SECURITY CONSIDERATIONS FOR WATER SUPERVISORY, CONTROL, AND DATA ACQUISITION RADIO

Water New Zealand September 2019

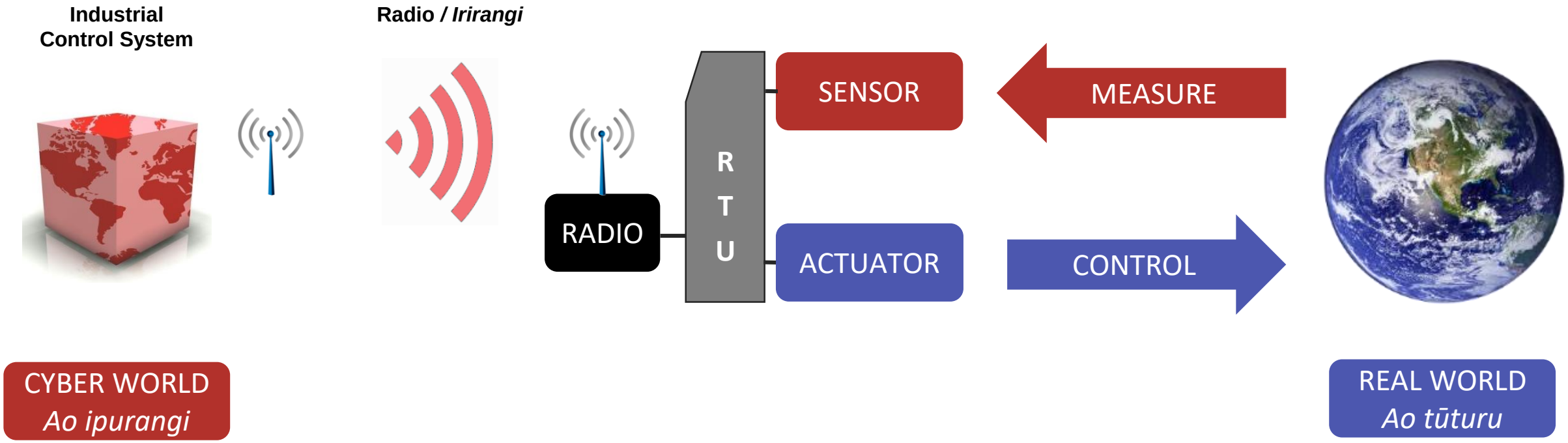
John Yaldwyn
Chief Technology Officer

4RF

SCADA – Supervision Control and Data Acquisition

Traditional transformative process, joining the real world with a digital counterpart

Connection between real world field devices and industrial control system often using wireless



UK example

Northern Ireland Water

14,130 square kilometres

1.8 million consumers

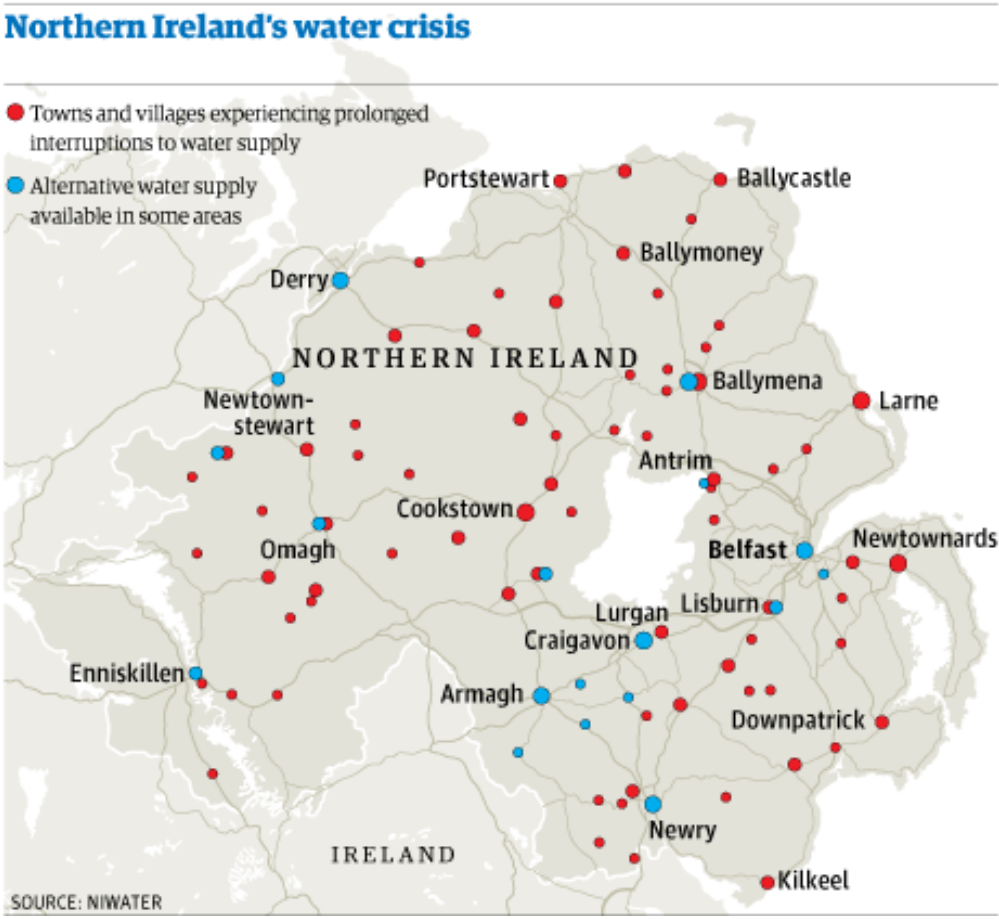
570 million litres per day fresh water

23 water treatment plants

2,540 remote telemetry radios connected to 34 duplicated master radio sites

- Telemetry device are connected via RS-232 serial
- Proteus protocol outstations at 2,400 bps and Talus T4e WITS-DNP3 outstations at 9,600 bps

Freshwater lake and reservoirs ~ 392 square kilometres



December 2010 water crisis left 40,000 people without water for more than 10 days.
Under investment driver for complete forklift SCADA system replacement.

