

Industrial  
Control  
Systems



**CUTAWAY SECURITY**  
INFOSEC CONSULTANTS



# Detecting Encrypted Radio Communications Using Universal Radio Hacker

Don C. Weber - @cutaway

Principal Consultant, Founder

© 2020 Cutaway Security, LLC. All Rights Reserved.

---

Presented at SANS Gas & Oil Summit on October 2, 2020



# Cutaway Security, LLC / Don C. Weber



- ICS Security Assessments
- Penetration Testing
- Security Research

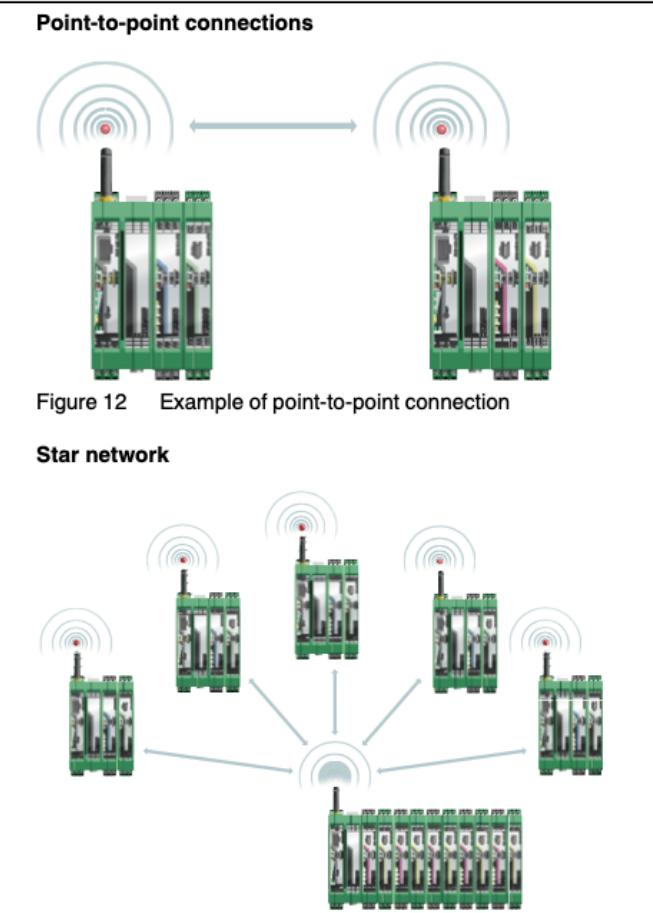
The white rectangular box contains the following elements:

- A circular logo for "SANS ICS410: ICS/SCADA Security Essentials". It features a blue gear-like background with the text "SANS" and "ICS" in white, and "ICS410" and "SCADA SECURITY ESSENTIALS" around the perimeter.
- A circular logo for "GICSP IT & OT". It features a grey gear-like background with the text "GICSP" at the top, "IT & OT" in the center, and "INDUSTRIAL CONTROL SYSTEMS" around the perimeter.
- A book cover titled "Assessing and Exploiting Control Systems". The cover is dark blue with a stylized illustration of industrial buildings, pipes, and a bridge.
- The text "SANS ICS410: ICS/SCADA Security Essentials" in blue.
- The text "Assessing and Exploiting Control Systems" in blue.

