

SANS

# Analyzing OT Radio Implementations for Attack Surface

Don C.Weber - @cutaway

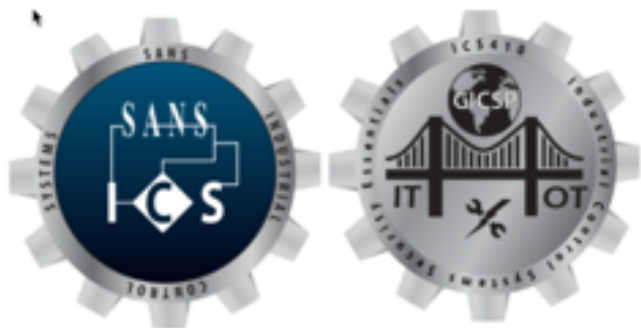
Cutaway Security, LLC.

Principal Consultant, Founder

© 2020 Cutaway Security, LLC. All Rights Reserved.



# Don C. Weber / Cutaway Security, LLC



SANS ICS410: ICS/SCADA  
Security Essentials



Assessing and Exploiting  
Control Systems

- ICS Security Assessments
- Penetration Testing
- Security Research



# Special Thanks



# ICS VILLAGE



## ICS410 ICS/SCADA Security Essentials

A mix of hands-on and theoretical class, being driven by a high skilled instructor, makes this the best training in ICS security.

**Rafael Issa, Technip**

### About the course

ICS410 is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

**REGISTER TODAY**



ICS410 Challenge Coin



# Disclaimer



Images and references within the presentation, unless specifically identified, are not meant to imply vulnerabilities in the vendor's solution. Proper implementation is typically, depending on the vendor, located in the solution's implementation guides.

Please read these guides and outline security requirements during the planning phases and integrate into factory and site acceptance testing.



# Why are we here?



Point-to-point connections

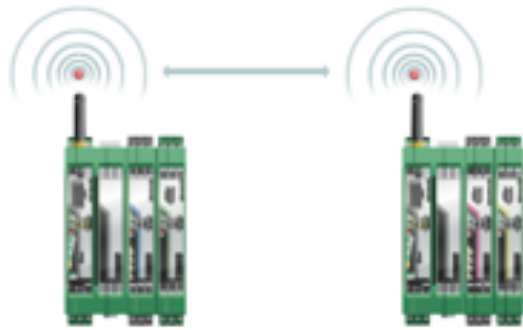
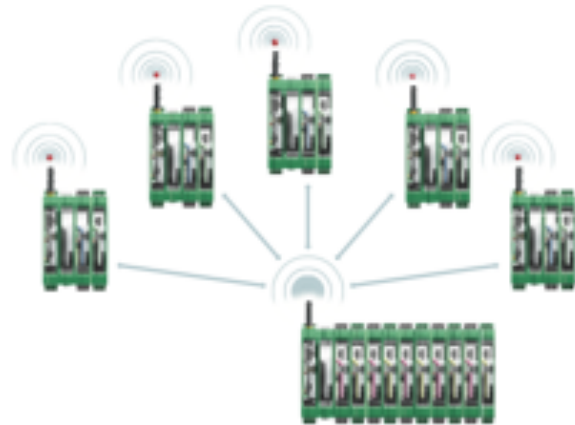


