Troubleshooting, Risk Management & Cybersecurity

Jacob Kemper
Technical Product Owner, HTT

SCADA ACADEMY

Outline

Troubleshooting

- General methods, tips and tricks
- Real examples

Risk Management

- Physical Security
- Disaster Preparedness

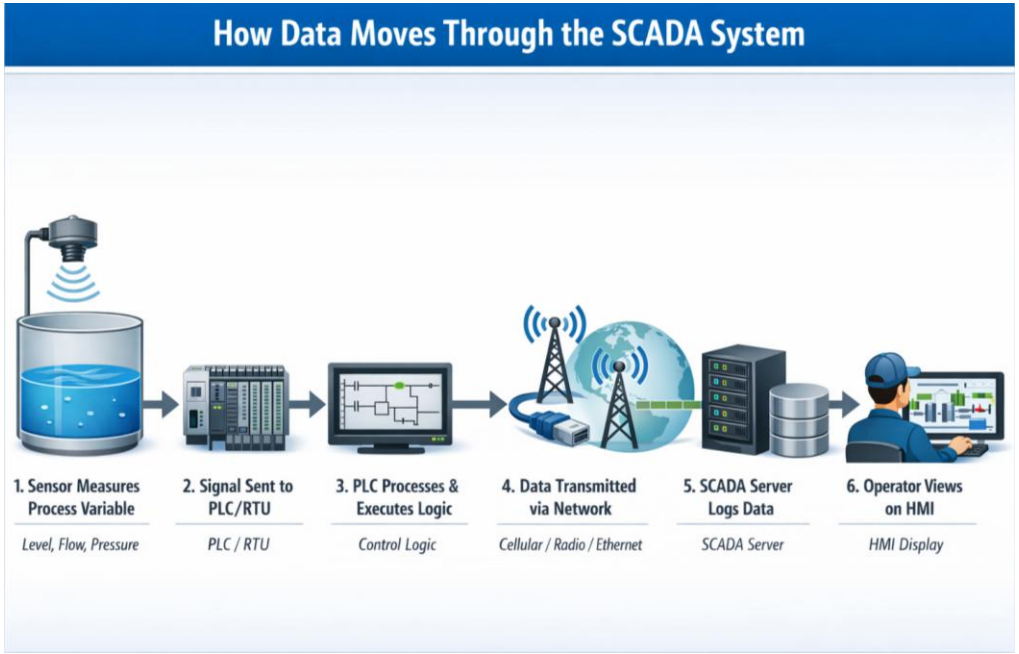
Cybersecurity

- Hardening weak points

Troubleshooting

Know How It Works

- Understand the flow of data
- Know how to look at our data as it moves along
- Know how to check on system health
- Know how to turn it off and on again
- Manuals are a great resource



Gather Information

Zoom out:

- Are there any other problems?
- What is the context?

Zoom in:

- When did this start?
- What do the logs say?

Locate the Problem- Divide and Conquer

- When we gathered information, we found a broken point
- Check another point in the data path
  - Health check: is it on and working?
  - Look at our data: is the piece that was broken also broken here?
  - Test: Can we send something across or through it?
- The results of these questions will point us in the right direction
- Repeat until you've found the source of the problem

Locate the Problem- Divide and Conquer

- Discovered the problem on HMI
- Check PLC

Locate the Problem- Spot the Difference

If we have access to a working example or system, we can spot the difference:

- Are there any differences in the configurations?
- Are there any differences in the logs?
- Any differences in the installation?

No? There may be a difference in the hardware

- If possible, try trading parts
- When the problem moves, you've found the source

Spot the difference can work even if we don't fully understand how it all works!

