A RESILIENCE CHECK LIST FOR WATER UTILITIES

ORWARN 2018 - Paul R. Nelson, P.E., EWEB Controls System Administrator

Increasing the *RESILIENCE* of a control system may be accomplished by any change that

- increases the **Robustness** of the system
- provides **Redundancy of elements**
- increases available **Resourcing** options
- increases **Rapid response** to changes or challenges
- Ideally, all four of these properties are addressed, and may be improved in any or all of the four constituent dimensions: *Technical, organizational, social, and economic*.

CHECKLIST

RESILIENCY CONCEPTS

- ☐ Definition: Are you familiar with the definition of resilience and how it may be applied to your utility or control system?
- ☐ Have your reviewed the 4 x 4 Resilience models as espoused by the MCEER and considered how this may be applied to your system?
- ☐ Have you reviewed the relevant ORP (Oregon [Washington] Resilience Plan) for your state and considered how it applies to your control system?
- ☐ Have you reviewed your local community hazard mitigation plan and considered how your control system improvement plan aligns?

ROBUSTNESS

Logic Software lifecycle

- ☐ Do you have documented control narrative or specification for every control station?
- ☐ Is your control logic developed following the specification?
- ☐ Is the logic tested with a written commissioning plan prior to production use?
- ☐ Do you have a MOC (Management of Change) methodology defined for the software?

HMI lifecycle

- ☐ Do you have a documented template for HMI development?
- ☐ Is your template based on the latest human factors studies e.g. High Performance HMI and/or ASM (Consortium for Abnormal Situation Management)
- ☐ Do you use trending to improve the ability of operators to understand and correct your operational processes?
- ☐ Have you provided operators training on your HMI implementation?

Alarming lifecycle

- ☐ Do you use a standard method for alarm prioritization?
- ☐ Is it based on the Alarm Management Handbook or similar International Standard?
- ☐ Have you followed an alarm rationalization procedure?
- ☐ Are your alarms defined in a master database?
- ☐ Do you follow a standard method once the alarm is deployed to manage drift away from the original design intent?

Continuous improvement

- ☐ Do you have an established way of using day to day failures to improve your system?
- ☐ Do you have an established measurement system for control system performance based on alarm count, failure count, disabled hardware or software objects, etc. for tracking of system health?

Communications

- ☐ Have you identified which of your communication technologies is most susceptible to failure?
- ☐ Do you have a plan in place to upgrade communication paths for instance replace communication lines subject to physical impact from excavation or collision?

REDUNDANCY

Servers

- ☐ Have you measured effective uptime of your system servers?
- ☐ Have you reviewed your need to address uptime via redundancy? If so do you have a plan in place to bring this to fruition?

Clients

- ☐ Do you have diversity of client deployment such that single or duplex failures do not inhibit ability to operate?

Communications

- ☐ Have you reviewed your communications to determine if redundant, diverse (non-common mode failure) paths are called for?

Remote annunciation

- ☐ Have you established diverse and/or redundant alarm delivery methods so that delivery of alarms is highly likely?

RESOURCEFULNESS

Client deployment

- ☐ Have you provided your Operators with a client interface that has connectivity to your system anywhere in your service area?

RAPID RESPONSE

Client deployment

- ☐ Are your operators able to respond to afterhours issues without having to travel to the office or station?
- ☐ Do you have a process information historian in place with a functional interface so that utility personal may study and report on system behavior include cause and effect relationships?

MULTI-DIMENSIONAL

Team development

- ☐ Do you have adequate breadth and depth of skills in your team to address control system issues?
- ☐ If not do you have a plan to address providing these skills through a combination of on the job training with formal industrial controls training?
- ☐ Do you recognize employees ($) for achieving relevant certifications?
- ☐ Do you have a good relationship with a qualified contractor or systems integrator that can provide support when the demands are too large for the in-house team?

References for further reading:

The MCEER (Multidisciplinary Center for Earthquake Engineering Research) which provides an applicable model for resilience applied to SCADA systems:
http://mceer.buffalo.edu

What went wrong in Flint:
https://fivethirtyeight.com/features/what-went-wrong-in-flint-water-crisis-michigan/

Oregon Resilience Plan:
https://www.oregon.gov/oem/Documents/Oregon_Resilience_Plan_Final.pdf

Eugene – Springfield joint natural hazard mitigation plan:
https://www.eugene-or.gov/683/Hazards

Software development lifecycle model:
https://www.testingexcellence.com/software-development-life-cycle-sdlc-phases/

ISA Certified Automation Professional:
http://www.controlsystemworld.com/blogs/how-to-pass-the-isa-cap-certification-exam

ISA Certified Control System Technician:
isa.org/isa-certification/certified-control-systems-technician/

High performance HMI:
Bill Hollifield, ISBN-13: 978-0977896912

Alarm Management Handbook:
Bill Hollifield and Eddie Habibi, ISBN-13: 978-0977896929

Abnormal Situation Management Consortium:
http://www.asmconsortium.net/