A Business Continuity Plan:

- "A document containing the recovery timeline methodology, test validated documentation, procedures, and instructions developed specifically for use in restoring organization operations in the event of a declared disaster."

- To be effective, the Business Continuity Plans also requires testing, skilled personnel, access to vital records, and alternate recovery resources including facilities.

- Simply Put, **Business Continuity** is working out how to stay in business in the event of disaster.
Disaster Recovery (DR)

- **Disaster Recovery (with respect to SCADA and IT):**
  - DR planning is preparation for disaster and creating a plan for response to disaster
  - DR allows you to prepare for, respond to and recover from a disruptive event

- **BCP vs. DR:**
  - BCP is the process of being prepared and getting your Utility back to the normal delivery of service
  - DR replaces the loss of Information Technology (IT)
  - You need both (BCP & DR)
Is My Utility Vulnerable?

Recent Events have Increased our Awareness of the Criticality and Vulnerability of our Utilities

• 9/11
  • Security – both Physical and Cyber
  • Disaster Recovery and Business Continuity
  • ANSI/AWWA G430 Security Practices for O&M
• 2003 East and Mid-West Blackout
  • New regulations for backup power
• Weather Extremes
  • Government and utilities re-define 100 year events as existing 100 year events are becoming decade events
• What are our objectives?
  • Ensure the safety of staff and public.
  • Ensure the production and delivery of safe water.
  • Prevent the spill of wastewater into the environment.
  • Support Business Continuity efforts.
  • Protect critical equipment from damage.
  • Protect existing data from loss.
  • Continue to collect critical data.
  • Return the business to normal operations ASAP.
For 2009, there were 610 total responses:

- 461 responses from drinking water utilities
- 149 responses from wastewater utilities.
**Resiliency**

- 86% have backup power capabilities for at least 24 hours and about half of water and wastewater utilities can provide backup power for 96 hours (4 days) or more (measure 19).
- Two-thirds of responding water utilities can provide 91–100% of minimum daily demand for water for up to 24 hours (measure 20).
- One-third of water utilities can provide 91–100% percent of minimum daily demand for 72 hours (measure 20).
Responsiveness

- 97% of water and 93% of responding wastewater utilities have an emergency response plan (ERP) (measure 15).
- 90% of water and 89% of responding wastewater utilities have reviewed and updated their (ERP) (measure 15c)
Preparedness

• Responses point to two areas for future improvement.

  • 50% of the respondents said they do not have a business continuity plan (measure 14).

  • 42% of responding water and 45% of responding wastewater utilities do not have crisis communication plans (measure 21).
What happens when SCADA & Information Management is Lost

Business Integration and Optimization

Operations Control

Level of Capability

Level 0
Local Hardwired Control

Level 1
Local Digital Control

Level 2
Remote Manual Control

Level 3
Remote Auto Control

Level 4
Enhanced Operations

Level 5
Optimized Operations

- Indicating Instruments
- Relays & Circular Charts
- PLC/DCS/RTU
- Local Data Loggers and OITs
- Control Modes (Local-only)
- Digital Controller (PLC/DCS/RTU)
- Network with Central HMI/SCADA Servers
- Control Modes (Remote-Manual, Local)
- Full automation
- Process Interlocks Exchanged over Network
- Automated Closed-loop control around a setpoint
- Control Modes (Remote-Auto, Remote-Manual, Local)
- System-wide Proactive Control
- Tools for Operations Optimization Analysis
- Business Systems Integration (SCADA, LIMS, CMMS, FIS, Hydraulica Model)
- Control Modes (Remote-Optimize, Remote-Auto, Remote-Manual, Local)
- Operational Flexibility
- Historical SCADA Data Management
- Decision Support System Provides Operator Advice
- Control Modes (Remote-Auto, Remote-Manual, Local)
Information Technology Management System
Automation & SCADA System

[Diagram of a SCADA and PLC network system, including components such as historians, servers, wireless communications, PLCs, RTUs, and secure remote monitoring.]
Most water agencies would be hard-pressed to maintain service levels if their SCADA system suffered a catastrophic (or even partial) failure.

- Operating Knowledge Retained in Control Strategies
- Improved Operating Efficiency
- Regulatory Compliance
- Operating Data for Planning
- Protection of People, Environment and Equipment

SCADA is Mission Critical!
SCADA System BCP & DR, Why SCADA?