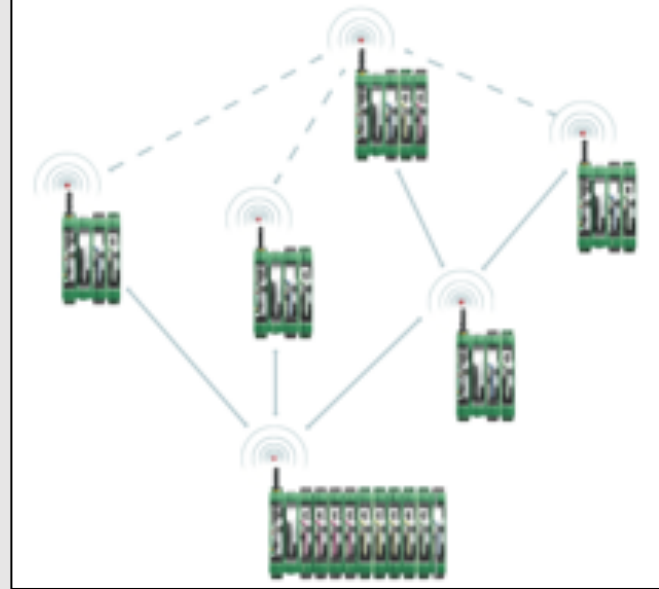
Figure 12 Example of point-to-point connection

Star network



- Radio gateways and end-points provide connectivity where wires cannot be used.
- Radio enabled end-points monitor and control the process.
- Radios will always receive, and attempt to process, any data (malicious or otherwise) sent to it.

Self-healing network



Source: Phoenix Contact RAD-900 User Manual  
<https://www.phoenixcontact.com/online/portal/us?uri=pxc-oc-itemdetail:pid=2702877&library=user&tab=1>



# Three Eternal Truths of Wireless Security + 1

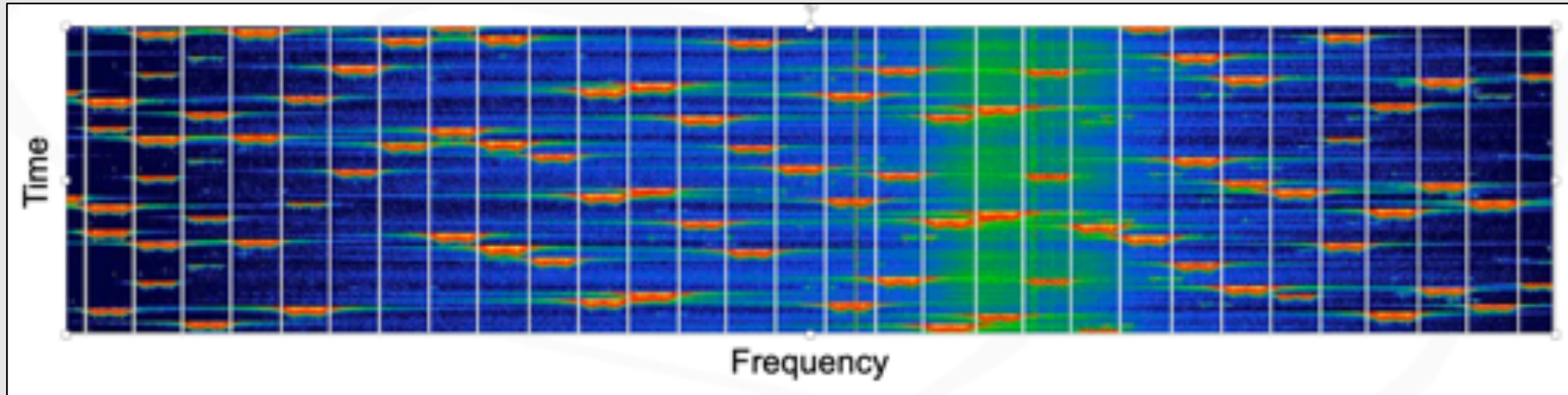


- Denial-of-Service attacks are easier and near impossible to defend against
  - Network capture is possible, regardless of frequency or hopping techniques
  - Attacker has at least a limited ability to communicate on the wireless network
- 
- "When utilizing industrial wireless for a communication path in a process, ensure the process is designed and engineered to operate safely and reliably without that communication." – Tim Conway, The SANS Institute

Source: SANS ICS410 ICS / SCADA Security Essentials  
<https://www.sans.org/course/ics-scada-cyber-security-essentials>



