

DNP REVOLUTION: **Past, Present and Future**

Security for DNP3

Grant Gilchrist, P. Eng.
EnerNex Corporation
DistribuTECH 2006

Agenda

- **Background: Types of Security**
- **Goals for DNP3 Security**
- **The IEC Working Group on Security**
- **The IEC 62351-5 Standard**
- **Implementing IEC 62351-5 in DNP3**
- **What's Next?**

Background: Types of Security

Main areas of security technology:

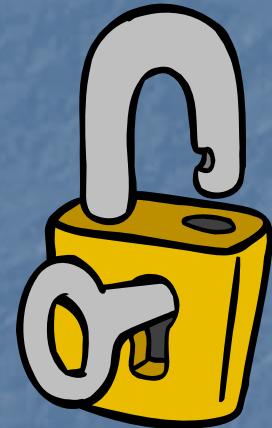
- **Authentication** – prove who you say you are
- **Integrity** – ensure the data hasn't been tampered with
- **Encryption** – hide data from eavesdroppers
- **Key Management** – distribute and revoke keys

Two different areas of application for DNP3

- **Serial links** – RS232, RS485, radio, dial-up
- **Networking** – Internet Protocols LANs/WANs

Different ways to do it:

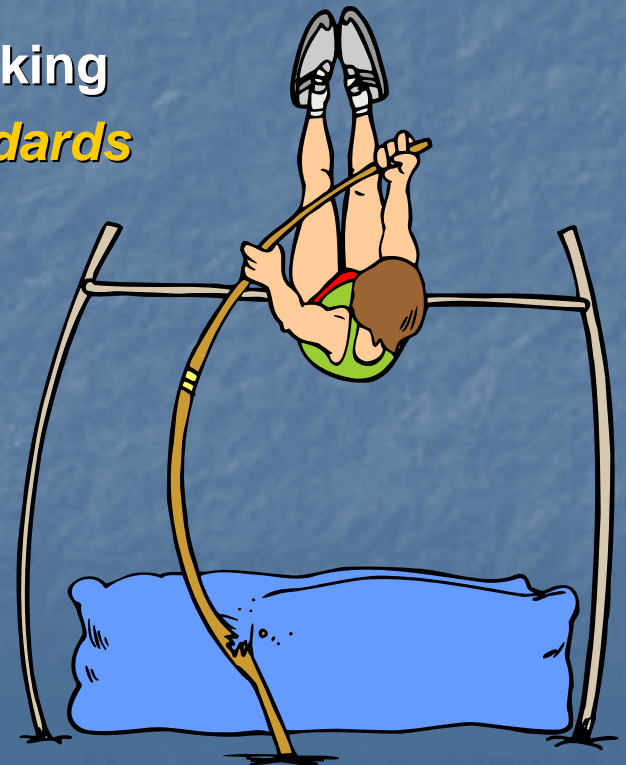
- **Externally** – in a separate device (“bump in the wire”)
- **Internally** – as a part of the protocol itself