Sensor and Signal Troubleshooting

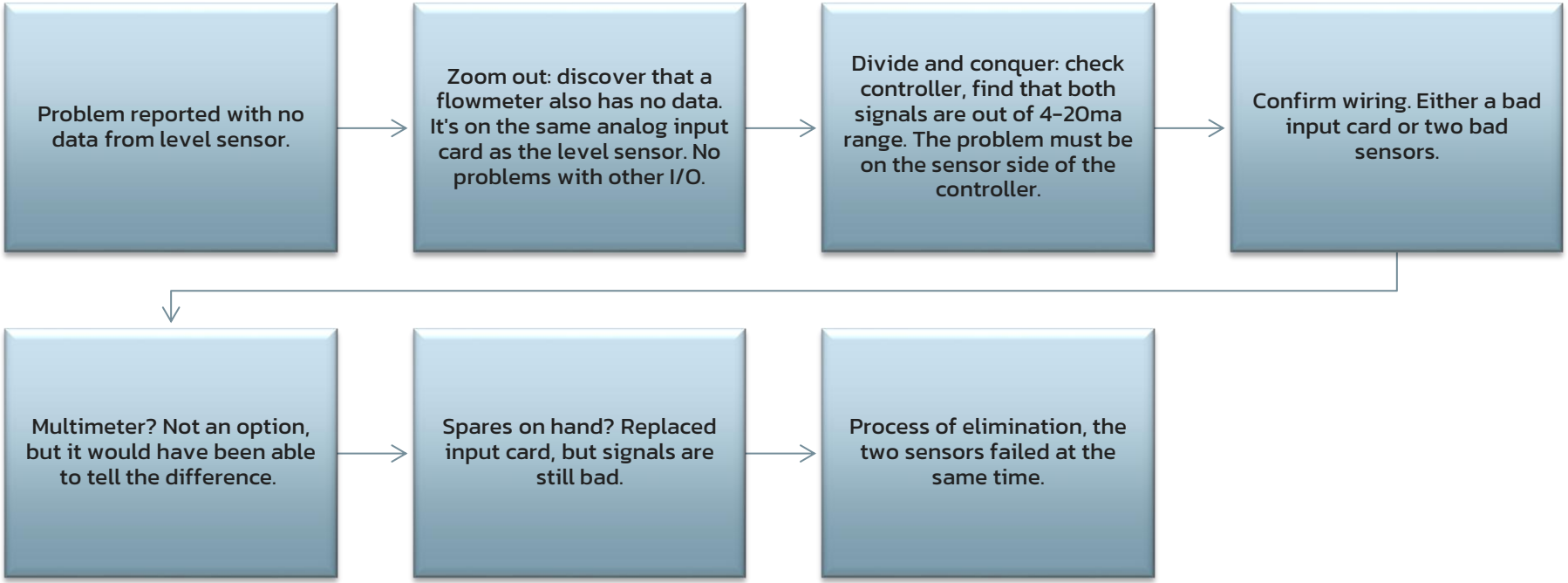
Spares

- Rule out or confirm hardware problems
- Can be a rapid way to find a working solution

