DISASTER RECOVERY OF EAST JAVA DISTRIBUTION CONTROL CENTRE

Haryanto WS
PLN Distribution East Java – Indonesia
haryantows@pln.co.id

Indra PERMANA
PLN Distribution East Java – Indonesia
indra.permana@pln.co.id

ABSTRACT

The reliable SCADA systems can not survive when natural disasters, fires, or other security threats that can damage system equipment occurs. In such circumstances, the utility company must strive to overcome the problems and quickly restore the supply of electricity to customers. Therefore we need a recovery system to maintain the reliability of the integrated SCADA system called SCADA system Disaster Recovery.

This paper discusses the development of a disaster recovery system in SCADA systems in East Java. Disaster Recovery SCADA systems works if SCADA system outages in a region due to an interruption or a natural disaster, the SCADA system operations can be handled by other SCADA systems in the region.

INTRODUCTION

East Java Distribution Control Centre (DCC) is a unit of PT. PLN (Persero) Distribusi Jawa Timur which in corporate structure is under Java Bali operation directorate of PT. PLN (Persero) Indonesia. East Java DCC has responsibility to manage 20kV distribution electricity system in East Java province which consist of 29 districts. Totally, East Java province is about ± 47.922 km² and number of population is 37.070.731 people. Until the end of August 2012, the number of customers has reached 15.414.504 (12.763 MVA), and system peak load of 4.216,7 MW was reached in Juli 2012.

East Java's power system capable of approximately 2.200 MW. There are distributed to customers using 20kV Feeder from 95 Main 150kV Substation with total 981 feeder. East Java DCC is divided into 3 operational pattern of the electrical power distribution systems, as shown in figure 1.

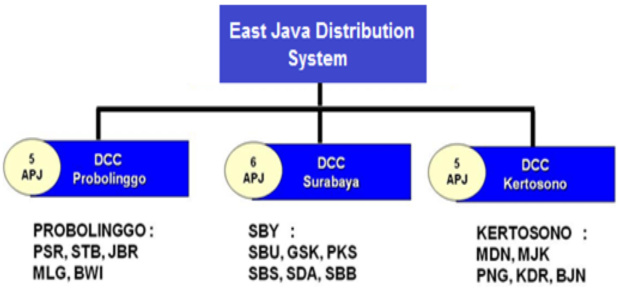

East Java Distribution System
5 APJ
DCC Probolinggo
6 APJ
DCC Surabaya
5 APJ
DCC Kertosono
PROBOLINGGO : PSR, STB, JBR MLG, BWI
SBY : SBU, GSK, PKS SBS, SDA, SBB
KERTOSONO : MDN, MJK PNG, KDR, BJN

Figure 1 Operational pattern of electrical power distribution

The idea to develop general pattern of power distribution system recovery is triggered by a widespread power outage events that occurred between June-September 2011. This idea arose because of the eruption of Mount Bromo that causes Pasuruan, Situbondo, Jember, Malang and Banyuwangi area affected by volcanic ash from Mount Bromo and have caused widespread power outages in the area. With the completion of the recovery pattern of the power distribution system is expected every activity of power distribution system recovery can be carried out in right steps, systematically and short time.

GENERAL FORMAT

The following is a map of the geographical distribution SCADA system operating region in East Java:

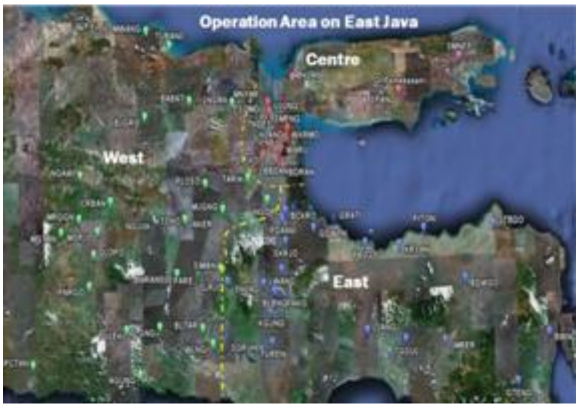


Figure 2 Geographical Operation Area

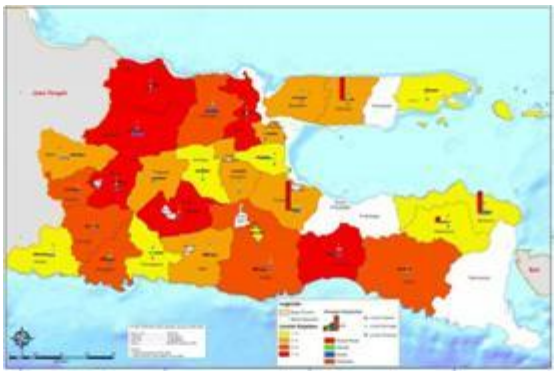


Figure 3 Map of Disaster in East Java during 2008-2012

Based on the record of natural disasters that occurred between the years 2008-2012, it can be seen that there is a potential threat of disaster in East Java that may interfere operation of the SCADA system, namely:

1. Catastrophe
2. Fire
3. Terrorism

Thus we need to anticipate recovering SCADA system, by placing the master station at two points in different locations.

