



# NOJA POWER

## DNP3 Security: Challenges and Solutions

Alan Scott

**NOJA POWER SWITCHGEAR PTY LTD**

[alans@nojapower.com.au](mailto:alans@nojapower.com.au)

Co-Authors:

Grant Gilchrist – EnerNex ([grant@enernex.com](mailto:grant@enernex.com))

Andrew West – Invensys ([andrew.c.west@ips.invensys.com](mailto:andrew.c.west@ips.invensys.com))

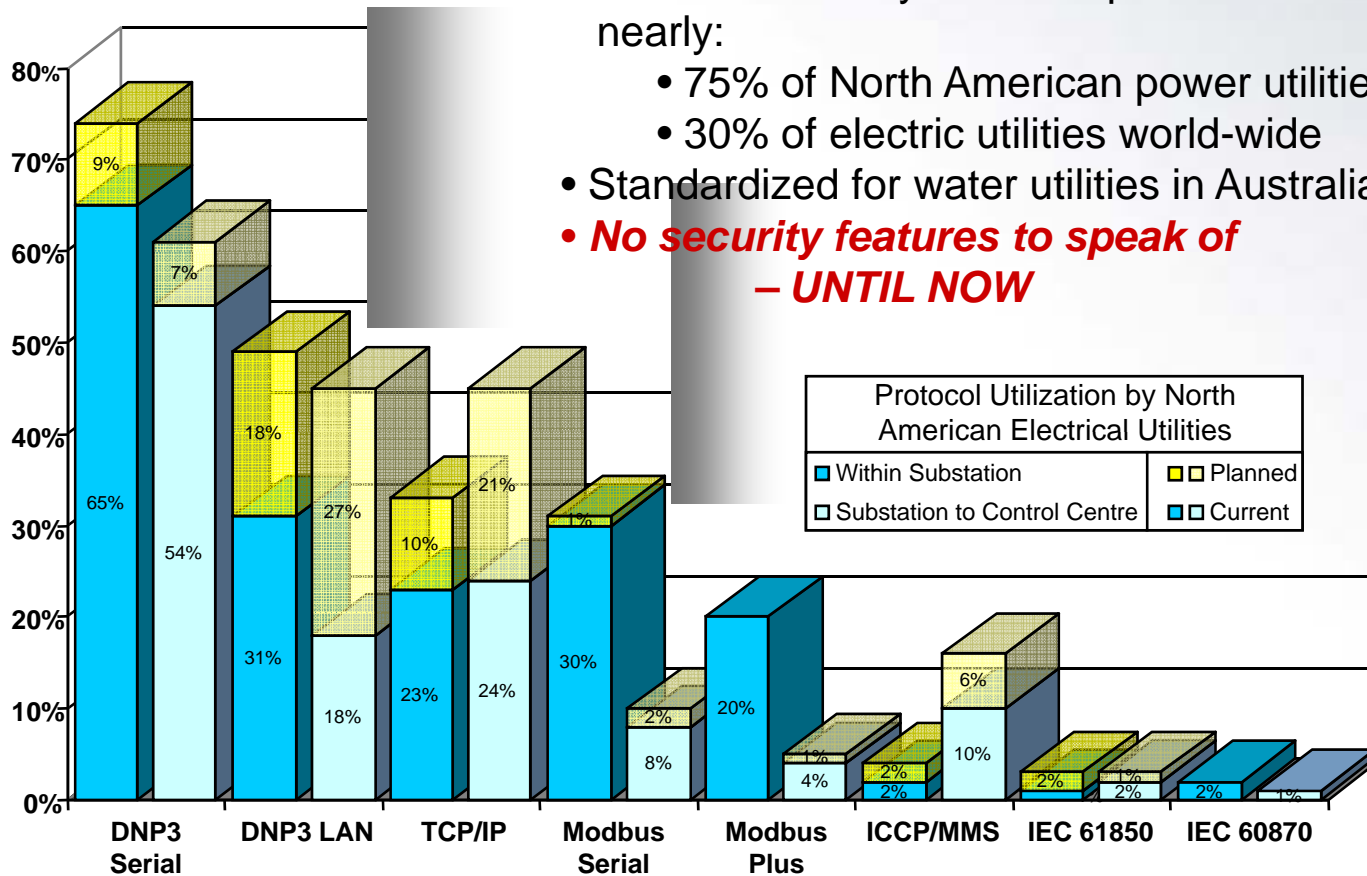
# Overview

- Security concepts
- DNP Security, overview and how it works
- Current state of Secure DNP
- How to use Secure DNP



# DNP3

- One of the most popular SCADA protocols
- DNP3 is currently in use or planned for use in nearly:
  - 75% of North American power utilities
  - 30% of electric utilities world-wide
- Standardized for water utilities in Australia, UK
- **No security features to speak of – UNTIL NOW**