Wellington example

Wellington Water

1,200 square kilometres

370,000 consumers

150 million litres per day fresh water

4 water treatments plants

305 remote telemetry radios connected to 19 master sites

- Telemetry RTU devices (Abbey) are connected via IP over Ethernet

River sources are the Hutt, Wainuiomata and Orongorongo Rivers

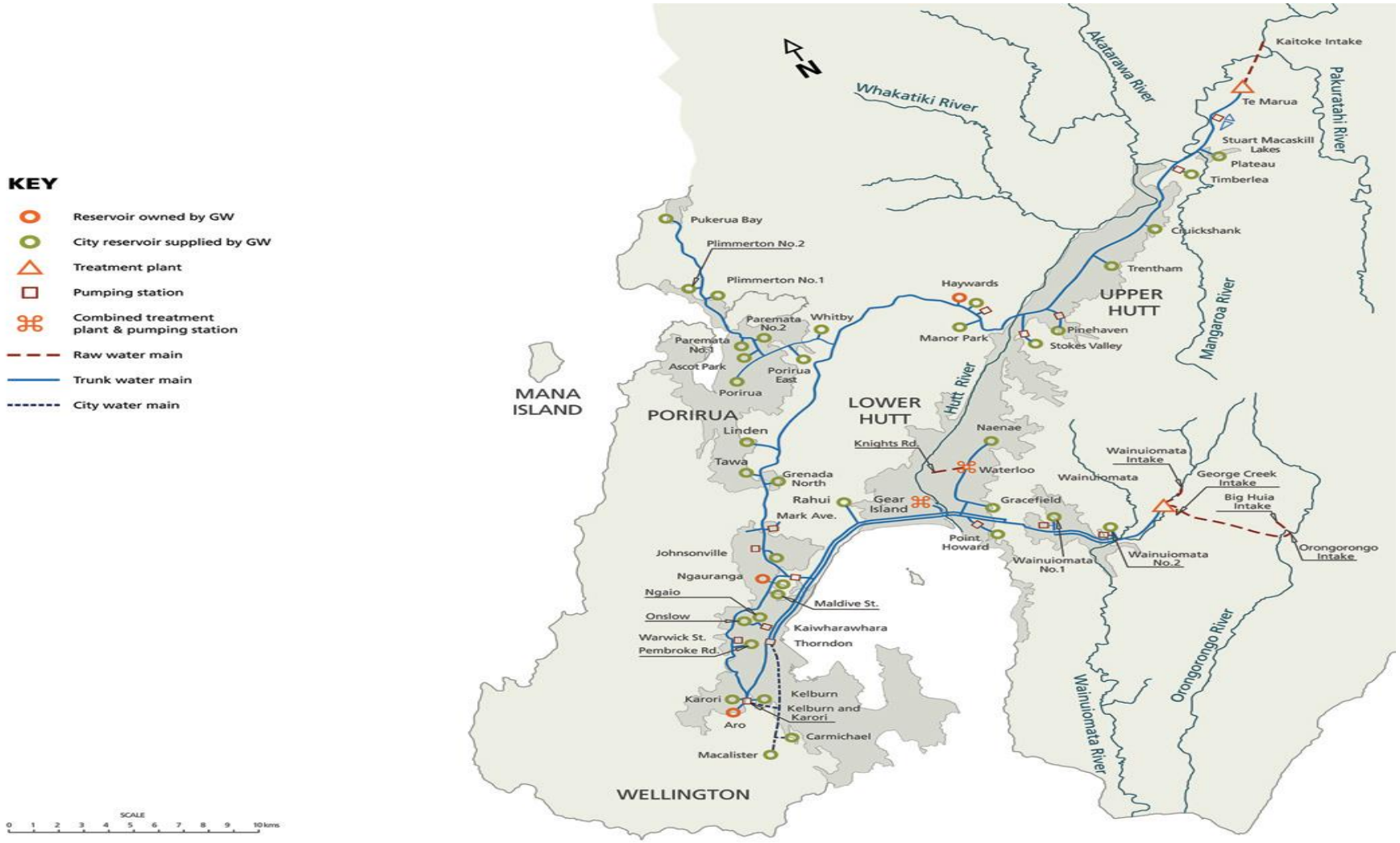
- Treated at two treatment plants – Te Marua and Wainuiomata

Ground water source is the Waiwhetu aquifer (recharged from the Hutt River)