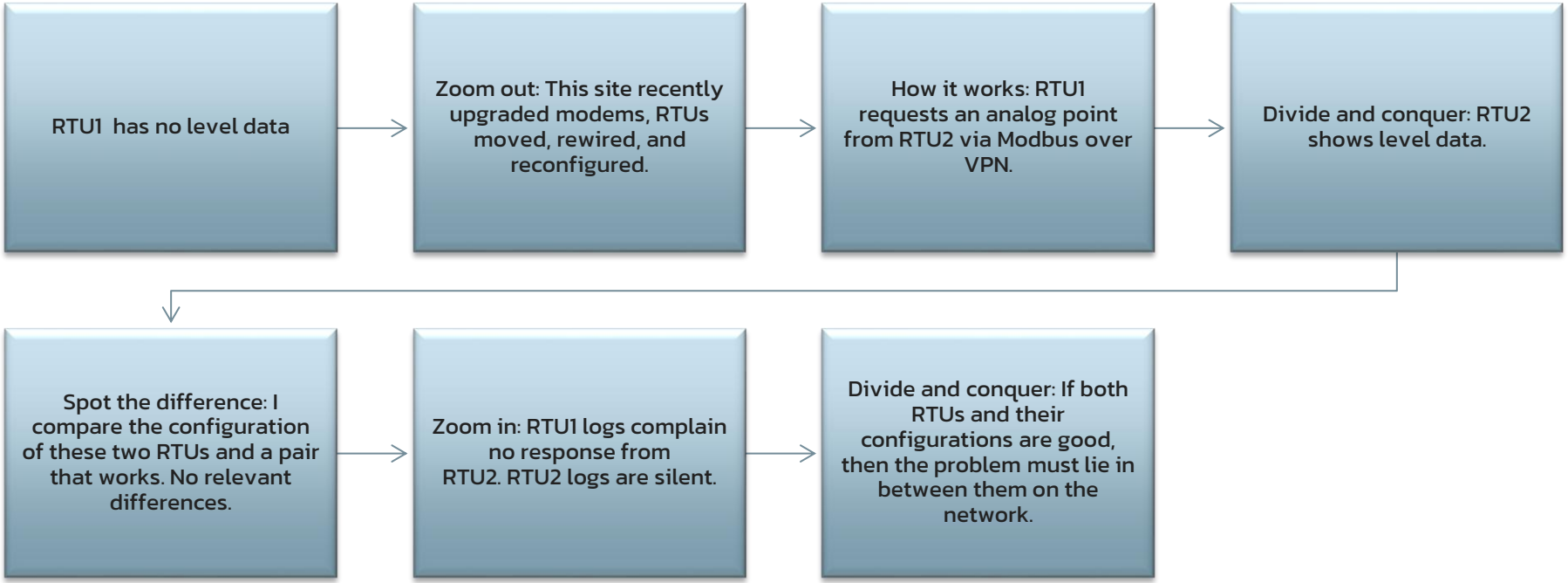
Multimeter

- Confirm voltage to powered devices
- Confirm signal
- Check continuity

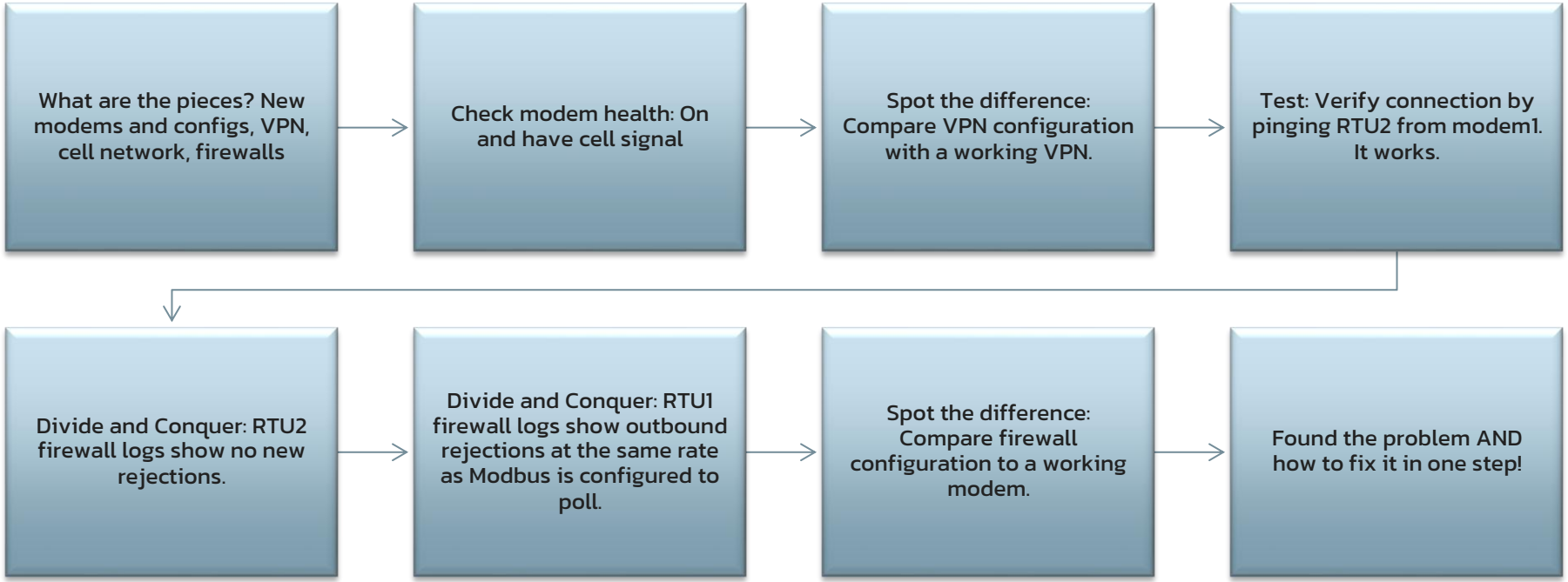
Real World Example 1: No Level Data



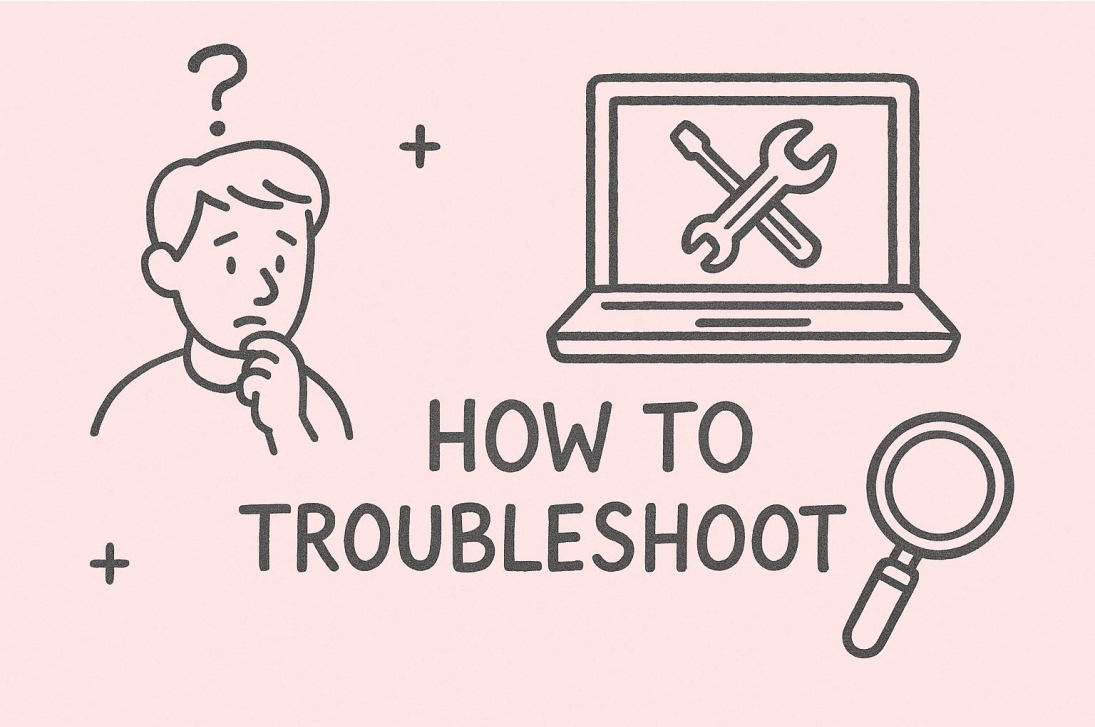
Real World Example 2: Telemetry Trouble



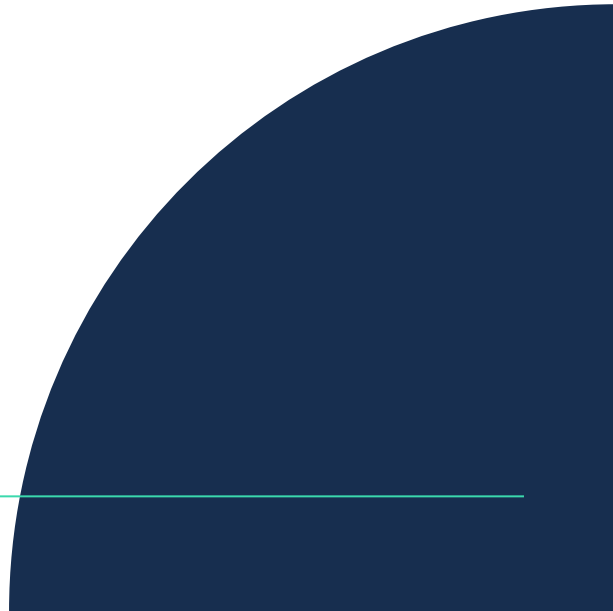
Real World Example 2: ~~Telemetry~~ Network Trouble



Questions About Troubleshooting?



Risk Management



What is Risk Management?

Knowing what could go wrong and preparing for it

- Physical security
  - Malicious tampering
  - Vandalism or theft
- Disasters
  - Power outage
  - Destructive weather: Flood, lightning, wind...
- Cybersecurity

What Can We Do To Mitigate Risk?