# Frequency Hopping



## Pros

- Prevents transmission collisions
- Helps with jamming and interference

## Cons

- Subject to eavesdropping
- Subject to injection
- False sense of security

Source: ControlThings.io Accessing and Exploiting Control Systems  
<https://www.controlthings.io/training>





# Wireless Attack Surface



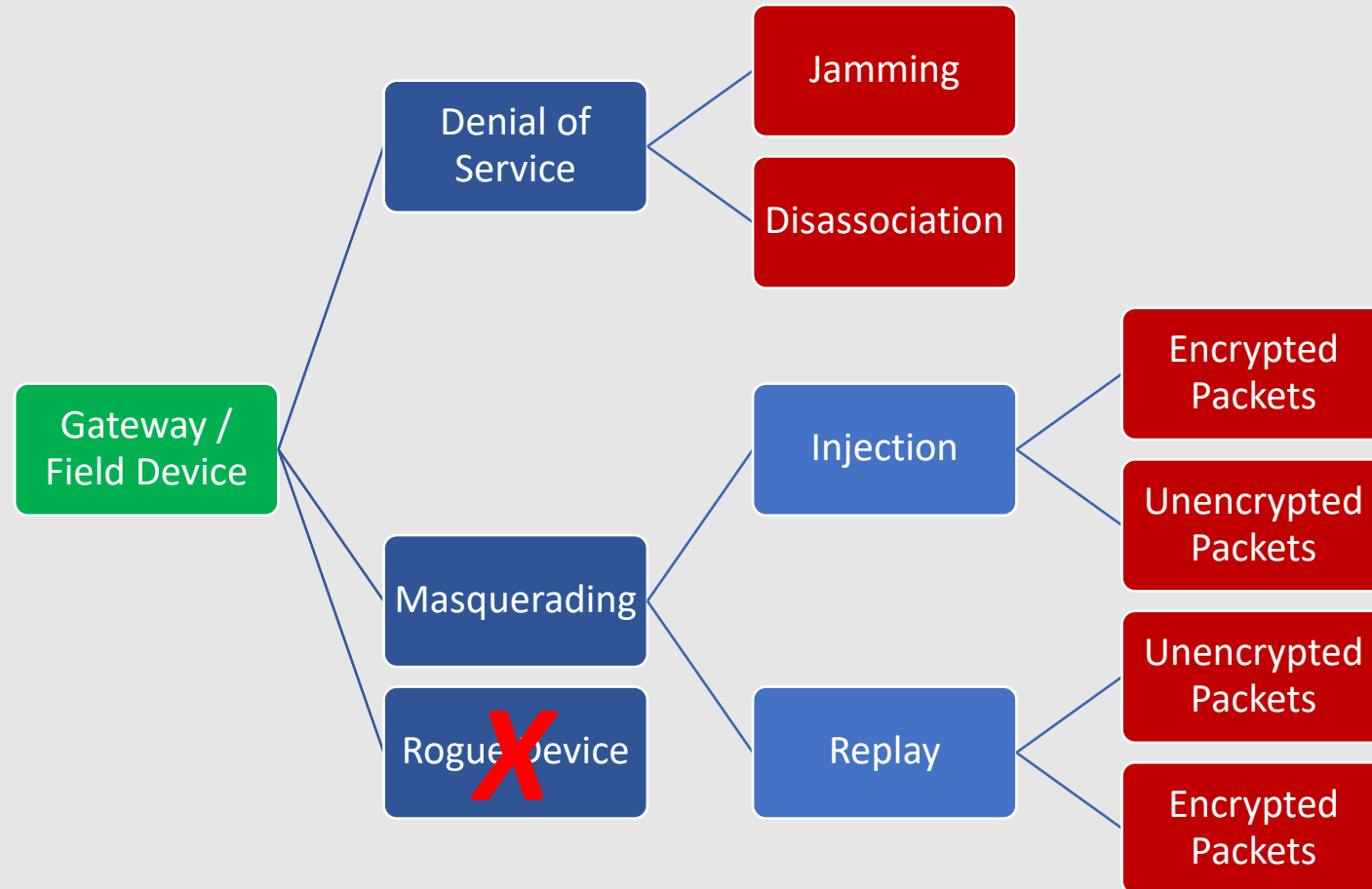
- Eavesdropping: Capturing the traffic
- Masquerading: Pretending to be your wireless network or devices
- Denial of Service (DoS): Blocking your traffic
- Rogue Access Points: Secret wireless links back to your network