Goals for DNP3 Security

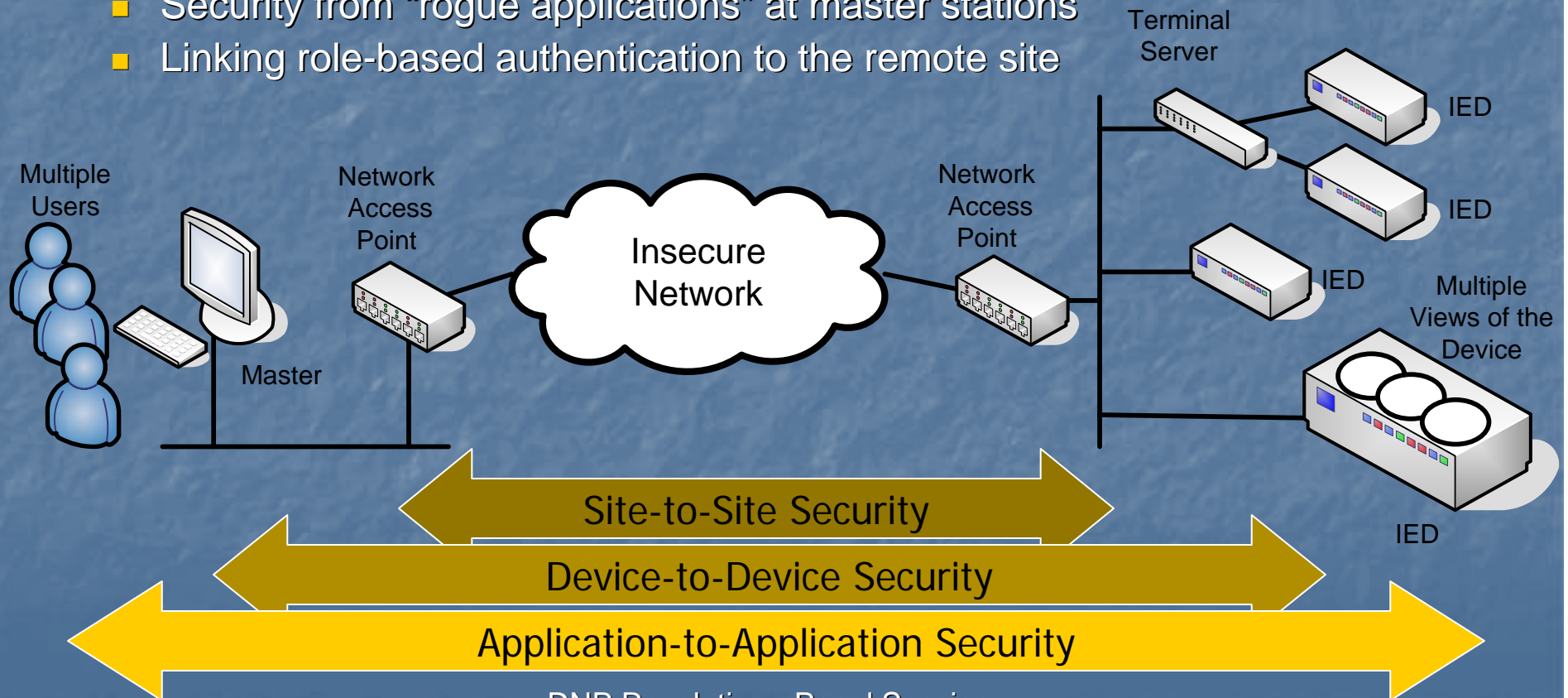
- Provide **authentication** and **integrity** at a minimum
- Leave open the possibility of encryption later
- **Remote key management** is a necessity
- Build it into the DNP **application layer**
- Ensure it's compatible with TCP/IP networking
- Make use of existing and developing **standards**

Build the DNP solution on the emerging
IEC 62351 standard!