Source: Newton-Evans Research 2005

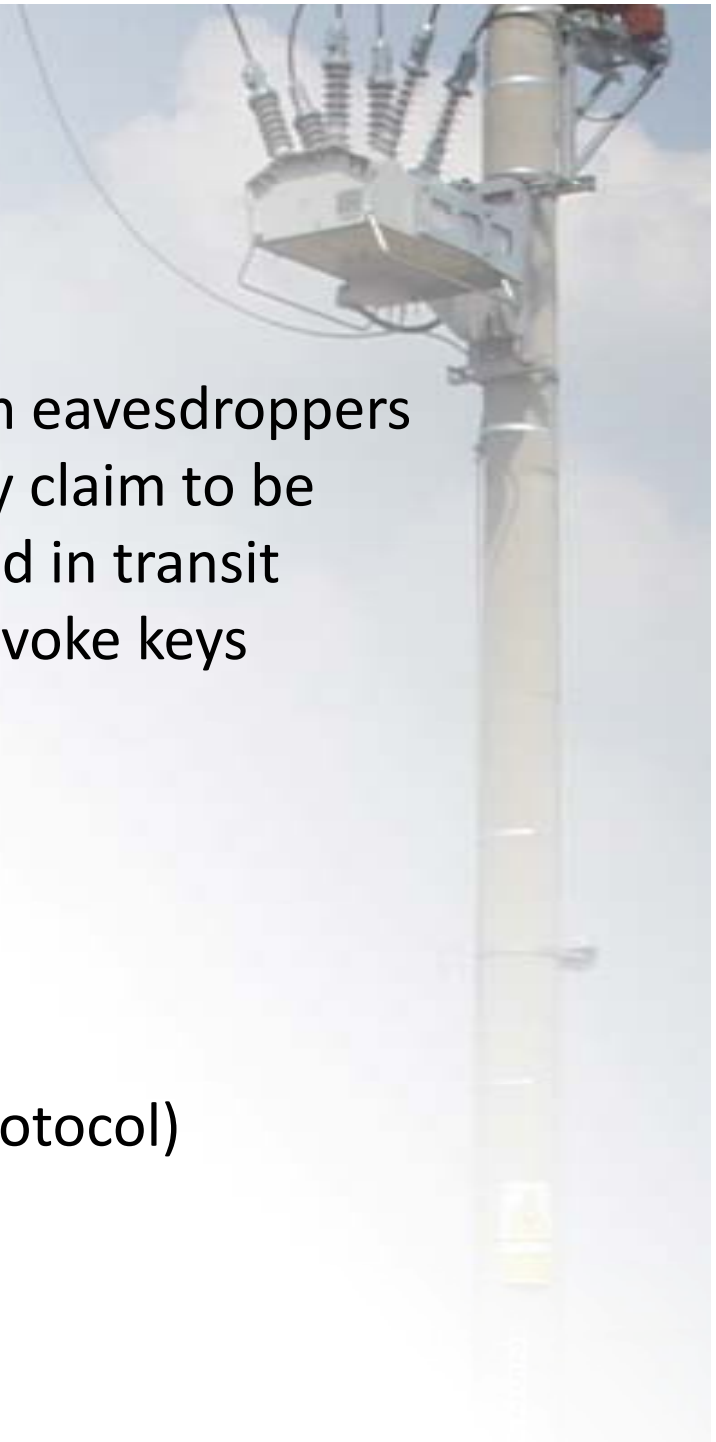
# 'Why' Security

- Threats / Risks  
Attackers, Bot-network operators,  
Criminal groups, Foreign intelligence services,  
Insiders, Phishers, Spyware/malware authors,  
Terrorists, Industrial Spies
- Typical Scenario  
Remote device operated over an unsecure and  
restricted capacity comms channel
- Regulation
  - NERC CIPs (Voluntary for now, Compliance Required  
by 2010)
  - NIST SP800-82



