SCADA System Traceability

Prepared by Trihedral for KROHNE Academy 2013

Barry Baker, P.Eng.

Agenda

1. Welcome
2. Introduction
3. What is the problem?
4. How bad could it be?
5. Malicious vs. Accidental configuration problems
6. Typical change cycle
7. Factors contributing to poor asset tracking
8. Industry solutions
9. Classical Models : Pros & Cons
10. Applying to SCADA Systems
11. Possible benefits
12. Case Study with live demo of distributed version control method
13. Summary review
14. Q & A
15. Post-test.

WELCOME !

Some housekeeping items before we get too far (and forget !)

Upon satisfactory completion of this course, you will receive CEU and/or CPE credits. Phoenix Contact is an authorized provider of CEUs licensed through the International Association for Continuing Education and Training (IACET).

Satisfactory completion requirements are as follows:

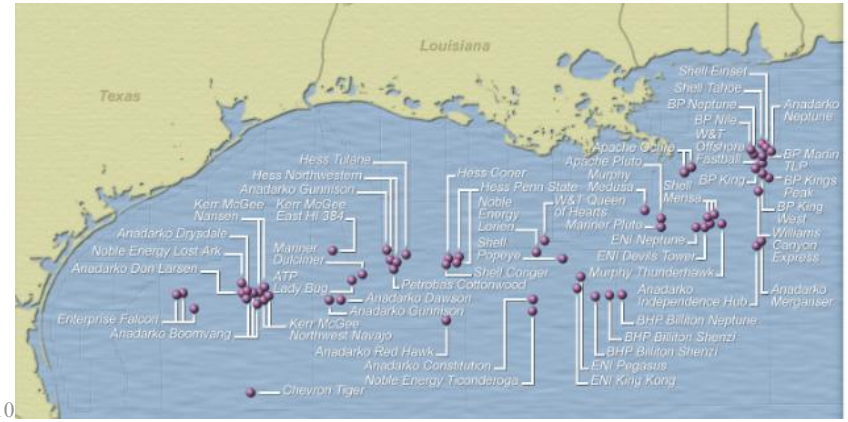
- Beginning of session – sign in sheet and pre-test
- End of session – post test and class evaluation

After completion of the course, the instructor will submit the class information to the corporate office training department.

CEU certificates will be mailed to each participant that fulfills the course requirements (meaning we need your mailing address!)

Introduction

- Trihedral was founded in 1986 as an HMI (Human Machine Interface) software provider.
- Our software, VTS™ and VTScada™, is installed in thousands of applications worldwide, via direct and indirect sales. The Oil & gas sector is largely served via OEM's who re-label the software as their own to serve a variety of specific applications.
- Trihedral has an active engineering group that supports end-customers and OEM's when they request custom SCADA developments. These endeavours can range from short "one-off's" to product or application "evolutions" over many years in various sizes. This ultimately requires systematic methods to ensure that what you *think* you are modifying is in fact that, *so that you get the results you planned !*
- Over 26 years we have used various tools to assist us in this task, ranging from free software in the public domain to off-the-shelf products from Microsoft and others. We would like to share with you some lessons learned on why this is an important consideration and some options available.