DISASTER RECOVERY PLAN

A disaster recovery plan (DRP) is a documented process of procedures to recover and protect a business information technology (IT) infrastructure in the event of a disaster. Such plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster. It is "a comprehensive statement of consistent actions to be taken before, during and after a disaster". The disaster could be natural or man-made. Man-made disasters could be intentional (for example, an act of a terrorist) or unintentional (that is, accidental, such as the breakage of a man-made dam)..

The needs of Disaster Recovery SCADA System

The reliable SCADA systems can not survive when natural disasters, fires, or threats of terrorist occurs. Therefore we need a recovery system to maintain the reliability of the integrated SCADA system called SCADA system Disaster Recovery. SCADA system Disaster Recovery works if the SCADA system outages in a region due to an interruption or a natural disaster, then the SCADA system can be handled by the other SCADA system in the normal area.
SCADA system Disaster Recovery also must be able to accommodate the operational pattern of electrical power distribution arrangements that are already running as shown in figure 4.
Based on the operational pattern of the electrical power distribution systems and the existing SCADA master station which is located in Surabaya (Central) and Probolinggo (Eastern), the disaster recovery SCADA system applied in both master stations.

Disaster Recovery System

The SCADA System Disaster Recovery can be described as follows:
Breakdown of SCADA System Disaster Recovery APD East Java:

a. Using four pieces SCADA Server, which is consists of two redundant servers in DCC Probolinggo (Eastern) and two redundant servers in Surabaya DCC (Central).
b. There is Workstation Client in DCC Kertosono (Western) with the main SCADA server in Surabaya DCC (Central) that communicate using 2 Mbps optical ground wire - clear channel
c. The communication between Central SCADA Server and Eastern SCADA Server using 2 Mbps optical ground wire - clear channel (red line in figure 4)
d. In a normal operation SCADA system, 2 servers in Probolinggo DCC (Eastern) working separately with 2 servers in Surabaya DCC (Central). The database of both master stations can be synchronized either manually or automatically. Probolinggo DCC (Eastern) handles the entire substation, switching substation, Recloser, LBS and Fault Indicator that located in the eastern region. As for the Surabaya DCC (Central) handle the entire substation, switching substation, Recloser, LBS and Fault Indicator that located in the western region.
e. If SCADA system in Probolinggo DCC failed due to disturbances, natural disasters, fires or terrorist attacks, the operation of the Eastern SCADA can be handled from Surabaya SCADA (central), so the process of monitoring, control and data acquisition from the electrical substations in the Eastern Region still can be operating normally. The illustrations as shown in figure 5.

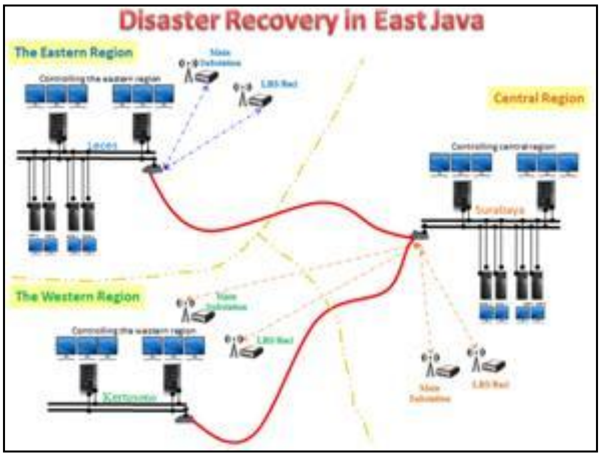


Figure 4 The Configuration of SCADA System Disaster Recovery

f. On the contrary, if the SCADA system in Surabaya (Central) failed due to disturbances, natural disasters, fires or terrorist attacks, the SCADA system Surabaya (Central) and Workstation Client Kertosono (Western) can be handled from SCADA Probolinggo (Eastern), as shown in Figure 6. Thus the process of monitoring, control and data acquisition from electrical substation for the Central Region and the Western Region still can be operating normally.