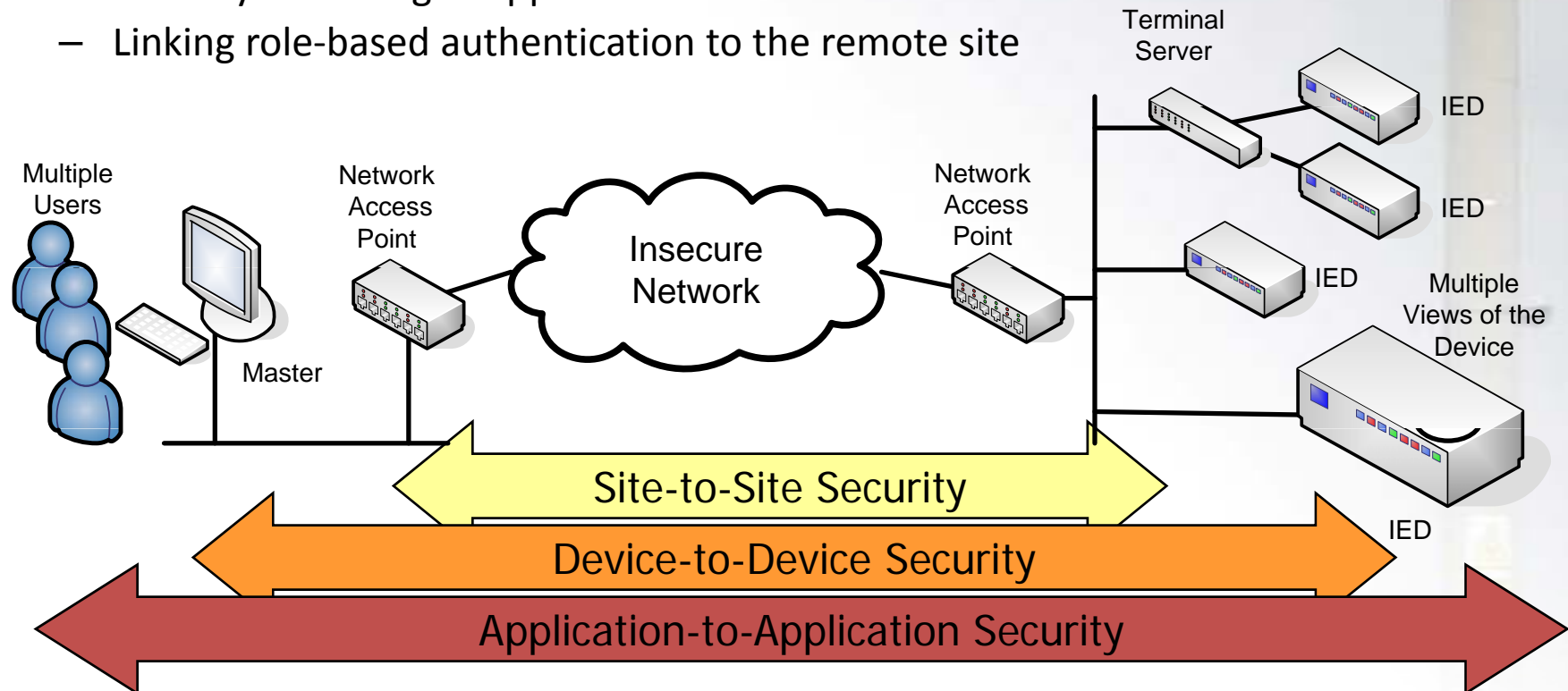
# Security Overview

- Security Technologies
  - Privacy (Encryption) – Hide data from eavesdroppers
  - Authentication – Parties are who they claim to be
  - Integrity – Data has not been changed in transit
  - Key Management – Distribute and revoke keys
- Types of network
  - Ratable (TCP/IP)
  - Serial Point to Point or Multi-drop
- Types of security implementation
  - Bump-in-the-wire (External devices)
  - Bump-in-the-stack (Integral to the protocol)