Why 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

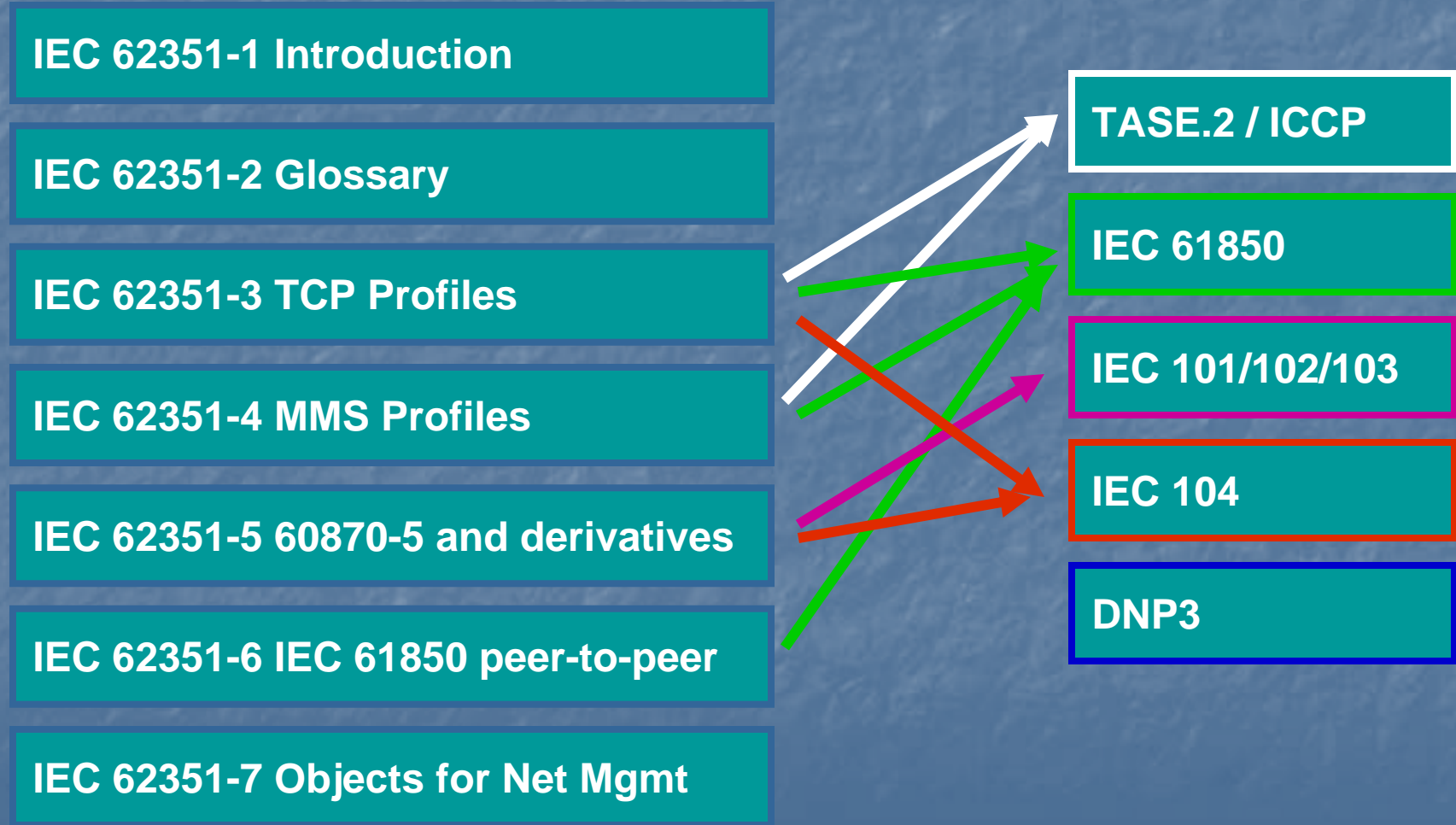


IEC TC57 Working Group 15

- Created to develop security solutions for all TC57 protocols:
 - IEC 60870-6 (TASE.2/ICCP)
 - IEC 60870-5-101,102, 103, 104
 - IEC 61850 (formerly UCA)
 - IEC 61968/61970 Common Information Model (was CCAPI)
- Must collaborate with other working groups to do so
- Scope has been also increased to address security policy and process in the industry
- Several work items approved in 2004
- Due to be finished by end of 2006 or early 2007