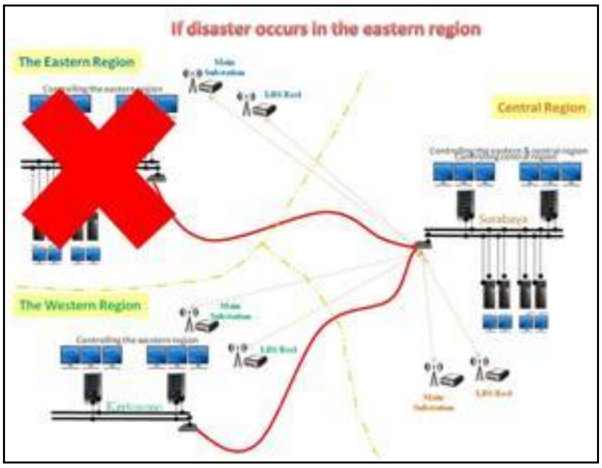


Figure 5 Configuration when SCADA Probolinggo (Eastern) failed

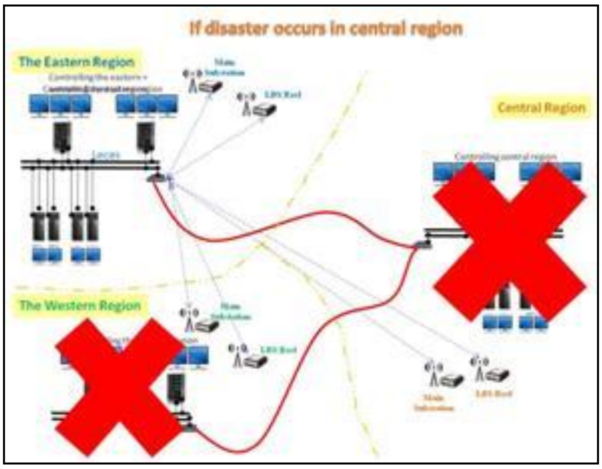


Figure 6 Configuration when SCADA Surabaya (Central) failed

Master Station Configuration

Below is the equipment configuration of the master station in Surabaya:

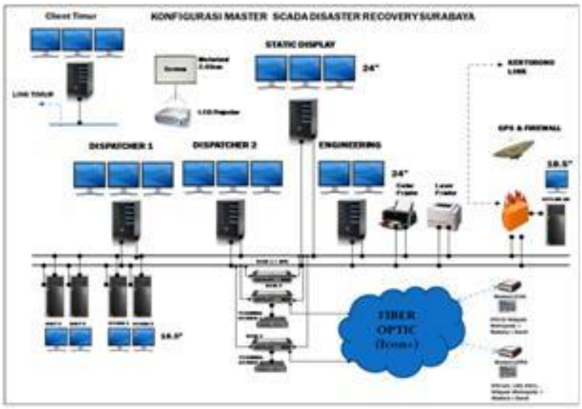


Figure 7 The Configuration of Surabaya Master Station (Centre)

The description of the Figure 7 above as follows:

1. SCADA Server (2)
2. Historical Server (2)
3. Offline Database Server (1)
4. Dispatcher Workstation (2)
5. Engineer Workstation (1)
6. Static Display
7. LCD Projector
8. Color Printer
9. Laser Printer
10. Ethernet Switch (2)
11. Terminal Server (2)
12. GPS & Firewall (1)
13. Eastern Workstation Client (1)

Below is the equipment configuration of the master station in Probolinggo DCC (Eastern):

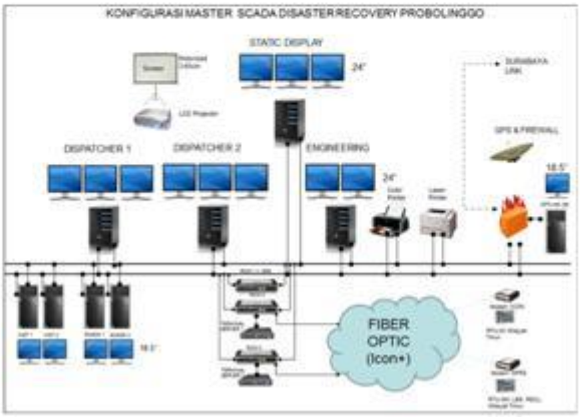


Figure 8 The Configuration of Probolinggo Master Station (Eastern)

The description of the Figure 8 above as follows :