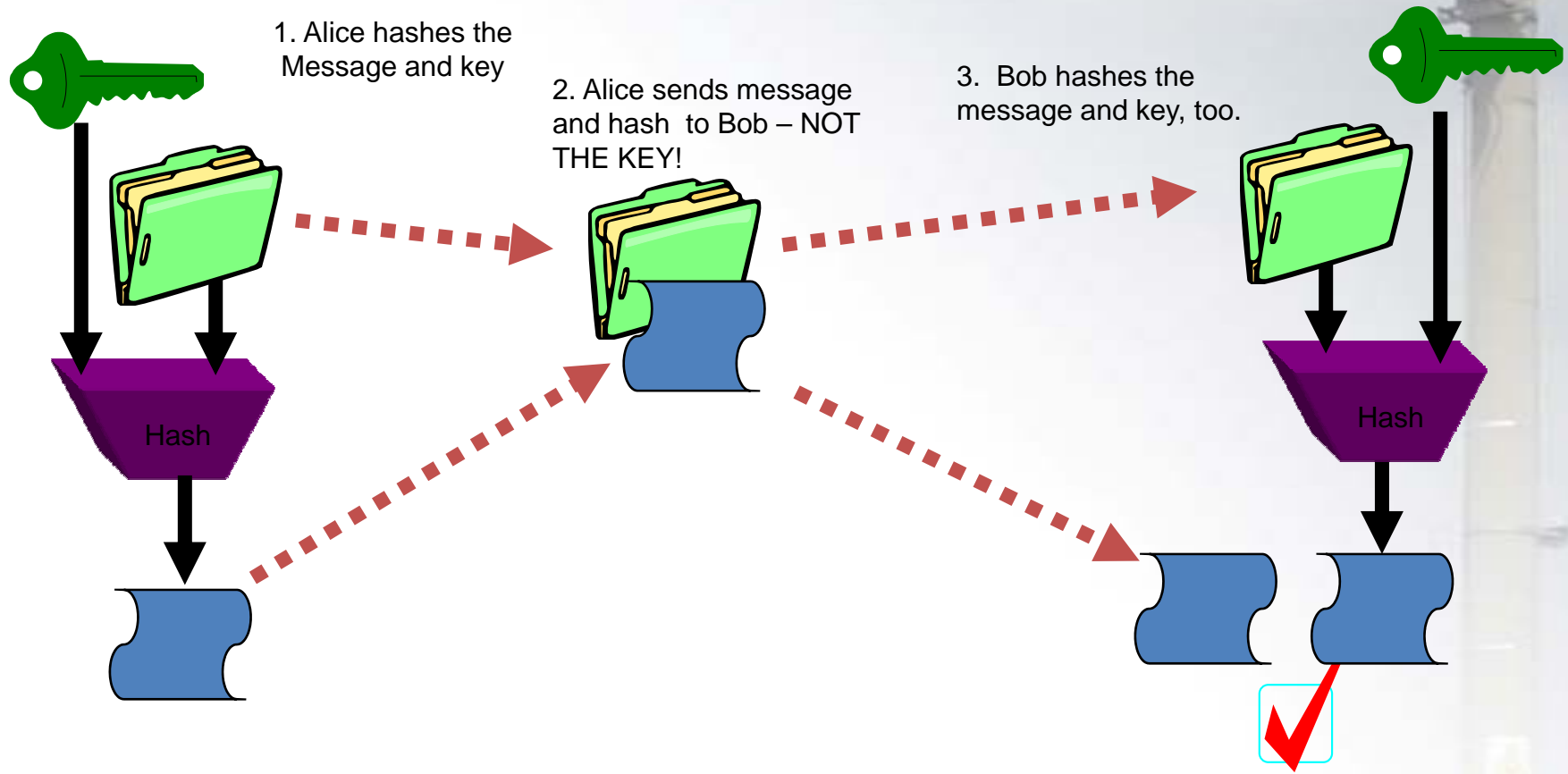


# Application Layer Security

- VPN Routers, link encryptors, etc. don't address:
  - Security at the local site
  - Security of serial DNP over unencrypted radios
  - Security of serial DNP over terminal servers
  - Security from “rogue applications” at master stations
  - Linking role-based authentication to the remote site