IEC 62351 Security Standards



IEC 62351 Can Apply to DNP3

IEC 62351-1 Introduction

IEC 62351-2 Glossary

IEC 62351-3 TCP Profiles

IEC 62351-4 MMS Profiles

IEC 62351-5 60870-5 and derivatives

IEC 62351-6 IEC 61850 peer-to-peer

IEC 62351-7 Objects for Net Mgmt

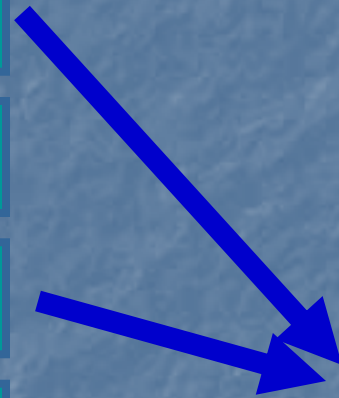
TASE.2 / ICCP

IEC 61850

IEC 101/102/103

IEC 104

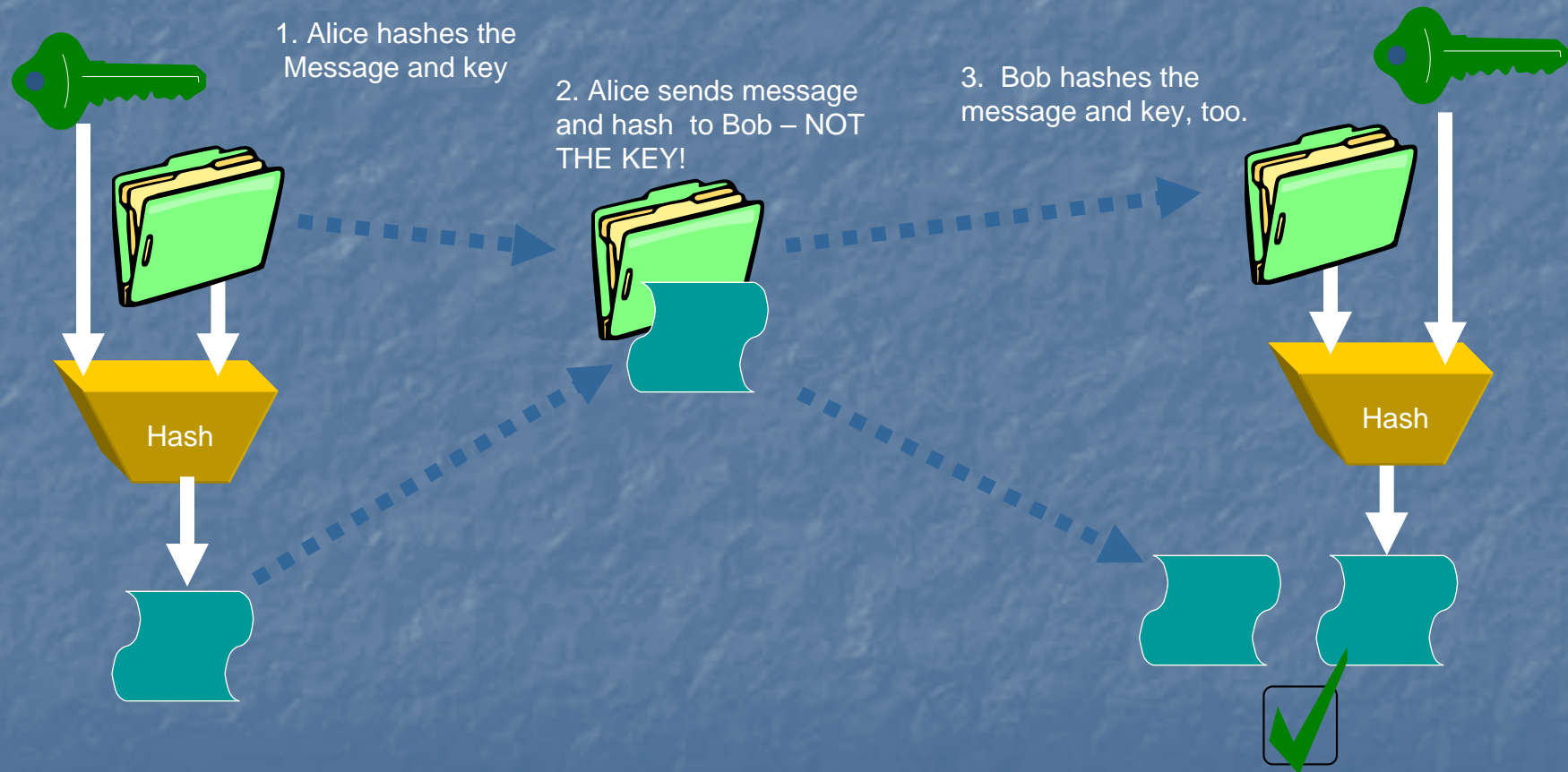
DNP3



Applying IEC 62351-5

- The standard defines a “*generic*” protocol
 - Message formats
 - State machines
 - Key lengths
 - Timers
 - Configurable parameters
 - Options
- DNP3 and the IEC 60870-5 protocols will define a “*mapping*”
 - Function codes and Objects to carry the generic messages
 - Default values and options
 - Interaction with the DNP3 or IEC 60870-5 protocol