- Physical security
  - Locks, gates, fences
  - Surveillance systems
- Disasters
  - Backup power supply, generator, battery UPS
  - Spare parts, redundant equipment
  - Procedures for manual takeover

Create a Personal Plan

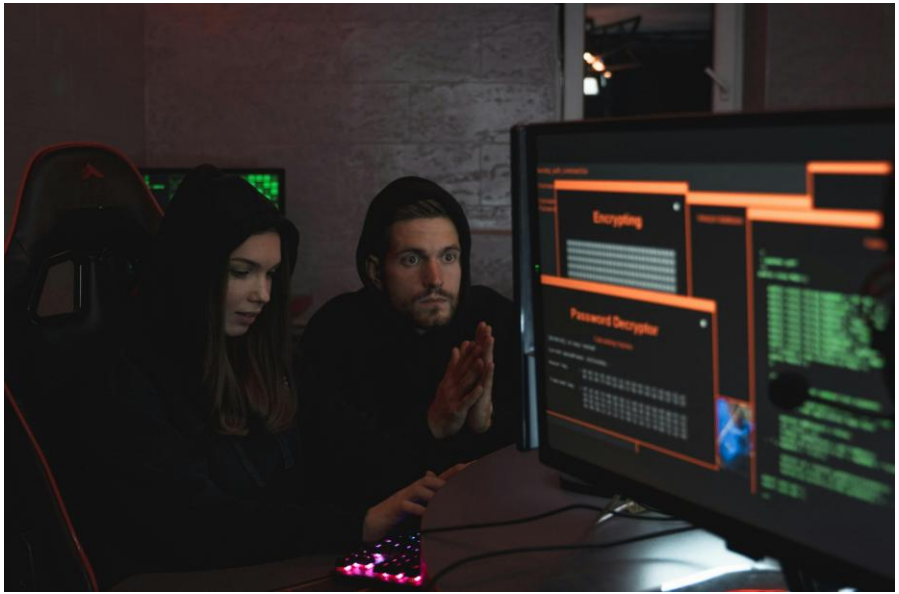
Risk Management is not one-size-fits-all

- Each facility faces different risks
- Prepare according to your ability
- Weigh mitigation against probability and severity

Cybersecurity

What is Cybersecurity?

- Protecting computer systems
- A specific kind of risk management.



Cybersecurity for SCADA Systems

Why are SCADA systems vulnerable to cyberattacks?

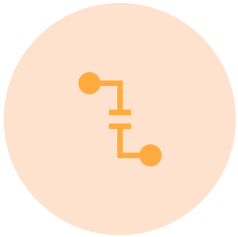
- Valuable targets
  - 2006–2023 there were 27 publicly disclosed cyber events in US water and wastewater
  - Critical infrastructure
  - Health and safety rely on dependable operation
- Made up of computers and networks
  - Controllers, PLCs, VFDs account for nearly 60% of the vulnerabilities
  - Need to be network-connected

Attack Vectors

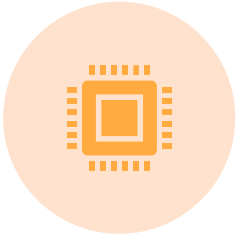
- Networks
- Authentication
- Software vulnerabilities

Minimizing Network Threats

Know what is connected to the internet



If possible, disconnect devices from public internet



Use firewalls, only allow necessary traffic between specific clients

Keep SCADA networks separate from other networks

Protecting Authentication

- Change factory default passwords
- Use strong passwords
- Use multi-factor authentication where you can
- Log authentication attempts. Be aware of failed attempts and unusual times.
- Change shared passwords when employees leave

Patching Software Vulnerabilities

- Apply security patches
  - According to a report by the FBI, NSA, and Cybersecurity and Infrastructure Security Agency (CISA), "In 2022, malicious cyber actors exploited older software vulnerabilities more frequently than recently disclosed vulnerabilities and targeted unpatched, internet-facing systems."
- Follow manufacturer guidelines
  - Nobody knows the equipment better than they do
- Patching software or firmware introduces risk. Balance it against exposure.

Questions About Risk Management or Cybersecurity?