The problem: Incomplete Record Keeping and The Potential for Loss

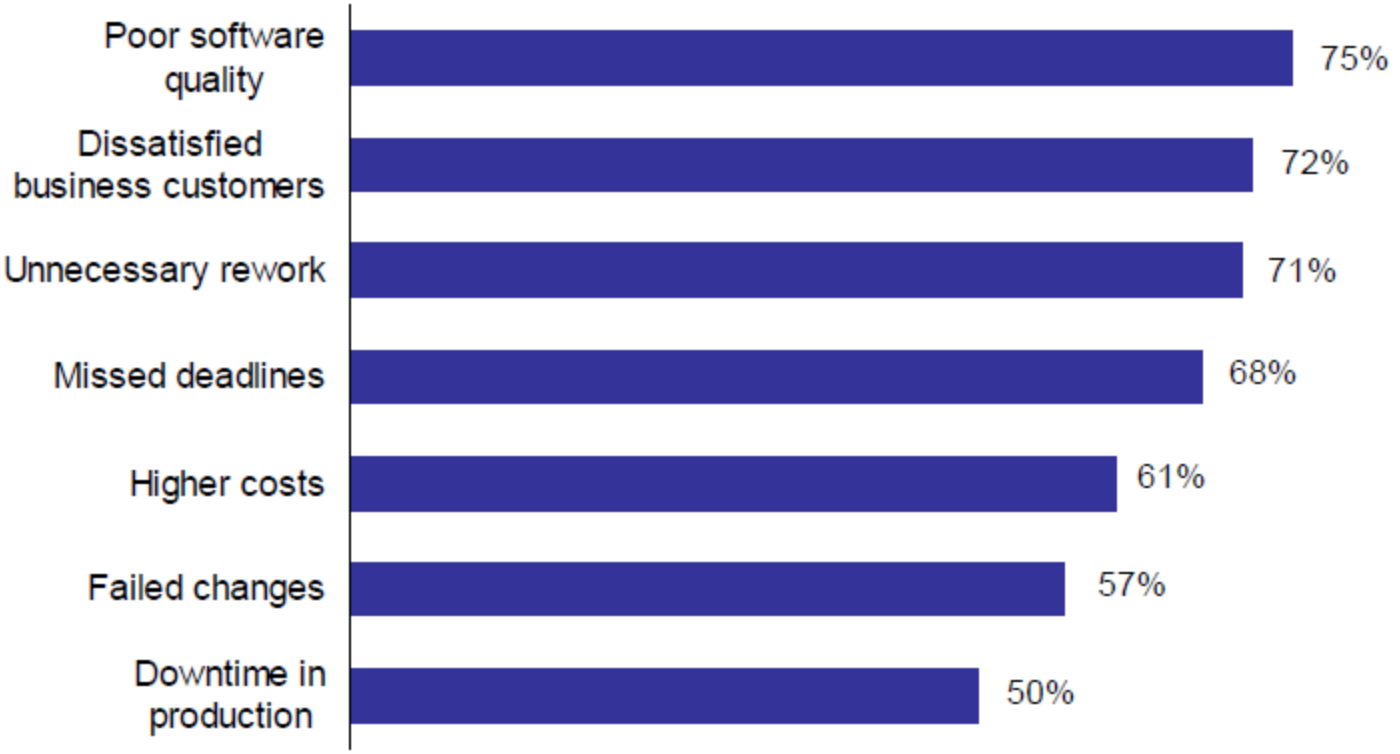
The importance of good record keeping : Manual vs. automatic

The absence of auditable tracking in SCADA

Potential losses to product, process and people

Lack of regulation and guidance compared with other industries

Survey of 102 NA companies: Lack of Software Change Management Processes causes problems in Critical Areas



Base: 28 North American $500M+ companies, of 102 surveyed, that do not have defined change management processes for all software (multiple responses accepted)

Source: A commissioned study conducted by Forrester Consulting on behalf of Serena Software, November 2006 http://www.serena.com/dcs/repository/solutions/software-change-mana.pdf,

How bad could it be? Why worry, be happy ?

The story of Phobus-Grunt & Yinghuo-1

Background:

Attempted Russian sample mission to the Mars moon Phobos , carrying the Chinese orbiter Yinghuo-1 and other experiments.

About 30,000 lbs with total estimated mission cost of 5 billion rubles ($163 M US).

First Russian-led interplanetary mission in 15 years.

Launched on 9 Nov 2011 into low earth orbit, but subsequent rocket burns failed and the left it stranded, with decaying orbit.

Initial worry on toxic spill from 7.51 metric tonnes of hydrazine and nitrogen tetroxide

NASA estimated could be most dangerous object ever to fall from orbit.