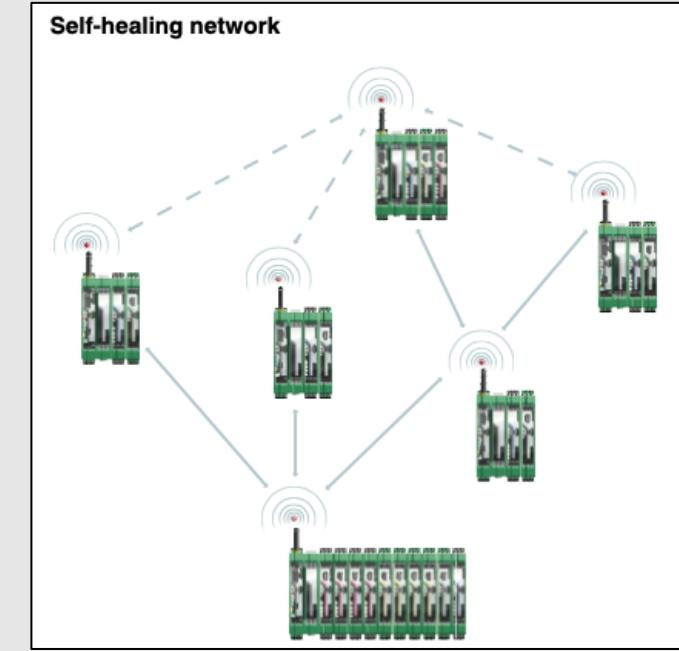




# Why are we here?



- 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.



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

# Wireless Solutions Provide Encryption

Wireless communication is based on Trusted Wireless 2.0 technology. The high demand for 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
Encryption:	OFF
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>



# 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>



# Prepare Equipment



- <https://github.com/jopohl/urh>
  - `pipenv install ipython, cython, urh, rfcat, pyserial, pyusb, pymodbus, cryptography`
- <https://greatscottgadgets.com/hackrf/one>