- SCADA is Critical Infrastructure
- “IT HAPPENS” - Forrest Gump, 1976

- Failure Mode and Effect Analysis
  - Prevent “IT”
  - Mitigate “IT”
  - Recover from “IT”
SCADA System BCP & DR, Examples of “IT”

• SCADA System UPS Circuit Failure
  • Cleaner plugged industrial floor polisher into UPS
• Failure of High-Availability SCADA Server
  • Both power supplies plugged into same UPS circuit. Circuit failed and server did not recover.
• Multiple PLC Processor (e.g. AB 5/40E) failures
  • Not enough spares
• Network Core Switch/Router Failure
  • Both power supplies failed, no spares
• Disinfection Redundancy
  • On everything but the PLC
• Where is the latest version of the program?
SCADA BCP/DR, a Sound Process

Goals of a SCADA BCP/DR Plan:

• To enhance operational continuity by enhancing SCADA System availability (uptime)
• Understand the business risk associated with failure
• Prevention of SCADA System Failures
• Mitigation of SCADA System Failures
• Recovery from SCADA System Failures
"Ask Yourself"

• Have you ever tested all applications and are your personnel willing to guarantee that all applications can be restored correctly?

• Are your personnel ready to wait 24 or 48 hours for their systems to return and do they know what to do while they’re waiting?

• Are all of your backup files synchronized between all applications, all platforms and all locations?

• Can you really restore all backup data in the time allowed by your recovery time objective?

• Does your planned recovery time include the time it will take for management to really "pull the trigger" and declare a disaster?
SCADA BCP & DR
Creating a Plan

• Governance
  • Business Impact Analysis (BIA)
  • Plans, Measures, and Arrangements
  • Readiness procedures
  • Quality assurance techniques
Establish Control, Governance

- Senior Managers / Steering Committee
  - Approve the governance structure
  - Clarify their roles and those of participants
  - Provide Strategic Direction
  - Approve results if Business Impact Analysis
  - Review the critical services and products that have been identified
  - Approve continuity and disaster recovery plans
  - Resolve conflicting interests and priorities
Establish Control, Governance

- **Recommended Steering Committee Members**
  - Executive sponsor – overall responsibility
  - Coordinator – “Project Manager”
  - SCADA Manager
  - Senior Operations
  - Engineering
  - Stakeholders

**Tactics:**
- Communication to stakeholders, internal and external
- Interviews, surveys and workshops
- Project Steering Committee cross-functional teams
- Investment of ideas & time
- Stakeholders support and defend plans and designs
SCADA BCP & DR
Creating a Plan

- Governance
- **Business Impact Analysis (BIA)**
- Plans, Measures, and Arrangements
- Readiness procedures
- Quality assurance techniques
Business Impact Analysis (BIA)

• A Business Impact Analysis (BIA) quantifies the impact of a system failure on the business including organization, production and equipment

• BIA Metrics:
  • Recovery Point Objective (RPO)
    • Amount of time a system component can be down before the business suffers
  • Recovery Time Objective (RTO)
    • How much time the IT department has to repair the failure before initiating the Disaster Recovery Plan.
  • System Availability Objective (SAO)
    • The uptime objective based on the criticality rating e.g. 99.999% or 99.995%
Business Impact Analysis (BIA)  
**FMEA Methodology**

- Structured Analysis for System Failure.
- Potential System Failure Modes and Events
- Effect, Severity, Frequency of Failures and Events
- Cause of Failures and Detection

<table>
<thead>
<tr>
<th>Function</th>
<th>Failure Mode</th>
<th>Effect of Failure</th>
<th>Potential Cause of Failure</th>
<th>Severity Rating</th>
<th>Occurrence Rating</th>
<th>Detection Rating</th>
<th>Preventative Actions to be Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
STEP 1  Define the FMEA Team – include all stakeholders: SCADA, Operations, Maintenance, Engineering.

STEP 2  Develop a Skeletonized Block Diagram of the SCADA System.

STEP 3  Describe the System Components and intended functions.

STEP 4  Brainstorm possible failure modes and their cause(s).

STEP 5  Describe the effect(s) of each failure mode and current mitigation strategies.