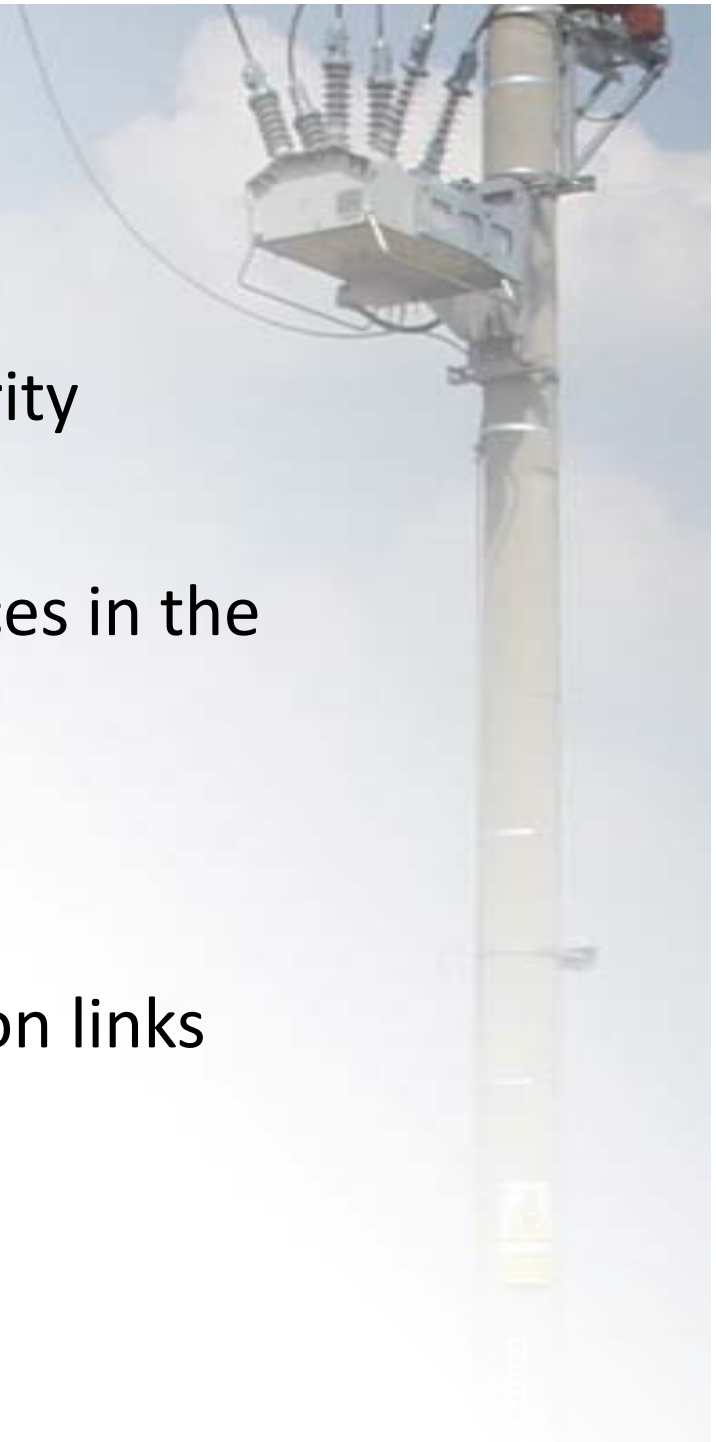
# Using a Hash to Authenticate



If Bob's hashed value matches Alice's, it has not been tampered with, and it must have been sent by Alice

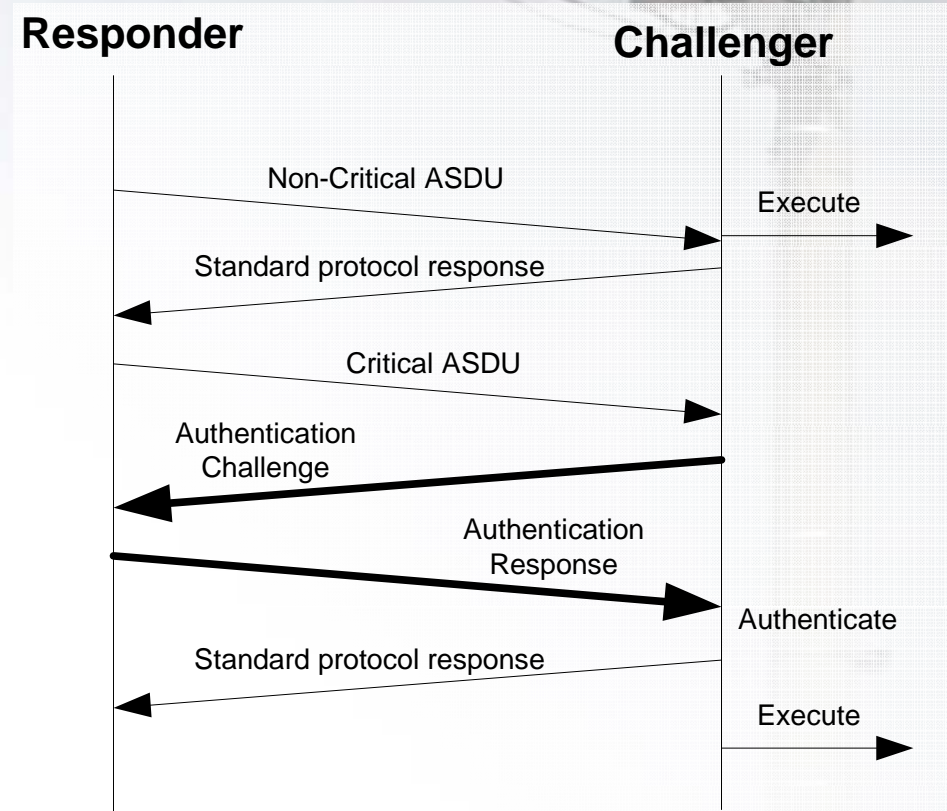
# Goals of DNP Security

- Provide Authentication and Integrity
- Low overhead
- Permit possibility of Privacy services in the future
- Support remote key management
- Built into DNP at application layer
- Compatible with all communication links supported by DNP
- Make use of existing standards