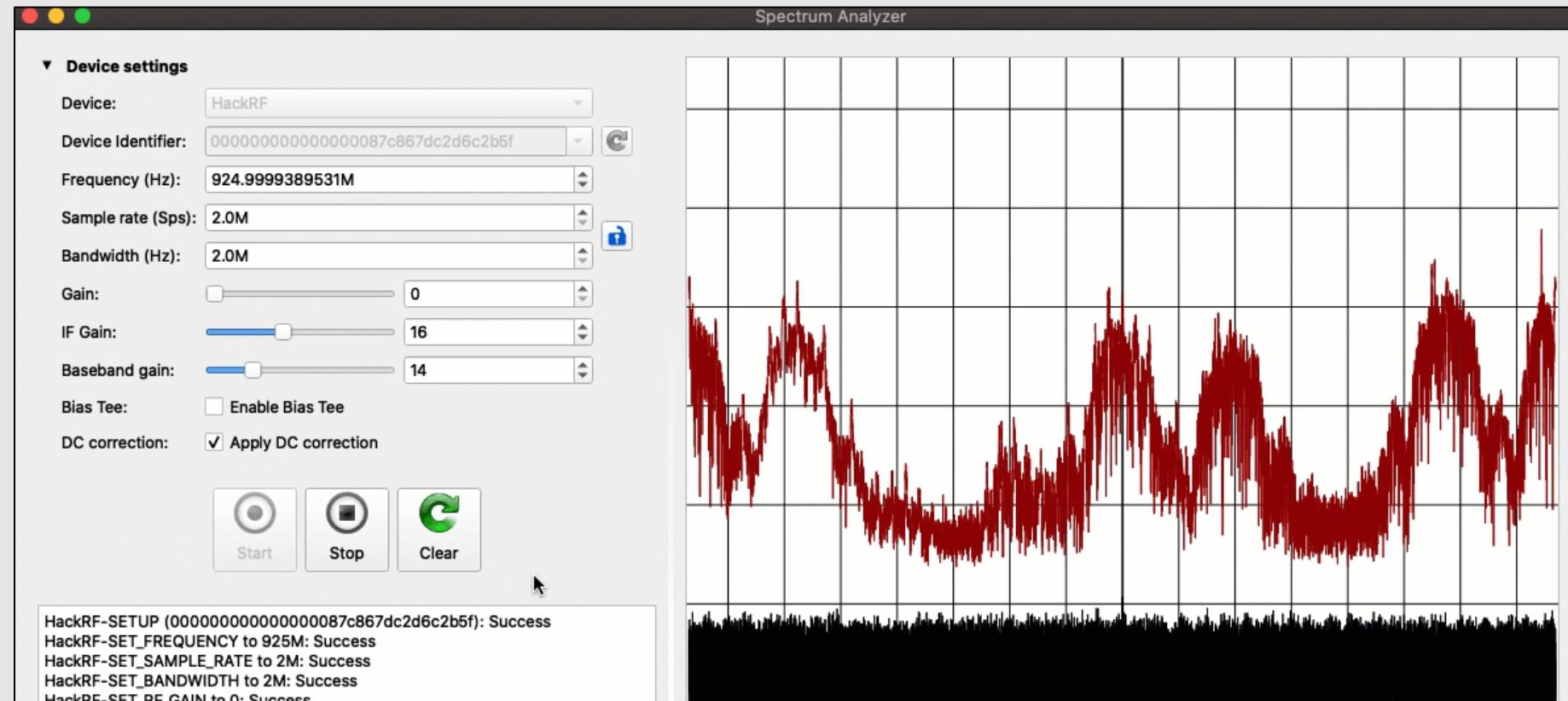




# Locate and Record Transmissions



- Select your radio and configure settings.
- Pick a frequency in the 900 MHz range.
- FHSS will hit frequencies over and over. Center on one.