.

Source: http://en.wikipedia.org/wiki/Fobos-Grunt

How bad could it be? Could the Sky fall ?

Phobus-Grant burned up on Earth atmosphere re-entry on 15 Jan 2012.

Location uncertain (Pacific Ocean, Brazil, Argentina??), components missing.

Possible early reasons given for failure from Russian officials :

- Sabotage by a foreign nation
- Risky decisions made in development due to lack of funding.
- US Radar stationed on the Marshall Islands inadvertently disabled the probe (but no evidence given)
- Microchips may have been counterfeit
- A burst of cosmic radiation caused computers to go into standby mode

Phobus Grant : What really happened

On 6th February 2012 the commission investigating concluded that Phobos-Grunt mission failed because of "*a programming error which led to a simultaneous reboot of two working channels of an onboard computer*."

Experts suggest it was the culmination of :

- poor quality control,
- lack of testing,
- corruption.

Russian president Dmitry Medvedev suggested that those responsible should be punished and perhaps criminally prosecuted...

Likely a few engineers & programmers were re-assigned to unpleasant places ....

SCADA Configuration Problems: Malicious vs. Accidental

Malicious Acts

- Intended to harm process, product or people (PPP)
- May intend to gather data for 3rd party use
- Contravene standard change procedures
- No record keeping
- Reported to authorities

Accidental Affects

- Unintentional. No intent to harm
- Completed by authorized users
- May or may not follow standard change procedures
- Good quality records may or may not be maintained
- Events may go unreported

Malicious Actions

Lack of record keeping makes identification difficult

"industrial production and human safety [are] at risk from cyber attacks" on SCADA systems - GAIT

Between 25 and 100 incidents per year in 2004. 70% perpetrated by outsiders. Statistics suggested year-over-year increase in frequency

Today. Millions of attacks per day. Many incidents are unknown.

> “Stuxnet has become the blueprint for today’s cyber weapons”
>
> - Veracode, Aug 08, 2012

Accidental Affects

Lack of reporting makes quantification difficult

Incidents reduced through

- Policy and procedure
- In-depth testing before introduction to production environment

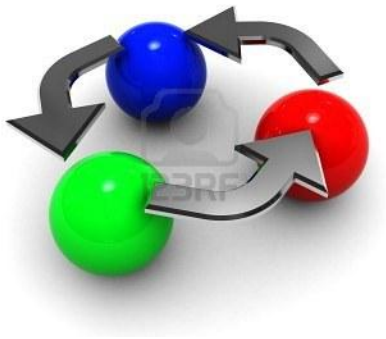
Difficult to test all consequence of change

Affects on PPP can vary widely

> “We couldn’t hold up the process for some silly procedure” - Jim, 2012
>
> “Bob asked me to add that” – Steve, 2010
>
> “I was bored and decided to teach myself how to program this thing” – Yuri, former employee, reported missing

Change Cycle in SCADA Systems

1. Initial system rollout
2. Many minor changes occur over time
   - More equipment monitored
   - Equipment and technology changes
   - Functionality improvements
   - Reporting/regulatory demands
3. Major system upgrade due to business needs or because of changes in associated systems (i.e. Hardware obsoleses, OS Version Changes)
4. *Go back to step 2 and repeat (iterations over avg. 10+ year lifespan of system)*



Factors Contributing to Poor Tracking

SCADA systems grow incrementally, requiring many small, minor changes

Various contractors/employees apply configuration changes

Change is often deployed quickly to minimize process interruption

Recording each minor change is time consuming

Options for Improvement - Security, Backup, Version Control

Security - Limit change privileges to authorized users using clearly defined policy and procedure

Backup - Ensure a known good state for the asset is available in the event of unexpected system upset

Version Control - Comprehensive traceability for problem identification and source determination

Each is a time-tested method for improving reliability or minimizing loss

Typical Security Issues

Highest security requires physical separation – often not feasible. Eliminate unauthorized access instead.