- Treated at the Waterloo treatment plant

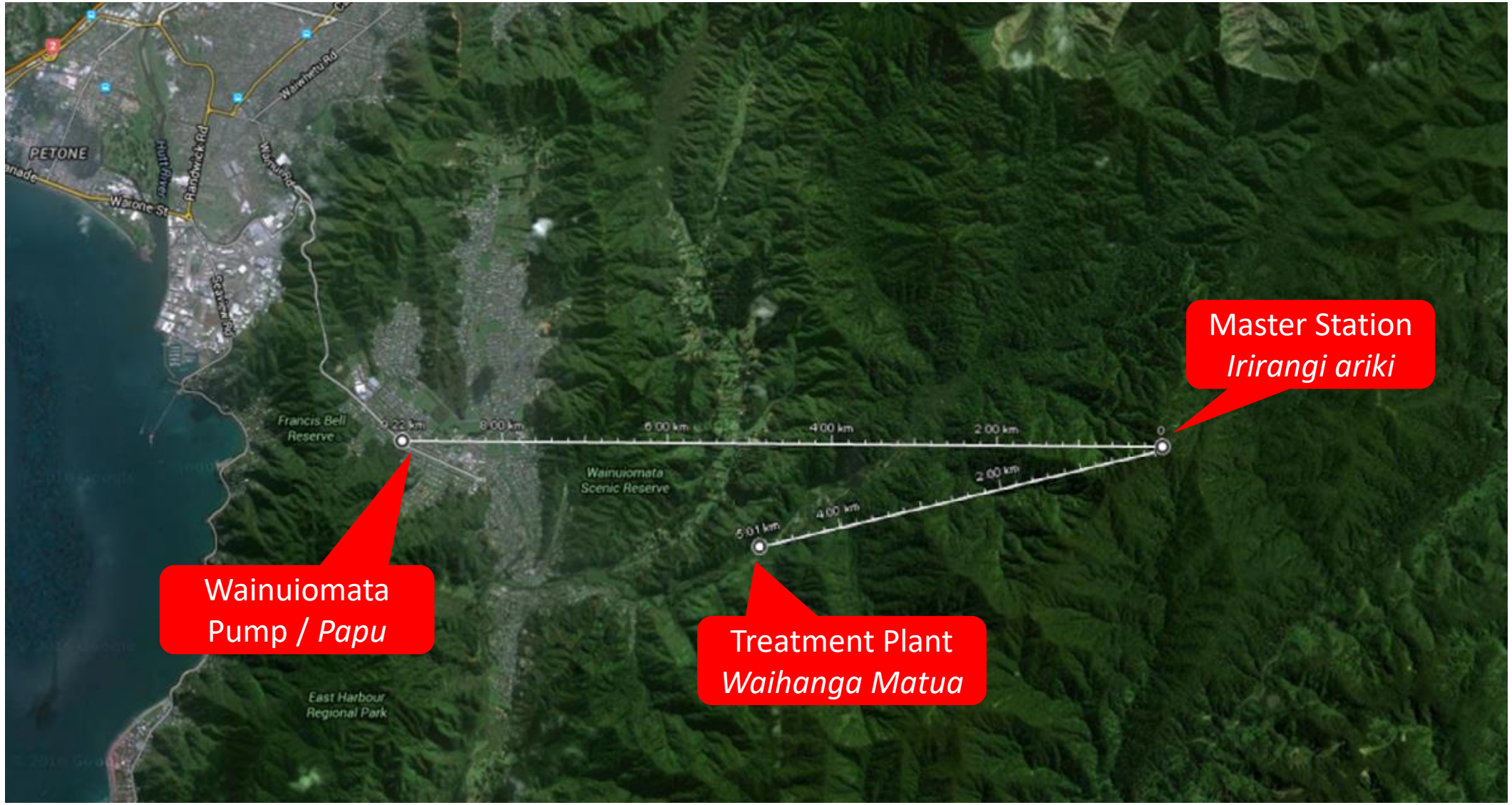
Wellington Water example

Greater Wellington Regional Council's wholesale water supply network, 2006



Mt Towai, Lower Hut

Wainuiomata and Orongorongo catchments



Australian example

Eurobodalla Shire Council

3,422 square kilometres

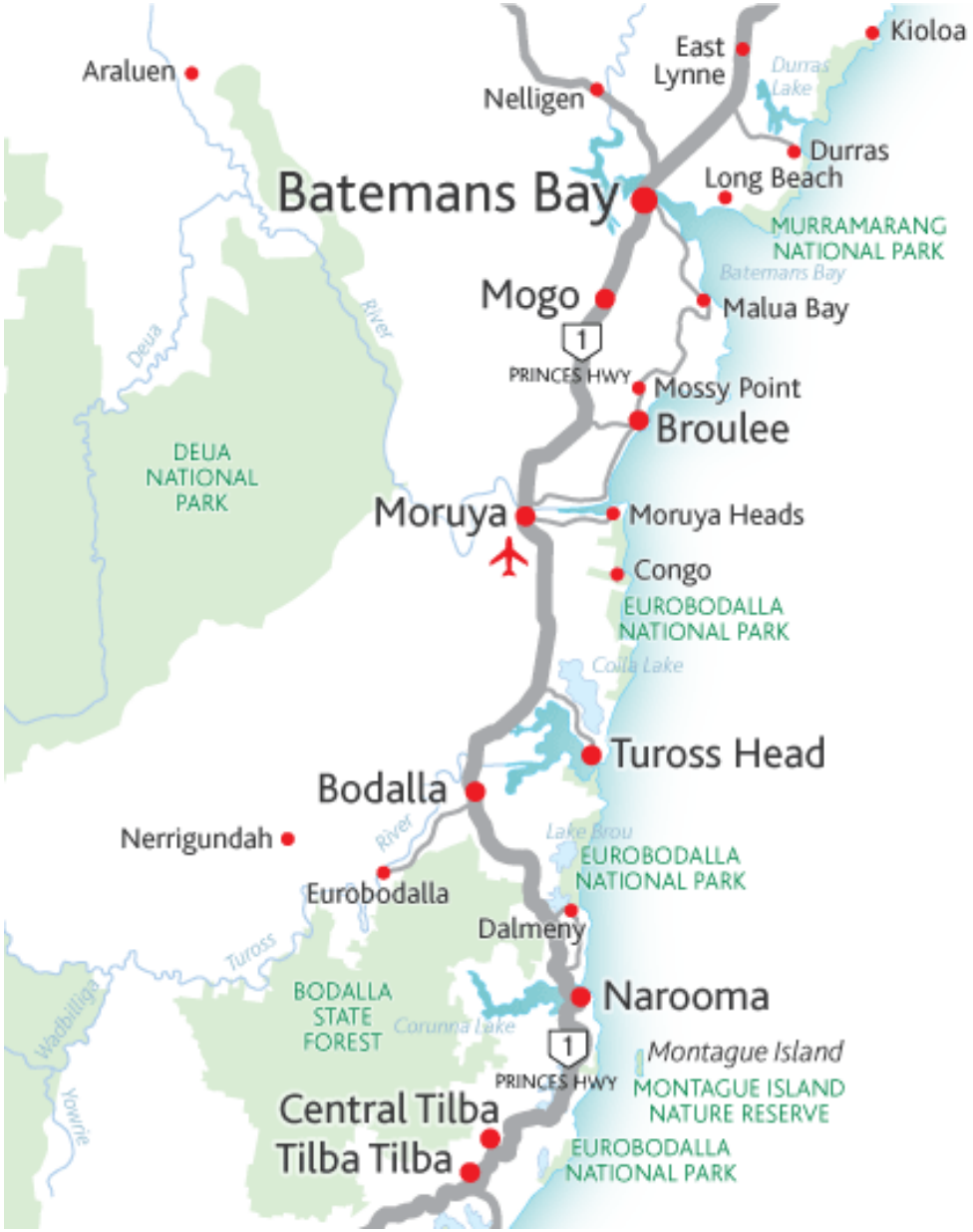
40,000 consumers

16.5 million litres per day fresh water

2 treatment plants

30 remote telemetry radios growing to 80 sites

- Telemetry (Serck PDS eNET) via DNP3 serial



Images: Eurobadalla Shire Council

Security

These wireless radio-based systems used for water utility communications are key critical infrastructure components

- Need to be reliable and resilient to avoid operational impact