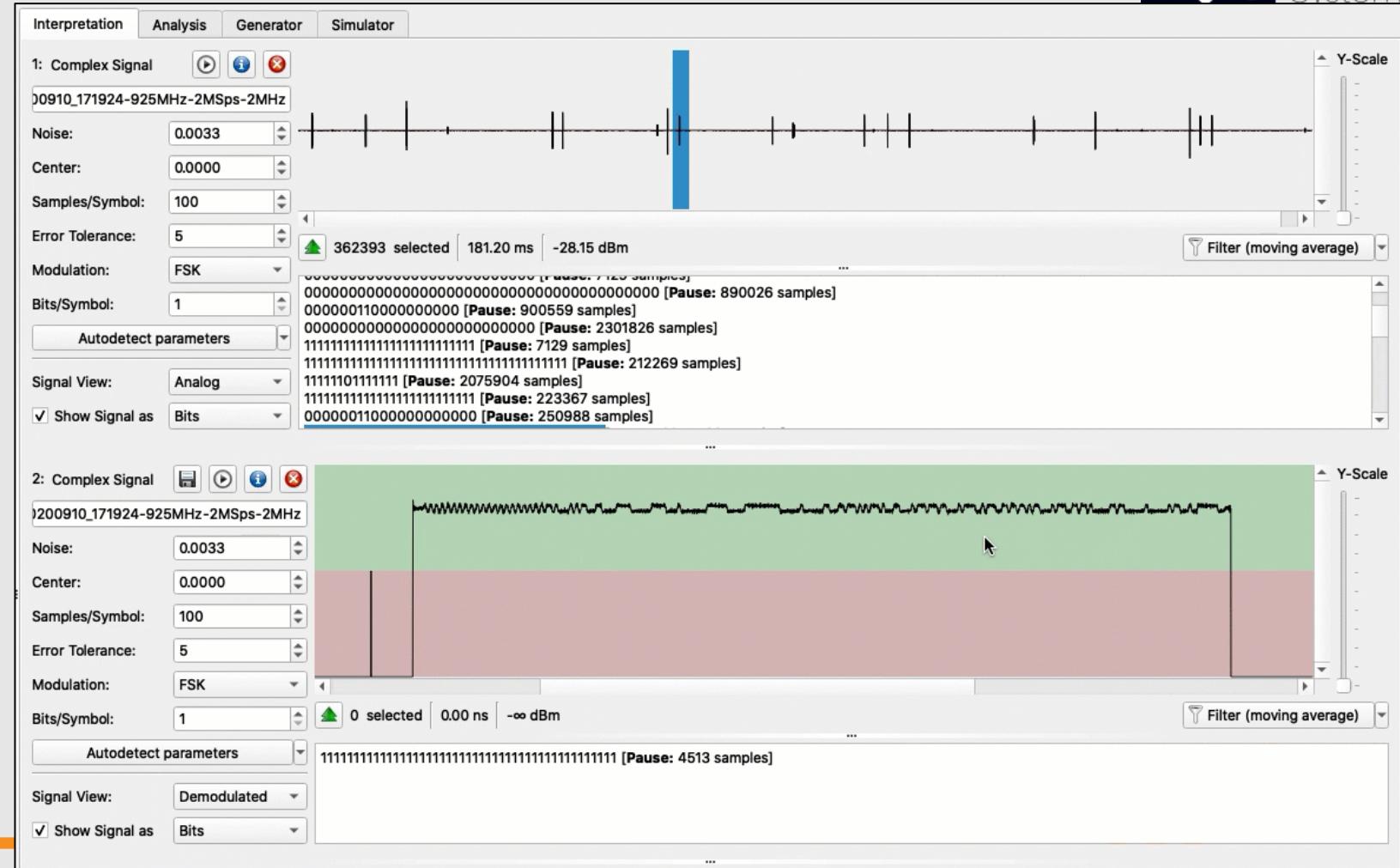




# Isolate and Analyze Transmissions



- Select a transmission to analyze.
  - Update "Center" setting to analyze transmissions not on center frequency.
  - Use waveform patterns to select Samples / Second
  - Review demodulated signal for expected patterns.

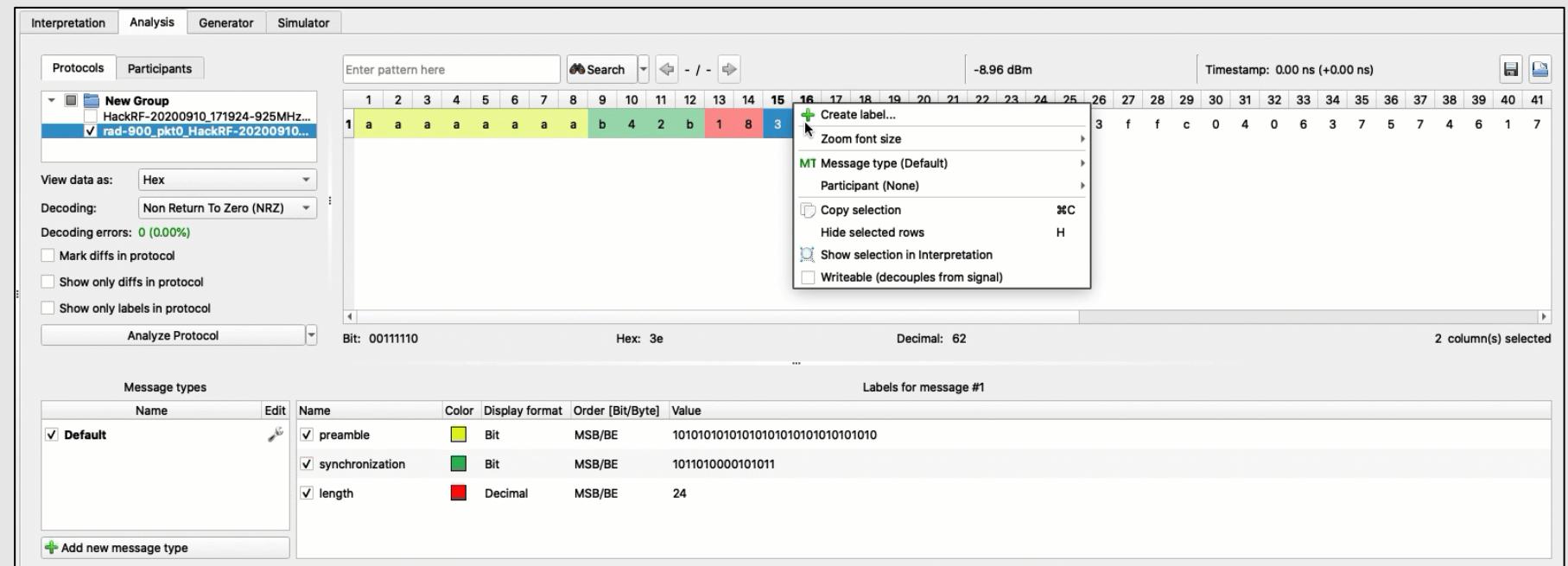




# Packet Field Identification



- Use "Analysis" tab to review packet contents.
  - Highlight and label packet contents.
  - Use these settings to automatically analyze other transmissions.