Source: SANS ICS410 ICS / SCADA Security Essentials  
<https://www.sans.org/course/ics-scada-cyber-security-essentials>





# Wireless Attack Tree





# Wireless Solutions Provide Encryption




Wireless communication is based on Trusted Wireless 2.0 technology. The high demand for a interference-free data transmission using the license-free 900 MHz band, in particular via the use of the FHSS method (FHSS) and 128-bit data encryption (AES), is fulfilled.

**7 Startup and configuration**

All RAD-900-IFS wireless modules have the same default configuration.

**Default settings**

Operating mode: I/O data mode (wire in/wire out)

 Data communication is only possible using I/O extension modules.

**Wireless interface**

Net ID:	127
RF band:	1
<b>Encryption:</b>	<b>OFF</b>
Network structure:	Star
Device type:	Slave
Data rate of the wireless interface:	125 kbps
Transmission power:	1 W (30 dBm)

**Encryption Off by Default**

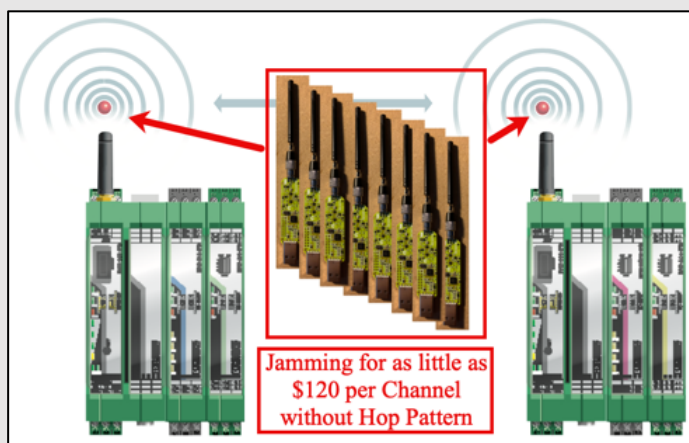
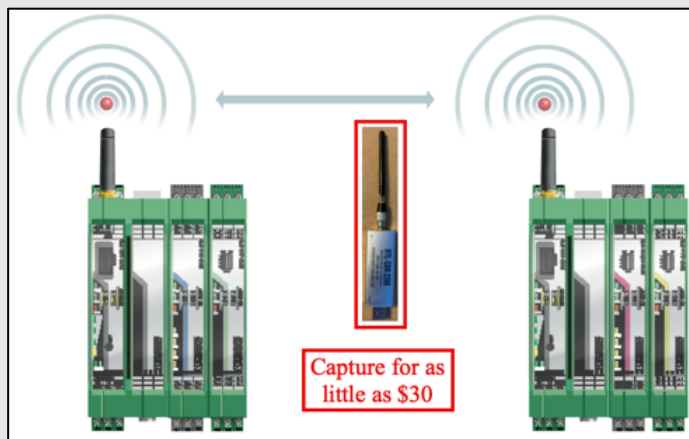
Source: Phoenix Contact RAD-900 User Manual  
<https://www.phoenixcontact.com/online/portal/us?uri=pxc-oc-itemdetail:pid=2702877&library=usen&tab=1>