- Require protection from malicious interference and cyber vandalism

Alternative systems such as cellular need careful evaluation in terms of availability and resilience

While security of supply is a top priority for water utilities, communication security often does not receive the attention it deserves

Water has **sometimes** been a **target** for hacktivists

Water **is a target** for terrorists and state actors

Security – an essential consideration

No longer just physical nor ‘security by obscurity’

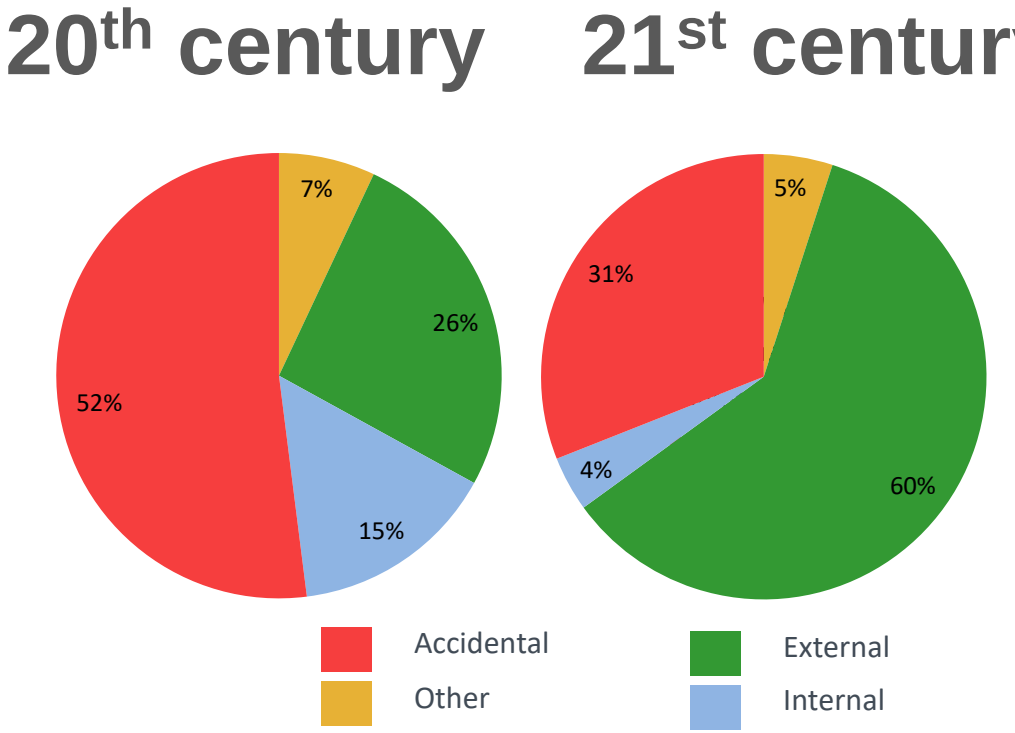
- Accidents no longer dominate risk

Open network standards enable enhanced monitoring and control

- But bring new vulnerabilities and attack opportunities

People risks

- Employees
- Ex-employees
- Those who ‘hack for fun’
- Terrorists and state actors