STEP 6  Analyze the Risk or Criticality of each failure and prioritize
Business Impact Analysis (BIA)

Brainstorm Potential Failures

• Possible Failures
  • Loss of Communication
  • Power Loss
  • Natural Disaster (Flood, Fire, etc.) Destroys system component (PLC, Communications, HMI, Historian)
  • Hard Drive Failures
  • Virus Destroys all Data
  • Vandalism or Theft
  • Over-heating
Business Impact Analysis (BIA)

FMEA Risk Priority Number

- Quantify the risk associated with failures

Risk Priority Number (RPN)

\[ RPN = \text{Severity} \times \text{Occurrence} \times \text{Detection} \]

- **Severity** – the severity of the failure effect on the system or process or business
- **Occurrence** – probability or frequency of failure
- **Detection** – the probability that the failure can be detected before the effect of the failure occurs.
Business Impact Analysis (BIA)

FMEA Severity Rating

Leveraging the ISA-TR91.00.02-2003 Criticality Classification Guideline as a Basis

| Legal (0 – 35)                     | • Failure to comply with regulations  
                                      | • Potential for fines or prosecution |
|-----------------------------------|---------------------------------------|
| Health & Safety (0 – 35)          | • Potential for harm to public or employees  
                                      | • Degree of harm                       |
| Performance (0 – 20)              | • Degradation in Service Levels.       
                                      | • Duration of event                     |
| Financial (0 – 10)                | • Staff over-time, external contractors  
                                      | • Repair or replacement of equipment    
                                      | • Loss of Revenue                       |

RPN = Severity x Occurrence x Detection
Business Impact Analysis (BIA)
FMEA Occurrence & Detection

- Occurrence
  - Probability of Failure
- Subjective
  - Anecdotal
- Objective
  - Quantifiable based on:
    - MTBF
    - Failures per Operating Hours (or Service Life)
    - Maintenance Records
    - Failure Database

- Reliability of detection method
  - Slow or non-existent detection receives highest score
- Typical delay between failure and detection
- Typical delay between notification or action

RPN = Severity x Occurrence x Detection
SCADA BCP & DR
Creating a Plan

• Governance
• Business Impact Analysis (BIA)
  • How Much Time to Respond
  • Risk Priority
• Plans, Measures, and Arrangements
• Readiness procedures
• Quality assurance techniques
SCADA BCP & DR
Plans, Measures, & Arrangement

- Mitigation Strategies
  - Spare Parts
    - How many and where
  - Back-up to Storage Server
  - Back-up to Portable Device (Tape or Hard drive)
  - System Redundancy
  - Response Procedures
  - Employee Training
  - 3rd Party Support
SCADA BCP & DR Plans, Measures, & Arrangement

• Analyze current recovery capabilities
  • Leverage existing Emergency Response Plans

• Prepare SCADA BC & DR Plans
  • Identify Command & Control Teams
  • Identify Communication “Tree”
  • Identify Communication and Timelines for escalation
SCADA BCP & DR
Creating a Plan

- Governance
- Business Impact Analysis (BIA)
- Plans, Measures, and Arrangements
- Readiness procedures
- Quality assurance techniques
SCADA BCP & DR Readiness Procedures

• Accessibility to SCADA BCP & DR Plans
• Accessibility to Communication Plan
• Standard Operating Procedures
  • Restoring Software
  • Restoring SCADA or Communication Programs
  • Operations
• Training on SCADA BCP & DR Plans
• Exercises / Drills
SCADA BCP & DR
Creating a Plan

• Governance
• Business Impact Analysis (BIA)
• Plans, Measures, and Arrangements
• Readiness procedures
• Quality assurance techniques
SCADA BCP & DR
Quality Assurance Techniques

- Internal Review
- External Audit
- Scheduled Reviews of Plan for Relevance
- Incorporate Lessons Learned from Incidents
SCADA BC & DR Planning
Is Your System Ready?

- Governance
- Business Impact Analysis (BIA)
- Plans, Measures, and Arrangements
- Readiness procedures
- Quality assurance techniques

All Utilities have a “Scotty” ........

But they are not always around...
Thank You for Your Time

Questions?
Resources

- 2009 Water Sector Measures Analysis

- AWWA: Voluntary Private Sector Accreditation

- Public Safety CA
  [http://www.publicsafety.gc.ca/prg/em/gds/bcp-eng.aspx#a02](http://www.publicsafety.gc.ca/prg/em/gds/bcp-eng.aspx#a02)
SCADA Business Continuity and Disaster Recovery

Presented By:
William Biehl, P.E.
913-601-0104 (mobile)
Bill.Biehl@we-inc.com