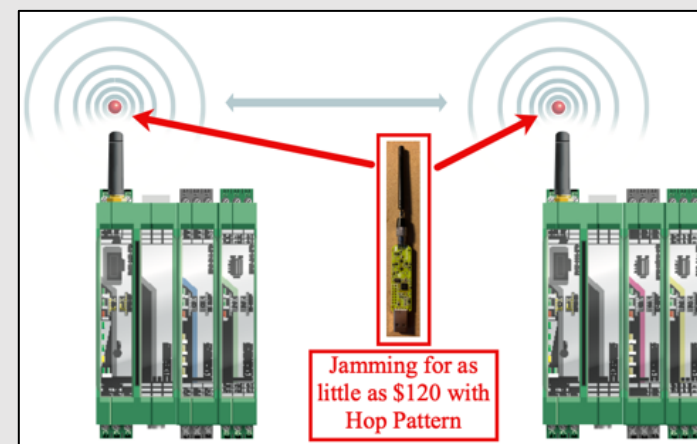
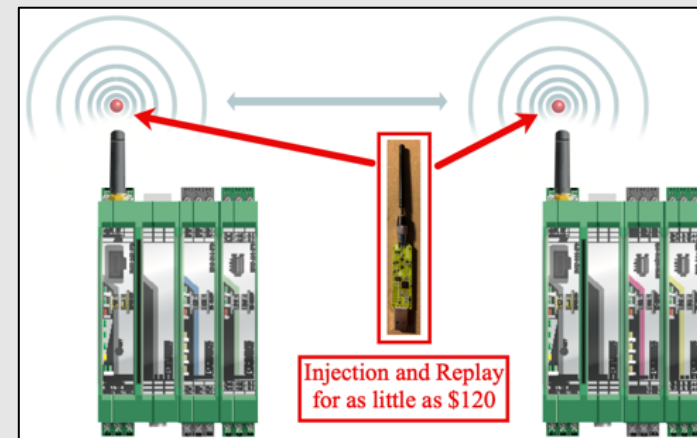
# Cost of Wireless Attacks



SANS  
ICS Industrial  
Control  
Systems



- Radios
  - RTL-SDR
  - HackRF / LimeSDR / Ettus
  - Yardstick / ApiMote / Ubertooth
  - Vendor Development Boards
- Spectrum Analyzers
  - GQRX
- Software Defined Radio
  - Universal Radio Hacker
  - Gnu Radio Companion
- Hardware Radio Software
  - RFcat
  - Killerbee / Killerzee
  - Ubertooth
  - Vendor Development SDKs

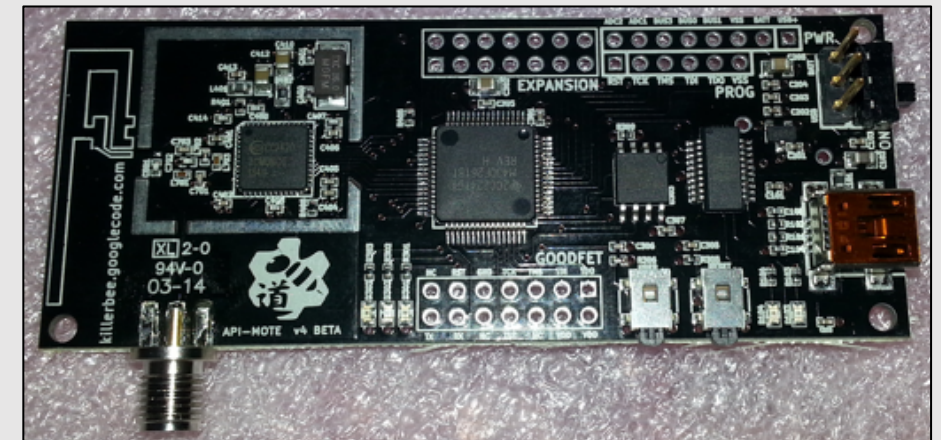
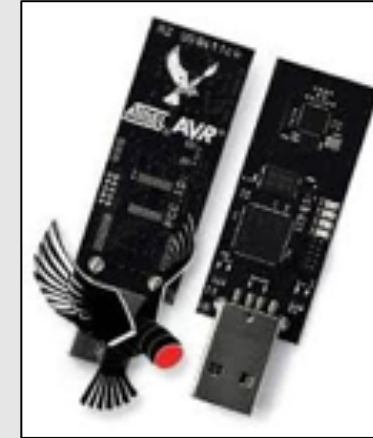