SCADA systems integrating disparate components do not share security management

- Multiple accounts
- Multiple security paradigms
- Multiple security logs

Authenticated users still make mistakes

Typical Emergency Backup Issues

May require SCADA asset to be taken offline during backup/restore

Processes run periodically rather than on-event

Methodologies

- Manual processes require strict procedure and enforcement
- Periodic automatic occurrence may not capture recent changes

Replication to more than one physical location

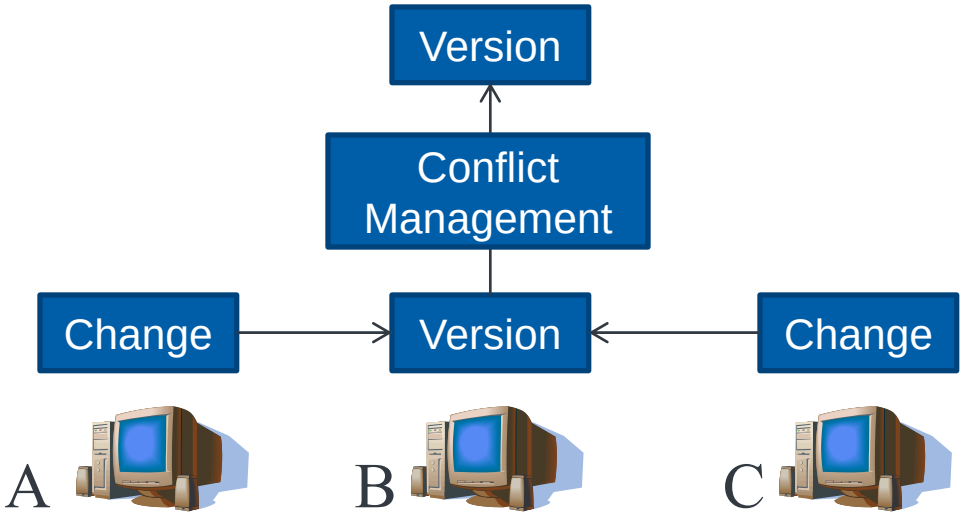
Typical Version Control Issues

Single change can affect many files. Not easy to determine which ones

Recording entire SCADA configuration for each version requires large storage capacity

Often a manual process - strict procedure and enforcement required

Repository replication to more than one physical location



How has Industry solved this problem ?

Version control industry definitions: (*Similar to but not like the other acronyms using "S&M")*

- **SCM**: Software Configuration Management or
- **SCCM**: Software Configuration and Change Management

• Goals of SCM

- **Configuration identification** - Identifying configurations, configuration items and baselines.
- **Configuration control** - Implementing a controlled change process.
- **Configuration status accounting** - Recording and reporting all the necessary information on the status of the development process.
- **Configuration auditing** - Ensuring that configurations contain all their intended parts and are sound with respect to their specifying documents, including requirements, architectural specifications and user manuals.
- **Build Management** - Managing the process and tools used for builds.
- **Process management** - Ensuring adherence to the organization's development process.
- **Environment management** - Managing the software and hardware that host the system.
- **Teamwork** - Facilitate team interactions related to the process.
- **Defect tracking** - Making sure every defect has traceability back to the source.

- - Source: Wikipedia

Classical Models of solutions

Solutions can have two varying methods:

- Centralized to monitor & control all changes.
  - No changes possible without connection to central DB (i.e. “check-in” or “check-out” privileges or “locks”)
  - Locks do what they imply - Exclusivity of changes from any other user.
  - Limit developments to one active “branch” or version.
  - Central DB is usually a single entity: *Things can grind to a halt when it is unavailable or cannot be connected to (i.e. no off-line or isolated activity).*

- Distributed or “standalone”
  - Localized repository to each development instance.
  - Each has a copy of all other developments, plus its own.
  - Instead of “locks”, works on a “merge” process.
  - Has benefit of multiple branches, multiple layers of redundancy, and permits off-line development .