1. SCADA Server (2)
2. Historical Server (2)
3. Offline Database Server (1)
4. Dispatcher Workstation (2)
5. Engineer Workstation (1)
6. Static Display
7. LCD Projector
8. Color Printer
9. Laser Printer
10. Ethernet Switch (2)
11. Terminal Server (2)
12. GPS & Firewall (1)

Below is the equipment configuration of the Kertosono Workstation Client:

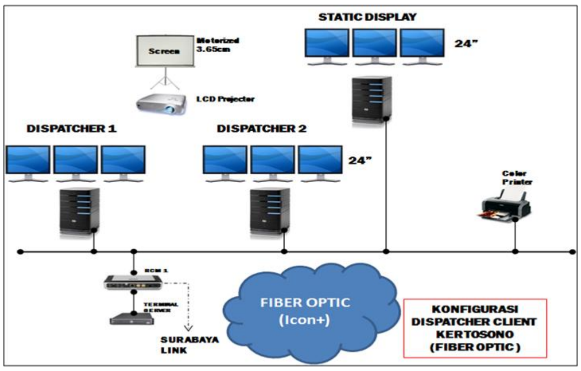


Figure 9 The Configuration of Kertosono Dispatcher Client (Western)

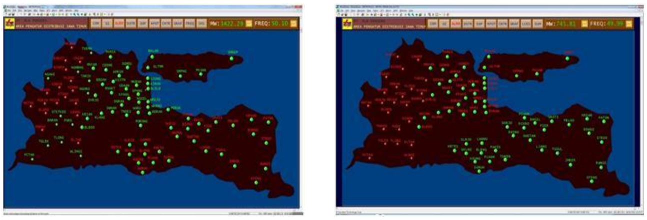
The description of the Figure 9 above as follows:

1. Dispatcher Workstation (2)
2. Static Display
3. LCD Projector
4. Color Printer
5. Ethernet Switch (1)
6. Terminal Server (1)

THE TESTING OF DISASTER RECOVERY SCADA SYSTEM

Disaster Recovery Plan SCADA systems have been applied in East Java DCC and inaugurated on February 10, 2012 by the Director of Operations of Java and Bali.

Under normal conditions, the operation of the SCADA system can be seen in Figure 11 and 12, which each Master Station works by zone area, namely Eastern DCC handles all substations and LBS at Eastern region and Central DCC handles all substations and LBS in the region of Central and Western.



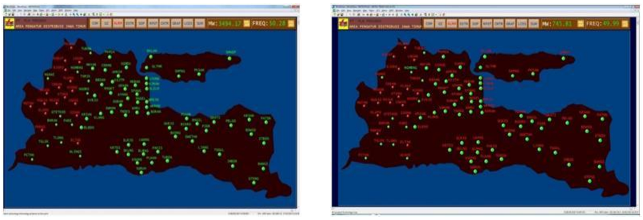
(a) (b)

Figure 10(a) Central DCC Normal Communication Line and (b) Eastern DCC Normal Communication Line

(a) (b)

Figure 11 (a) Central DCC DRP Normal Communication Monitoring and (b) Eastern DCC DRP Normal Communication Monitoring

After integration, the Disaster Recovery system has been tested by turning off all communication line substations which is in the eastern region from Central DCC. Gradually the substation communication line in the Eastern Region will be read non-active (Failed) from Eastern DCC. Then the central master stations take over the data communication from Eastern DCC to Central DCC. The captured image of active line communication in Central DCC and failed communication line in the Eastern DCC can be seen in the figures below.



(a) (b)

Figure 12(a) Active Communication Line – Central DCC view and (b) Failed Communication Line – Eastern DCC View

When the DRP SCADA system in Central DCC has been activated, then the SCADA Server in the East DCC will fail automatically. This mechanism is shown in Figure 13.

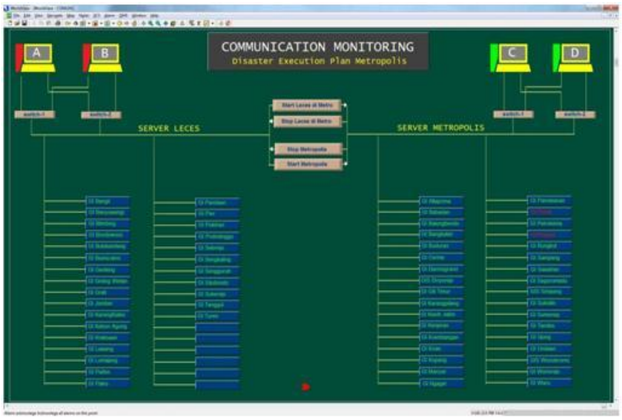


Figure 13 The Active DRP Communication Monitoring in Central DCC

The figures 12 to 13 show the result of the DRP SCADA system test in East Java DCC, with the success rate and accuracy of 100%. When testing the DRP SCADA System, the execution control of circuit breaker also done from Central DCC to one of feeder in Eastern Region (Probolinggo Substation). The execution has been carried out with the 3 seconds response time.