# Industrial Wireless Solutions



- WirelessHART and ISA100 Attack Tools
- Killerbee Framework and Hardware
  - 2017 RevICS Security "WirelessHART for Wireshark (and KillerBee)"
    - <https://www.revics-security.com/2017/08/02/wirelesshart-for-wireshark-and-killerbee/>
  - 2018 Nixu Cyber Security "It WISN't me, attacking industrial wireless mesh networks"
    - <https://conference.hitb.org/hitbsecconf2018dx/materials/D2T1%20-%20It%20WISN%E2%80%99t%20Me%20-%20Attacking%20Industrial%20Wireless%20Mesh%20Networks%20-%20Mattijs%20van%20Ommeren%20and%20Erwin%20Patternote.pdf>

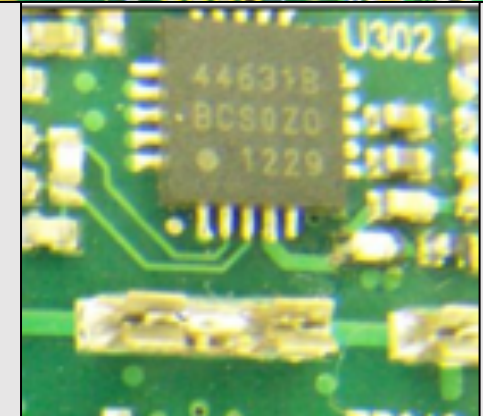
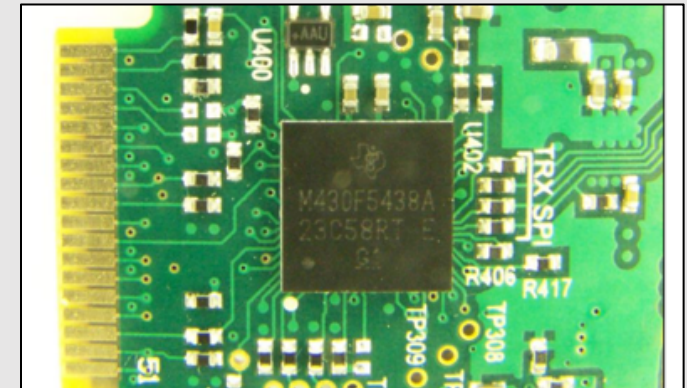




# Vendor Technical Implementation



- Additional Considerations for Wireless Implementations in Critical Infrastructure
- Radio capture and hardware analysis to determine
  - Frequency Hopping Patterns
    - Extracted from firmware analysis
    - Discovered from hardware analysis
  - Encryption Implementation
    - Data whitened transmissions appears like encryption
    - Encryption configuration and modes
    - Proprietary encryption
  - Physical programming concerns



Source: RAD-900 FCC Documentation





# Conclusion



- Understand your process and ensure it can operate when the radios cannot communicate.
- Outline security requirements before implementation.
- Test to verify requirements after implementation and maintenance.
- Support research into toolsets that help conduct assessments to ensure proper implementation.

ICS VILLAGE



Industrial  
Control  
Systems



**CUTAWAY SECURITY**  
— INFOSEC CONSULTANTS —



Don C. Weber - @cutaway  
don@cutawaysecurity.com  
<https://www.cutawaysecurity.com>

Thomas Van Norman  
<https://www.icsvillage.com/contact-us>



ICS410 ICS/SCADA  
Security Essentials

A mix of hands-on and theoretical class, being driven by a high skilled instructor, makes this the best training in ICS security.

**Rafael Issa, Technip**

### About the course

ICS410 is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

**REGISTER TODAY**



ICS410 Challenge Coin