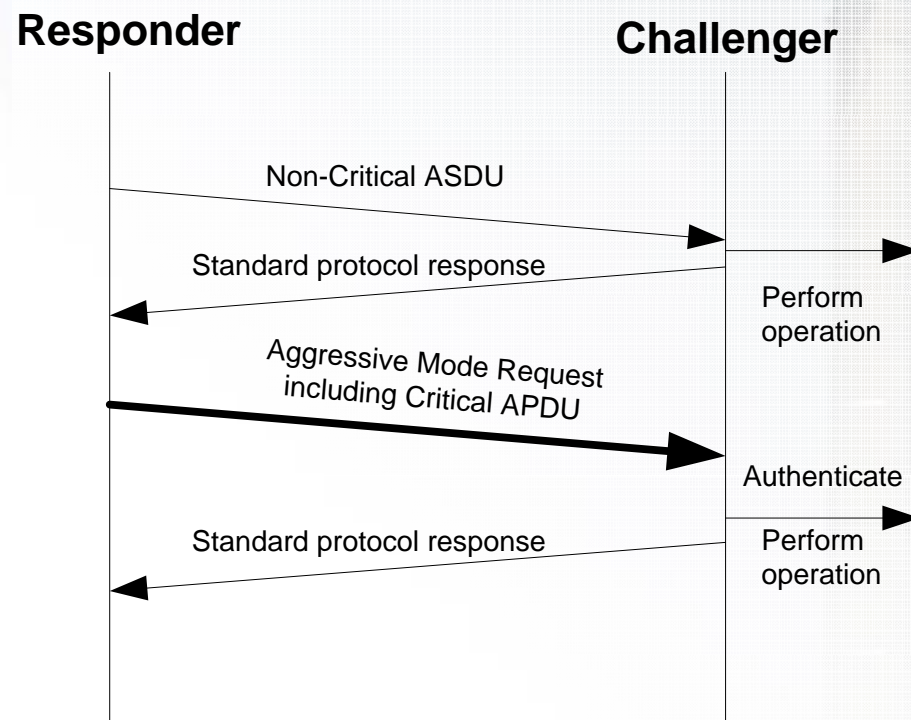
# Challenge - Response

- Either end can challenge
  - At initialization
  - Periodically
  - A critical function
- DNP defines which functions are considered “critical”
- Challenge contains:
  - Pseudo-random data
  - Sequence number
  - Required algorithm
- Response contains:
  - Hash (*HMAC*) value based on the challenge and the key
  - Sequence number



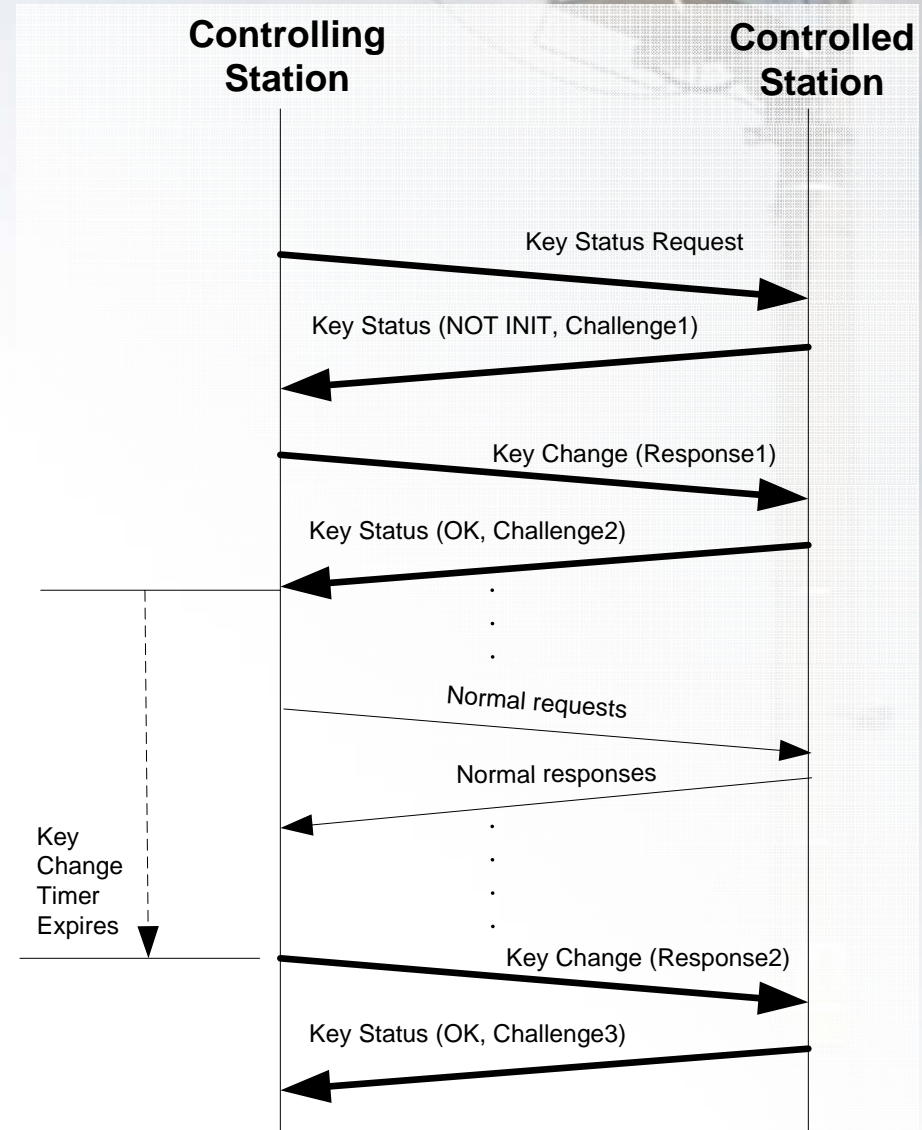
# “Aggressive mode”

