01 PROBLEMS & STRATEGIES OF PROCESS CONTINUITY

Papers	Problems / Strategies	Permanent Data loss	No System Restoration	Unauthorized Access	No System Backups	No Service Availability
[8]	Fault-Tolerant Systems	N/A	N/A	N/A	N/A	Remain functional to a degree in disaster
[11]	Hot Start	N/A	N/A	N/A	N/A	Have an alternative system site
[9]	Reciprocal Arrangements	Have a backup processing system	N/A	N/A	N/A	Use the uncritical system in place of critical
[12]	Event Reconstruction	N/A	Trace show system stop functioning	Trace the system offender	N/A	N/A
[10]	Contingency Plan	N/A	N/A	N/A	Always ready for worse	N/A
[13]	Manual System	Don't stop working	N/A	N/A	N/A	N/A
[14]	Paper documentation	Personnel know-how system works	N/A	Personnel ready to stop offenders	Everyone knows what to do in disasters	N/A

REFERENCES

[1] Davison, R. (2007). Project pre-check: The stakeholder practice for successful business and technology change. Victoria, BC: Trafford.

[2] Moh Heng, G. (1996). Developing a suitable business continuity planning methodology. Information Management & Computer Security, 4(2), 11-13.

[3] Gray, J., & Siewiorek, D. P. (1991). High-availability computer systems. Computer, 24(9), 39-48.

[4] Blumenau, S. M. (1999). U.S. Patent No. 5,875,478. Washington, DC: U.S. Patent and Trademark Office.

[5] Fallara, Peter. "Disaster recovery planning." Potentials, IEEE 22.5 (2003): 42-44..

[6] Nagata, T., & Sasaki, H. (2002). A multi-agent approach to power system restoration. Power Systems, IEEE Transactions on, 17(2), 457-462.

[7] Wang, Y. F. (2010). U.S. Patent No. 7,774,643. Washington, DC: U.S. Patent and Trademark Office.

[8] Koren, I., & Krishna, C. M. (2010). Fault-tolerant systems. Morgan Kaufmann..

[9] Bandura, A. (1978). The self system in reciprocal determinism. American psychologist, 33(4), 344.

[10] Chakravarthy, S., & Mishra, D. (1994). Snoop: An expressive event specification language for active databases. Data & Knowledge Engineering, 14(1), 1-26.

[11] Chrabaszcz, M. (2001). U.S. Patent No. 6,263,387. Washington, DC: U.S. Patent and Trademark Office.

[12] Gladyshev, P. (2004). Formalising event reconstruction in digital investigations(Doctoral dissertation, University College Dublin)

[13] Holsapple, C. W., Whinston, A. B., Benamati, J. H., & Kearns, G. S. (1996).Instructor's manual with test bank to accompany decision support systems: a knowledge-based approach. West Publishing.

[14] Parnas, D. L. (1994, May). Software aging. In Proceedings of the 16th international conference on Software engineering (pp. 279-287). IEEE Computer Society Press.

[15] Lawler, C. M., Szygenda, S. A., & Thornton, M. A. (2007, April). Techniques for disaster tolerant information technology systems. In 2007 1st Annual IEEE Systems Conference (pp. 1-6). IEEE.

[16] Szygenda, Stephen A., Thornton, Mitchell A., "Disaster Tolerant Computer and Communication Systems", Department of Engineering Management, Information and Systems & Department of Computer Science and Engineering, SMU, 2004

[17] Nedic, D. P., Dobson, I., Kirschen, D. S., Carreras, B. A., & Lynch, V. E. (2006). Criticality in a cascading failure blackout model. International Journal of Electrical Power & Energy Systems, 28(9), 627-633.

[18] Reis, S. D., Hu, Y., Babino, A., Andrade Jr, J. S., Canals, S., Sigman, M., & Makse, H. A. (2014). Avoiding catastrophic failure in correlated networks of networks. Nature Physics, 10(10), 762-767.

[19] Jansen, W. A., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing.

[20] Lee, P. A., & Anderson, T. (1990). Fault tolerance. In Fault Tolerance (pp. 51-77). Springer, Vienna.

[21] Turoff, M., Chumer, M., de Walle, B. V., & Yao, X. (2004). The design of a dynamic emergency response management information system (DERMIS). Journal of Information Technology Theory and Application (JITTA), 5(4), 3.

[22] Haerder, T., & Reuter, A. (1983). Principles of transaction-oriented database recovery. ACM computing surveys (CSUR), 15(4), 287-317.

[23] Chung, L., & do Prado Leite, J. C. S. (2009). On non-functional requirements in software engineering. In Conceptual modeling: Foundations and applications (pp. 363-379). Springer, Berlin, Heidelberg.

[24] Hiatt, C. J. (Ed.). (2000). A primer for disaster recovery planning in an IT environment. Igi Global.