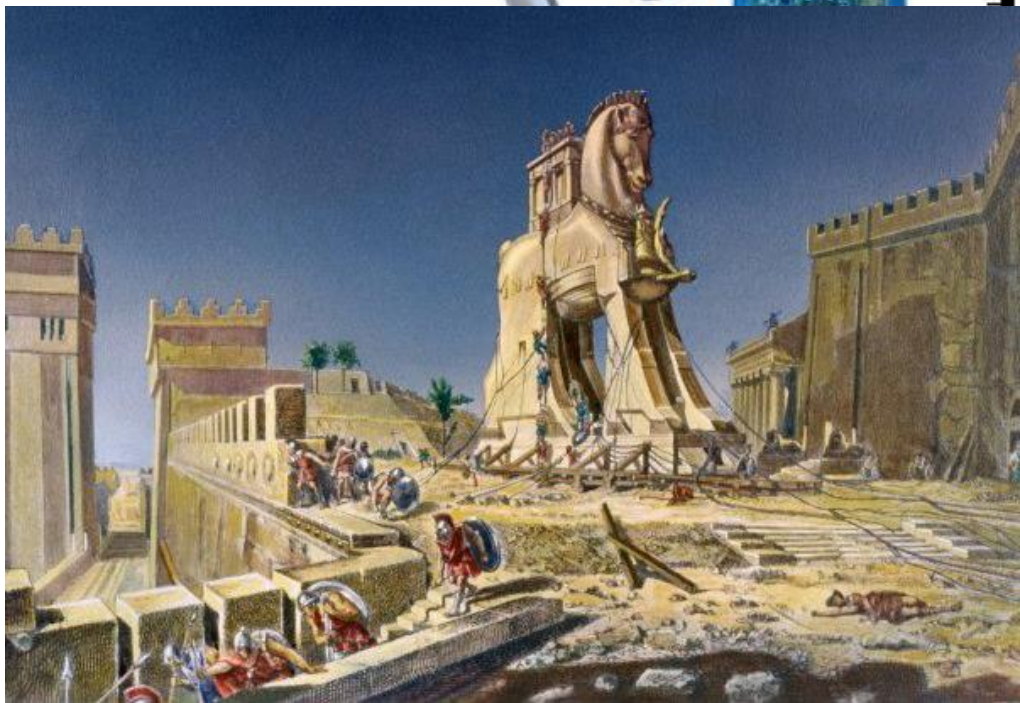
Security Incidents and trends in SCADA and process industries
Eric Byres, David Leversage, Nate Kube - British Columbia Institute of Technology

Attack vectors

Need to consider a 360-degree perimeter, review the ‘risk surfaces’ or interfaces of an individual SCADA product or ICS system for weakness.

- Interface such as serial, Ethernet, USB, and the over-the-air RF path
- Consider both user data plane and management perspectives
- Standardised IP interface risks

Trojan horse / hōiho



Protect these interfaces

Guard against malicious software

Over-the-air symmetric encryption

Encryption is used to reduce information leakage

- **Robust cryptographic algorithm important**, today this is AES

Key is symmetric, same key used to decrypt and encrypt

- AES 128 bit block with 128, 192, or 256 bit keys

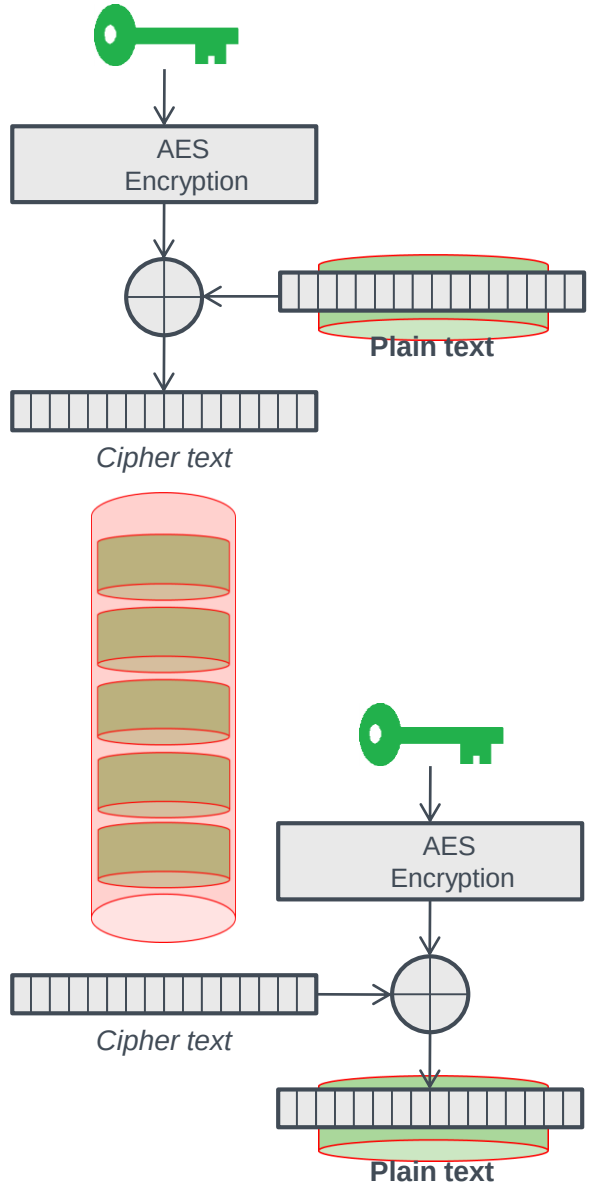
Security based on algorithm and shared secret key

- **Algorithm is public so key must be secret**

Why change the key?

- Repetitive traffic increases ‘depth’ weakens protection
- **Regularly changing key** guards against compromise