How do they apply to SCADA systems ?

Solutions generally come in two “flavours” :

- External to SCADA System
- Integrated to SCADA System

External to SCADA

- Generally “bolt-on’s” or “third-party solutions”.
- Some examples (many specialized available):
  - Apache Subversion (“SVN”). Distributed under Open-Source License (free to use but not *within* products that are not free !). Distributed technology.
  - Microsoft Visual SourceSafe (VSS): Centralized Technology, rolled into Team Foundation Server
- Pros:
  - Can be readily acquired independent of SCADA system
  - Used with multiple aspects of the system.
- Cons:
  - Operate independent of SCADA system.
  - Cannot provide **on-line** roll-back , promotion or investigation within SCADA system.
  - Rely on people remembering to track changes - No automatic tracking.

Integrated with SCADA

Can provide (depends upon vendor) :

- Automatic change tracking on system development or maintainance operations: no user actions
- Provide for live, real-time investigation of problems (& Resolutions!)
- Multiple layers of redundancy

In Summary

•Reduced development and deployment time

•Decreased administration and procedural enforcement

•Reduced likelihood of human error

•Faster recovery time

Benefits of Tight Component Integration

Backup and version control components integrated into the SCADA development and management environment.

Shared security management and event recording

Automated configuration backup with linked user credentials

Automated change recording with traceability – linked user credentials

What to Look for in a Version Controlled SCADA Environment

1. Automatic recording of configuration changes with a traceable version history
2. Tamperproof, distributed repository
3. Incremental change storage
4. Support for multiple developers (merging)
5. Separation of change creation and deployment privileges
6. Online configuration change testing & deployment
7. Rollback and change reversal
8. Simultaneous deployment across SCADA network
9. Supports Off-line and *authorized* third-party change introduction
10. Provides view of who is out of sync
11. Provides for editting server lists
12. Provides export & import of configuration data, with tracking & auditing

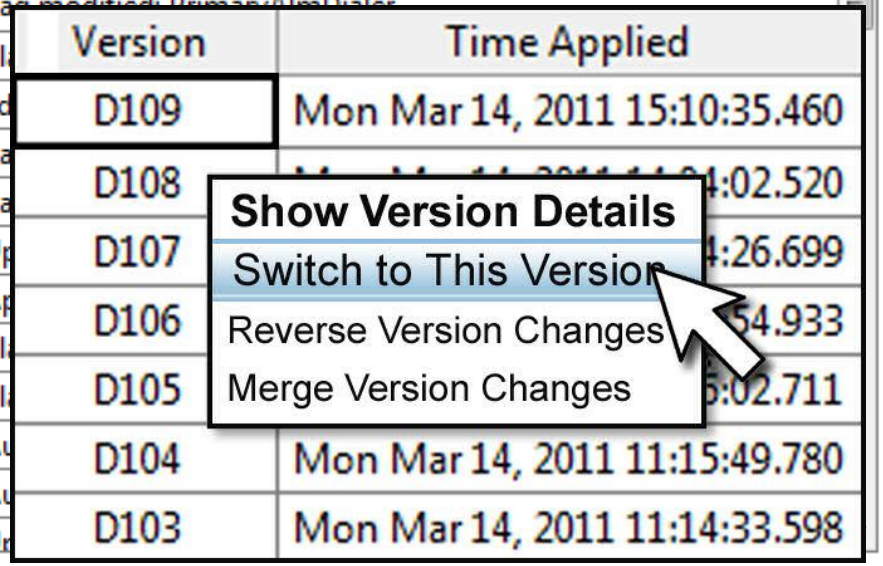
Real-time Change Recording

Workstations

Workstation	Last Update	Current Version
BLAIR-LAPTOP2	Wed Apr 04, 2012, 14:47:15.867	BLAIR-LAPTOP2-D272
CHRISTOPHERL	Fri Jun 08, 2012, 12:04:38.119	CHRISTOPHERL-D112
VTSDEMO	Wed Jan 18, 2012, 08:47:27.156	VTSDEMO-D6