- Can include authentication data at the end of the DNP message
- Slightly less secure
- Uses much less bandwidth
- Requires a formal challenge-response *first*



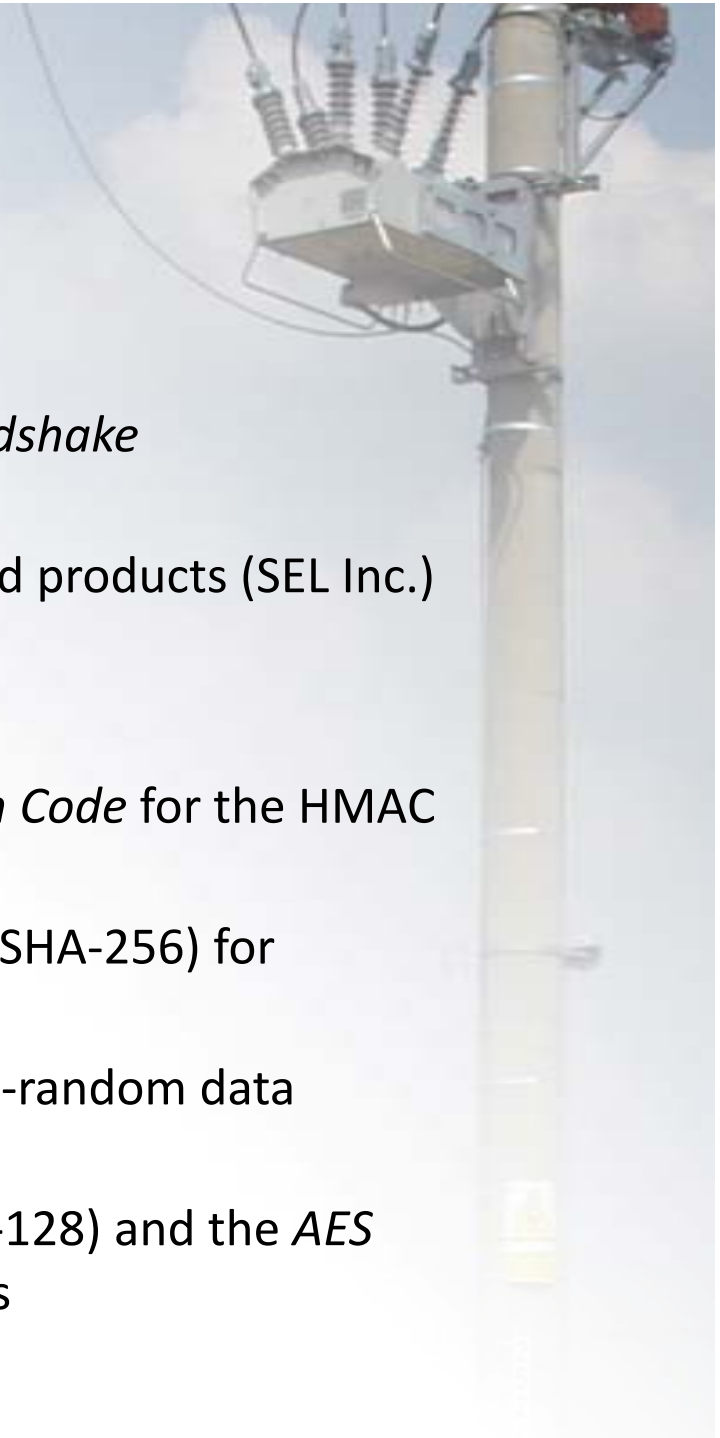
# Session Key Management

- Uses 128-bit keys minimum
- Two types of keys
- Session key (Temporary)
  - Initialized on start-up
  - Changed every 10 minutes or so
- Update key
  - Used to encrypt session keys
  - Pre-shared
- Keys encrypted using Advanced Encryption Standard (AES) “key wrap”
- Key change incorporates challenge-response