So we also need a means to distribute new keys

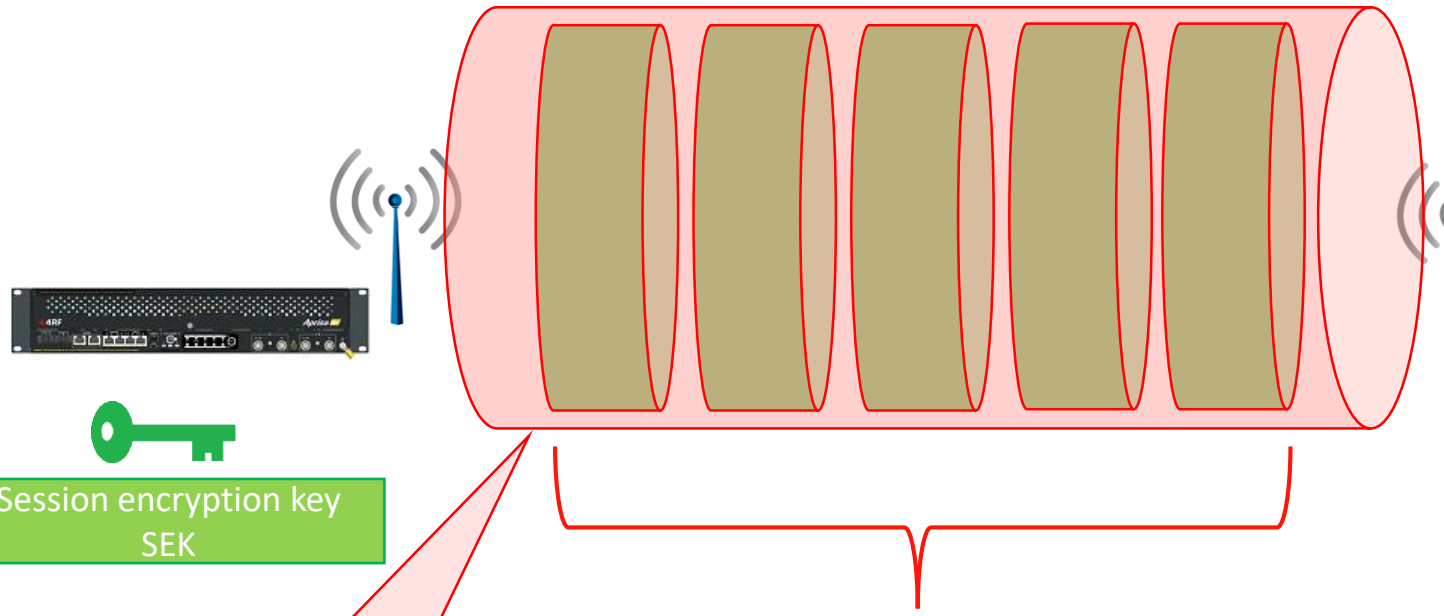


Master to remote encryption

Mater radio
Irirangi ariki

Air interface / *Irirangi*

Remote radio
Irirangi mamao



Session encryption key
SEK

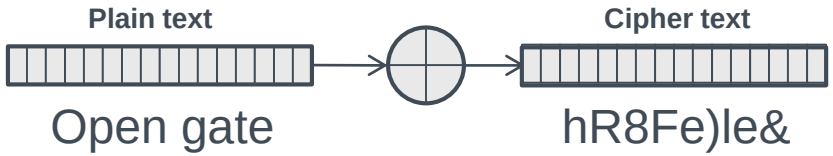
Session encryption key
SEK

NIST FIPS PUB 197 AES encryption (using Rijndael version 3.0) symmetric encryption algorithm covers all air interface packets

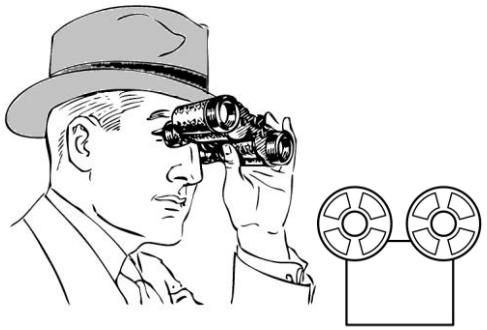
NIST SP 800-38C Cipher Block Chaining Message Authentication Code (CBC-MAC) based on NIST special publication 800-38C and RFC 3610 using AES secures packet message integrity

Security – is encryption enough?

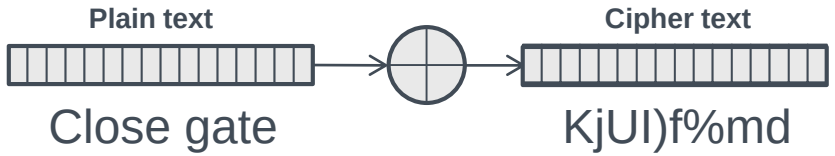
Open gate operation



Hacker / *tangata kino*



Close gate operation



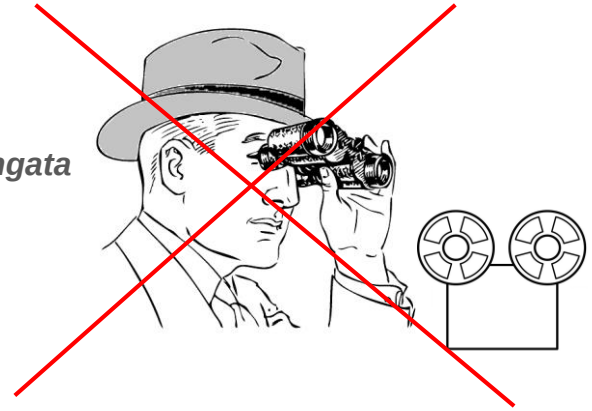
Images: Seqwater / Government of Queensland

Security – is encryption enough?

Cipher text

hR8Fe)le&

(open gate)



Hacker / *tangata kino*

Images: Seqwater / Government of Queensland

How do we stop this?

- We need a means of message authentication!