Version Log for CHRISTOPHERL (Total of 128 records in log)

Version	Time Applied	User	Comment
CHRISTOPHERL-D112	Fri Jun 08, 2012 12:04:38.119	admin	Tag modified: PrimaryAlmDialer
CHRISTOPHERL-D111	Mon Jun 04, 2012 16:31:18.692	Logged Off	Pl
CHRISTOPHERL-D110	Tue Apr 17, 2012 15:07:27.187	admin	Ed
BLAIR-LAPTOP2-D272	Wed Apr 04, 2012 14:47:16.173	admin	Ta
BLAIR-LAPTOP2-D271	Wed Apr 04, 2012 14:47:07.802	admin	Ta
CHRISTOPHERL-D109	Mon Apr 02, 2012 14:25:39.754	admin	Up
BLAIR-LAPTOP2-D270	Fri Mar 30, 2012 13:07:42.773		Ap
CHRISTOPHERL-D108	Thu Mar 29, 2012 11:29:31.256	Logged Off	Pl
CHRISTOPHERL-D107	Fri Mar 23, 2012 12:44:56.706	Logged Off	Pl
CHRISTOPHERL-D106	Wed Mar 21, 2012 16:25:13.648	admin	Au
CHRISTOPHERL-D105	Wed Mar 21, 2012 15:21:06.844	admin	Au
BLAIR-LAPTOP2-D252	Wed Mar 21, 2012 15:19:56.343	admin	Un



Case Study Solution: A Fully Integrated Solution

Multiple developers integrate independent and inter-dependant changes

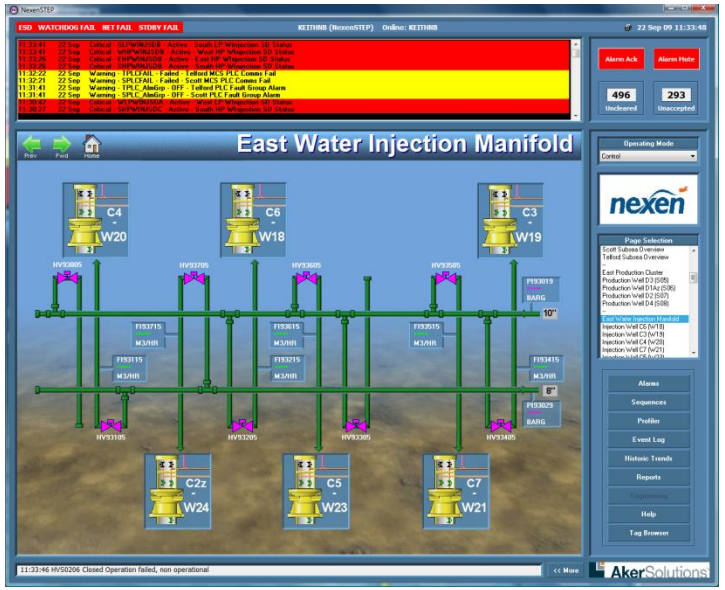
Remote access to system is via two-stage access

- Authenticated VPN access to server environment
- Authenticated SCADA developer access

Changes are merged into the live system without requiring restart of servers or clients

Current (pre-change) state and Updated (post-change) states are automatically recorded

Incremental change details are available for future analysis.



Summary

SCADA systems are critical, trusted assets

Incorrect SCADA configuration can incur substantial loss

Change is expected but difficult to record

Version control, security and backup mitigate loss

Version control can be:

- external or internal,
- free or paid,
- Follow a central or distributed model.

Tight component integration of security, backup and version control combine all elements under one “foot-print” with linked traceability of user actions.

The end result: Improved cost control and reliability, reduced administrative burden

Q&A

Your turn to speak !

Post-test

Did we teach you anything (useful) ??