# Analyze Packet Contents





# Interesting Encryption Facts

Wireless communication is based on Trusted Wireless 2.0 technology. The high demand for 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.

- RAD-900-IFS datasheet indicates **128-bit data encryption (AES)**.
- Silicon Labs Si4463 Radio and Si4112 RF Synthesizer datasheets **do not describe on-chip encryption** or the implementation of AES.
- Texas Instruments MSP430F5438A datasheet **does not describe on-chip encryption** or the implementation of AES.
- So many questions:
  - AES uses 16-byte block size and IV should equal block size
    - "cutawaysmash" = 12 bytes
    - Encrypted data = 24 bytes? 16 bytes of data + 8 bytes of IV?
  - Management packets are not encrypted
  - Only data is encrypted, not full packet

# Assessment Continued...



- Encryption Analysis
  - Send data with different byte lengths playing with block boundaries.
  - Send same data using different keys and key lengths.
  - Phoenix Contact PSI Conf accepts key lengths of "min. 4, max 16 characters".
- Retransmit packets
  - Properly configure URH to resend captured packets via HackRF
  - Configure Yardstick One to send packet using rfcat
- Determine if radio protocol can be used for Denial-of-Service attacks.
- Redo all testing using Modbus commands to control end-points.



# Non-technical Radio Security Assessment



1. Obtain managing radio configuration file. \*
2. Grep 'Encryption' \*\*
3. Note results \*\*\*
4. ???? \*\*\*\*
5. Profit

```
Windows PowerShell
PS CutSec 09/09/2020 14:05:38
> Select-String .\*.dat -Pattern Encryption
radio_preso_serial-rad-900_20200907.dat:18:RadioEncryptionEnabled=False
radio_preso_serial-rad-900_20200907.dat:19:RadioEncryptionKey=
radio_preso_serial_enc-rad-900_20200909.dat:18:RadioEncryptionEnabled=True
radio_preso_serial_enc-rad-900_20200909.dat:19:RadioEncryptionKey=0000
PS CutSec 09/09/2020 14:05:40
```

\* Phoenix Contact RAD-900-IFS, in this example

\*\* You'll be on Windows, so `Select-String .\ -Pattern Encryption`

\*\*\* Mitigate here, if these are your radios. If not, note "Key" value.

\*\*\*\* ???? is shorthand for Report / Document

A large, stylized letter "S" logo, half red and half orange, positioned to the left of the word "Conclusion".

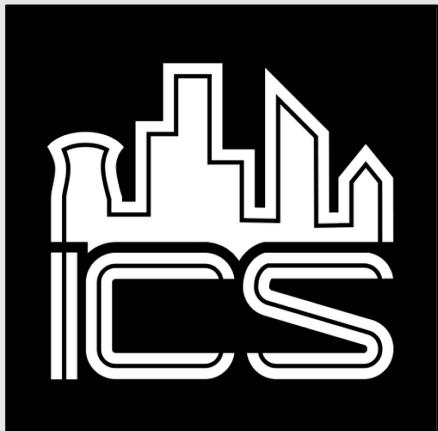
# Conclusion

- Understand your process and ensure it can operate when the radios cannot communicate.
- Default settings are not encrypted and can be intercepted and analyzed.
- Test to verify requirements after implementation and maintenance.
- Support research into toolsets that help conduct assessments to ensure proper implementation.





# Special Thanks



ICS VILLAGE



ICS410 ICS/SCADA  
Security Essentials

## 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



# iMovie: Analyzing Radio Transmissions Using URH



# Analyzing Radio Transmissions Using URH

<https://www.cutawaysecurity.com>



[https://www.cutawaysecurity.com/wp-  
content/uploads/2020/09/CutSec\\_WWHF\\_URH\\_HowTo2.mp4](https://www.cutawaysecurity.com/wp-content/uploads/2020/09/CutSec_WWHF_URH_HowTo2.mp4)



Industrial  
Control  
Systems



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

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



ICS410 ICS/SCADA  
Security Essentials

#### 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