Message Authentication – CCM CBC MAC

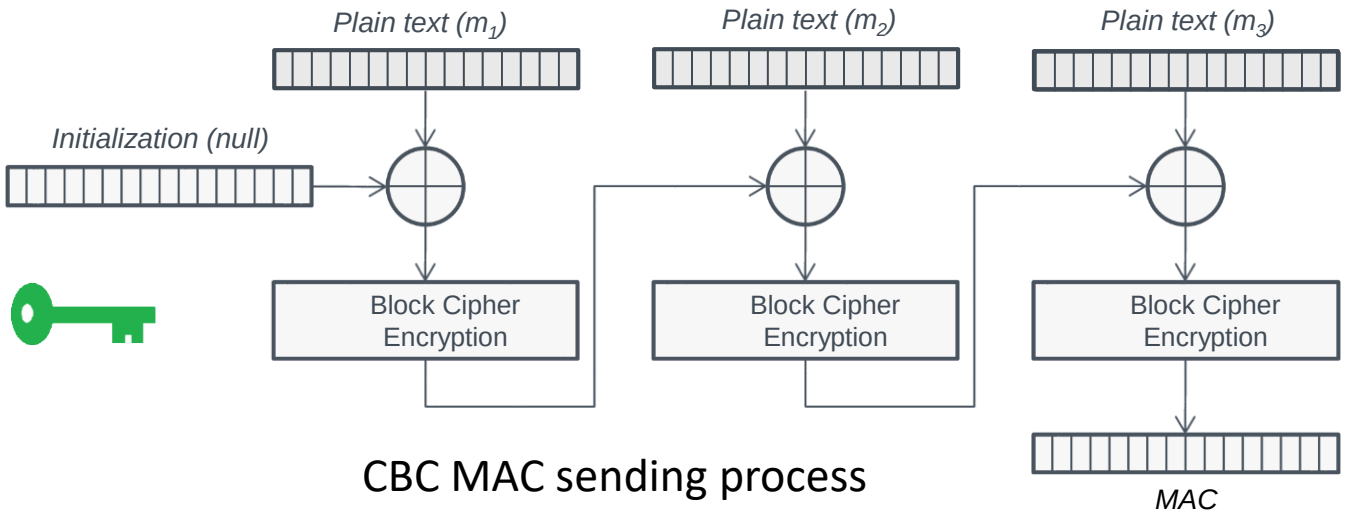
Counter mode encryption with cipher block chaining message authentication

CCM CBC MAC method with AES block cipher = NIST SP 800-38C / RFC3610

Generates message authentication code (MAC) (then optionally encrypt)

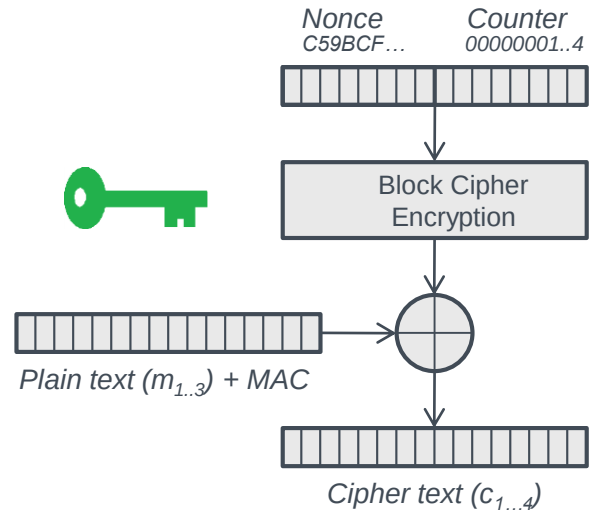
Send unique MAC with message for checking by receiver

- Method creates unique message ‘fingerprint’



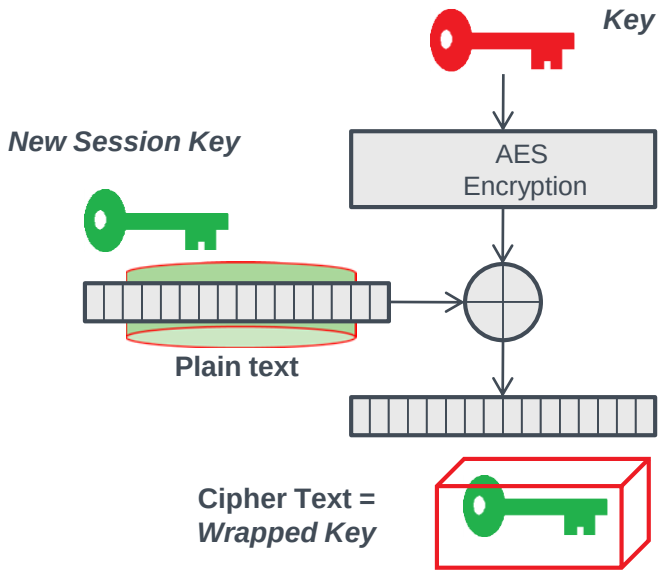
CBC MAC sending process

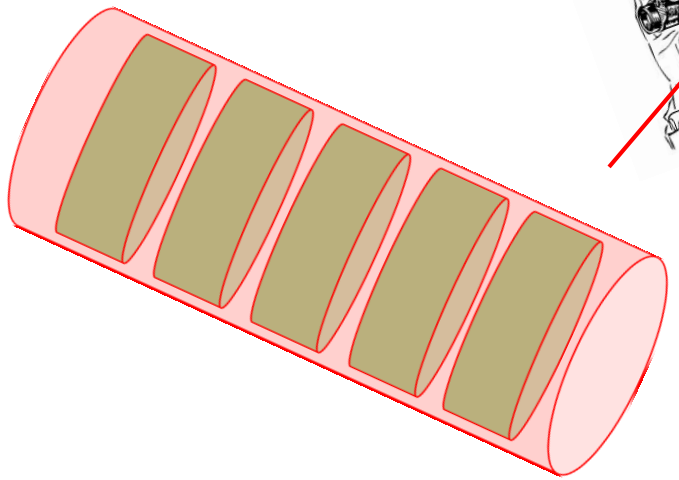
Note: diagram simplified as process is repeated once for each message plus MAC