COMPARISON BETWEEN SCADA EAST JAVA DRP AND COMMON DRP SYSTEM

General Disaster Recovery System

As redundancy and disaster recovery mandate reshape network planning priorities, the role of back-up operations centers and supporting transmission architectures has become a key area of focus. Utility operators are looking for ways to strengthen multilayer protection at Layer 1, where leased lines and transport equipment form the critical underlying infrastructure for the transmission of data, voice, SCADA, surveillance video, and other traffic between points in a utility telecom network.

Poll-able SCADA systems using RTU data bridging technologies, while essential to utility operations, are also a source of concern in terms of potential reliability and security exposures. Moreover, the elements that comprise these systems are being discontinued by many equipment vendors, even though they are critical elements of the legacy utility telecom infrastructure.

For utility operators, an ideal disaster recovery solution must incorporate an efficient RTU data bridging function along with multi-layer protection mechanisms (hardware, link, path, site), to ensure the continuation of important legacy applications while improving the security and reliability of SCADA infrastructure.

Some of the most common strategies for the data protection are as follows:

[1]. Backups made to tape and sent off-site at regular intervals

[2]. Backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk

[3]. Replication of data to an off-site location, which overcomes the need to restore the data (only the systems then need to be restored or synchronized), often making use of storage area network (SAN) technology

[4]. The use of high availability systems which keep both the data and system replicated off-site, enabling continuous access to systems and data, even after a disaster.

In addition to preparing for the need to recover systems, organizations also implement precautionary measures with the objective of preventing a disaster in the first place. These may include:

(1) Local mirrors of systems and/or data and use of disk protection technology such as RAID

(2) Surge protectors — to minimize the effect of power surges on delicate electronic equipment

(3) Use of an uninterruptible power supply (UPS) and/or backup generator to keep systems going in the event of a power failure

(4) Fire prevention/mitigation systems such as alarms and fire extinguishers

(5) Anti-virus software and other security measures.

Implementation In SCADA East Java Disaster Recovery System

Based on some of the points above can be obtained the comparison between SCADA East Java Disaster Recovery system with other Disaster Recovery System,

(1) East Java SCADA DRP System did not have to implemented multi master RTU, because the SCADA DRP System works by routing of the data communication line.

(2) The back up data between the DRP Server is not automatically real time. It doesn’t need a large bandwidth communication data, so it cost is very effective. The back up data will be done manually by the engineer in the event of changes in the SCADA database. In this case, the SCADA system requires the commitment from the engineer to implement the data backup Standard Procedure.

(3) The server of SCADA DRP System located in separated place with monitoring function (Control Centre) in each server. Both server not only use as the back up server, but also as real time monitoring and control system. When the disaster occurs, the monitoring and control system still can be done from the normal control centre.

CONCLUSIONS

Extracting from the above discussion and exposure, it can be taken some conclusions as follows

a. To ensure the continuity of electrical power distribution operations system in East Java, The State Electrical Company (PLN) needs Disaster Recovery system in the SCADA system.

b. The reliable SCADA systems can not survive when natural disasters, fires, or threats of terrorist occurs. Therefore we need a recovery system to maintain the reliability of the integrated SCADA system called SCADA system Disaster Recovery.

c. SCADA system Disaster Recovery works if the SCADA system outages in a region due to an interruption or a natural disaster, then the SCADA system can be handled by the other SCADA system in the normal area.

d. the use of Disaster Recovery System can simultaneously make one of SCADA Master Station acts as IDCC, so IDCC can be used to monitor the whole area

The suggestions from above discussion are as follows:

a. The placement of two Master Station SCADA System which is mutually back up should be in two different places apart.
b. The two Master Station SCADA System which is mutually back up should be placed in two different places that separated by great distance.

REFERENCES

[1]. Disaster Recovery Planning Process. Geoffrey H. Wold. Disaster Recovery Journal. Adapted from Vol. 5 #1. Disaster Recovery World© 1997

[2]. PLN, 2010, SCADA Roadmap, 2010-2014, PLN, Surabaya, Indonesia A.B. Author, 1999, *Book Title,* Publisher, City, Country, 122-127.