# Referenced Standards

- Proven techniques
  - Challenge-Response from the *Challenge-Handshake Authentication Protocol* (RFC 1994)
  - Key management from existing NIST-approved products (SEL Inc.)
- Proven algorithms:
  - FIPS 198 *Keyed-Hash Message Authentication Code* for the HMAC algorithm
  - FIPS 180-2 *Secure Hash Standard* (SHA-1 and SHA-256) for hashing
  - FIPS 186-2 *Digital Signature Standard* pseudo-random data generation algorithm
  - FIPS 197 *Advanced Encryption Standard* (AES-128) and the *AES Key Wrap Algorithm* to distribute session keys



# DNP Security - Status

As of November 2007:

- Security protocol finalized
- Will be submitted to Users Group in Jan 08
- There are existing implementations
- Looking for pilot sites
- Under evaluation by security labs for official recognition (e.g. NIST)
- Future work:
  - Extend protocol to support remote distribution of update keys
  - Add privacy



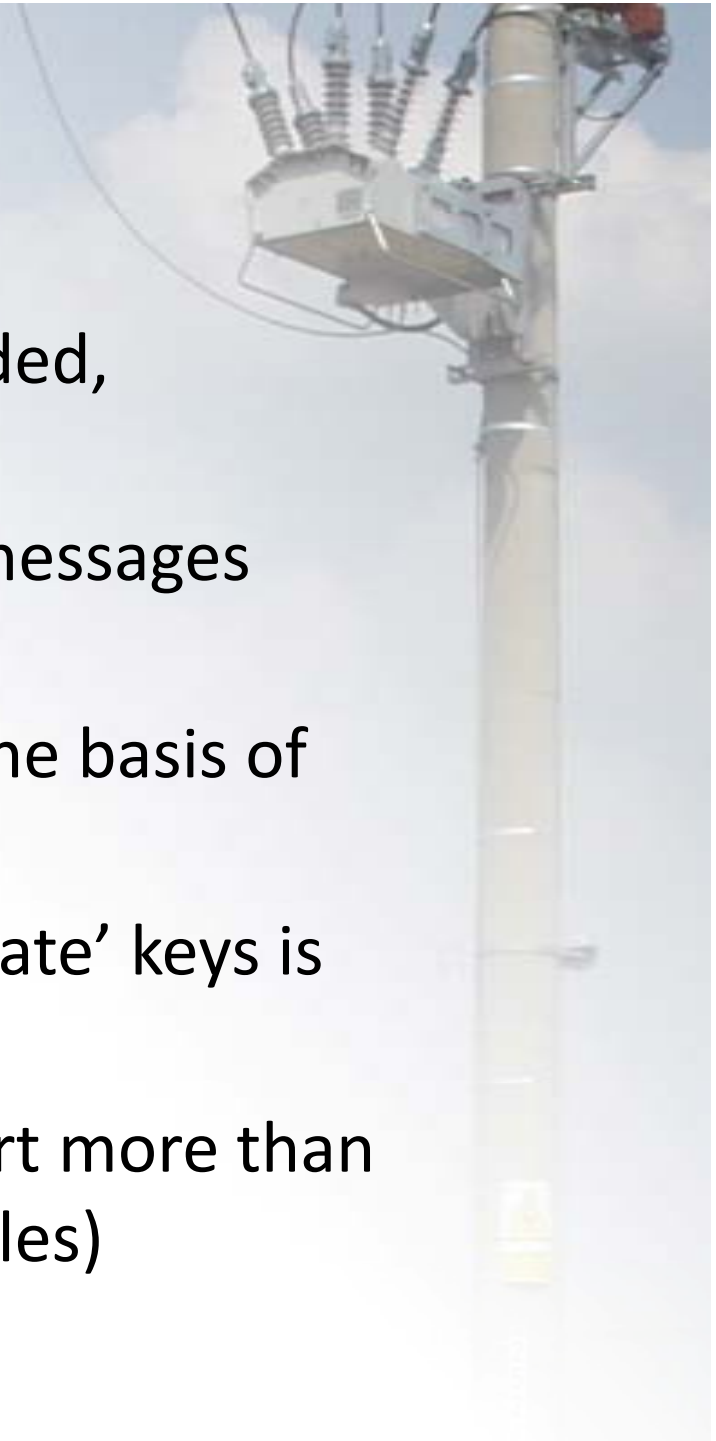
# Using Secure DNP

- There is no such thing as off the shelf security
- Consider within context of overall security plan
  - What is being protected
  - Defined security boundaries
  - Existing security policies and procedures
  - Remember the human factor



# DNP Security Model

- Authentication / Integrity is provided, Encryption is NOT
- The relying party chooses which messages require authentication
- Authentication is established on the basis of pre-shared 'update' keys.
- Distribution/Management of 'update' keys is not defined (yet)
- Outstations may optionally support more than one update key (multiple users/roles)



# Summary

- Security is increasingly becoming an issue
- Secure DNP protocol:
  - Provides authentication and integrity
  - Minimal overhead
  - Backwards compatible
- Implementations are becoming available