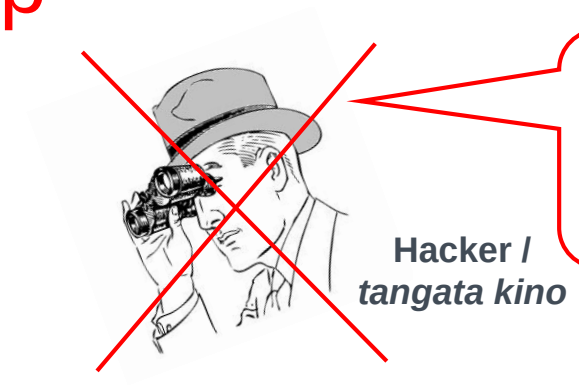


CBC MAC receiving process

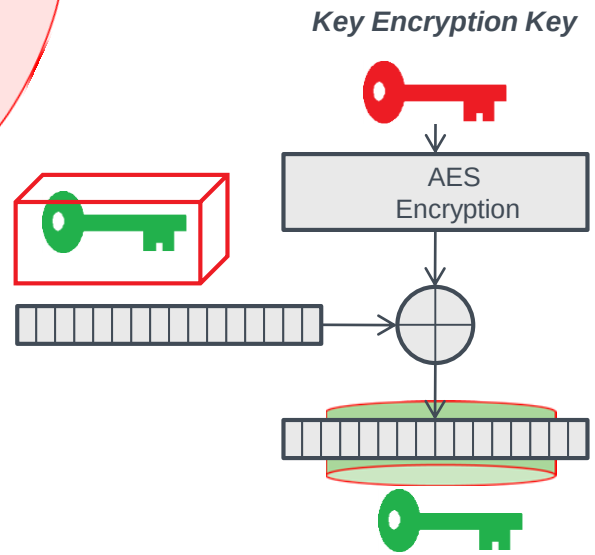
OTAR operation using Key Wrap







Even if hacker has discovered current SEK he is unable to unwrap new SEK as it is encrypted with the unique KEK



Actually not just AES but algorithm to RFC 3394

Use KEK to encrypt new SEK

- Result is wrapped new SEK

Transmit wrapped new SEK over-the-air

Unwrap new SEK using previously loaded KEK

Over-the-Air Rekeying – NSA / NIST Key Wrap

Changing encryption keys at regular intervals significantly improves the security

The NSA (NIST) Key Wrap method enables encryption keys remotely throughout the network

Key Wrap mechanism **supports the secure distribution of a session encryption key** (SEK) by encrypting with a pre-stored encryption key (KEK)

- SEK used for normal traffic transmission, changed over-the-air
- KEK used only for encrypting keys, manually loaded into terminals at deployment

The input to the key wrap process is the KEK and the new SEK treated as the plaintext

Need to carefully maintain shared secret keys, change SEK daily/monthly/quarterly as desired

Change KEK in any circumstances that could give rise to key compromise

Physical asset security: tamper audit on radio

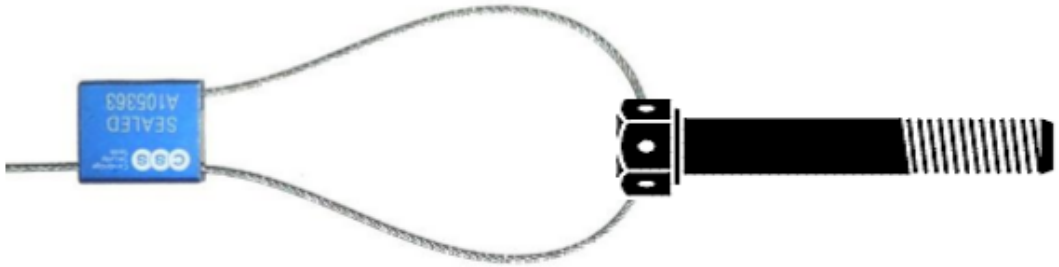
FIPS 140-2 Level 2 (physical considerations)

Tamper detection important (tamper evident seals and anti-tamper electronic detection)

Secure radio to immovable surface using drilled head bolts and meter seals

- Prevent access inside equipment without leaving evidence of attack
- Prevents physical manipulation
- Needs regular audit

Ultimate protection is electronic tamper detection

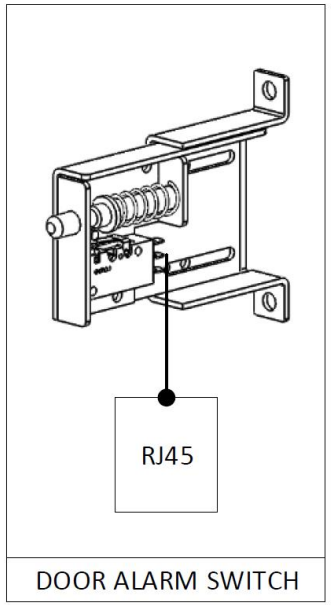


HOLO-GUARD standard FIPS Labels

Physical security: tamper detection electronic perimeter

Alarms on indoor and outdoor (shown) cabinet access

- Monitor perimeter



19” rack mount door alarm switch example

Security summary

360-degree review, attack vectors, physical security review

Over the air data encryption

- Recommend AES with 128, 192, or 256-bit keys

Data authentication - NIST SP 800-38C Cipher Block Chaining Message Authentication Code

- Based on NIST 800-38C and RFC 3610 using AES prevent or man-in-the middle hacker

Over the air re-keying of AES session keys

- Change session keys periodically to prevent collection of depth from repeated short SCADA messages

Browser TLS security

- Use modern cryptography (TLS1.2/1.3, HTTPS using 256-bit ECC or better)

Management system security

- SNMP with security (SNMPv3)

?

Thank you