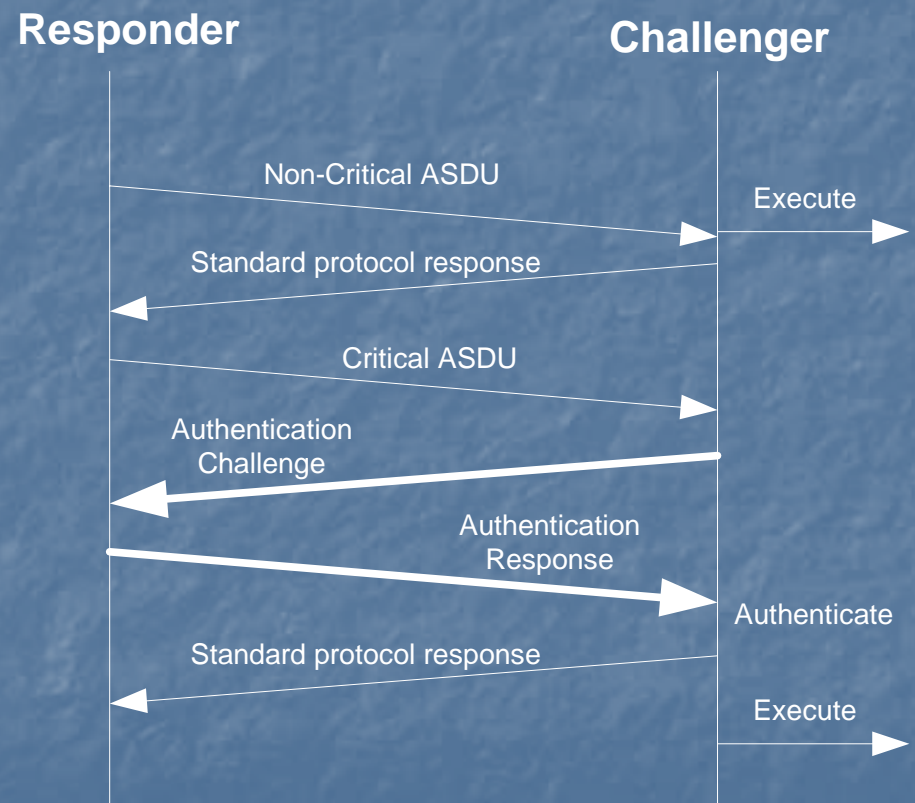
Using a Hash to Authenticate



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

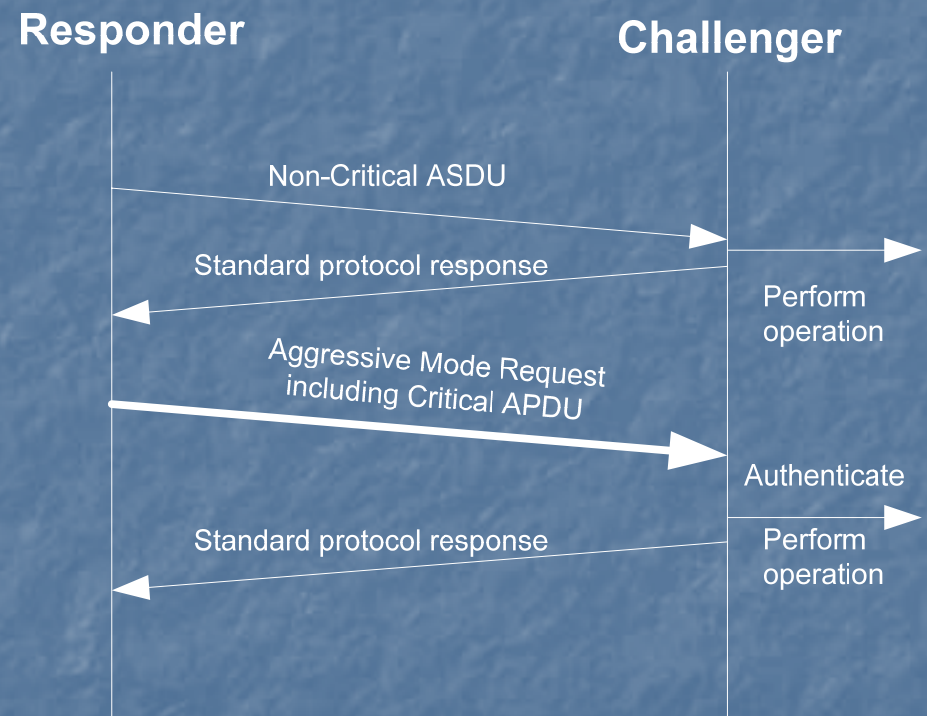
Challenge-Response

- 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



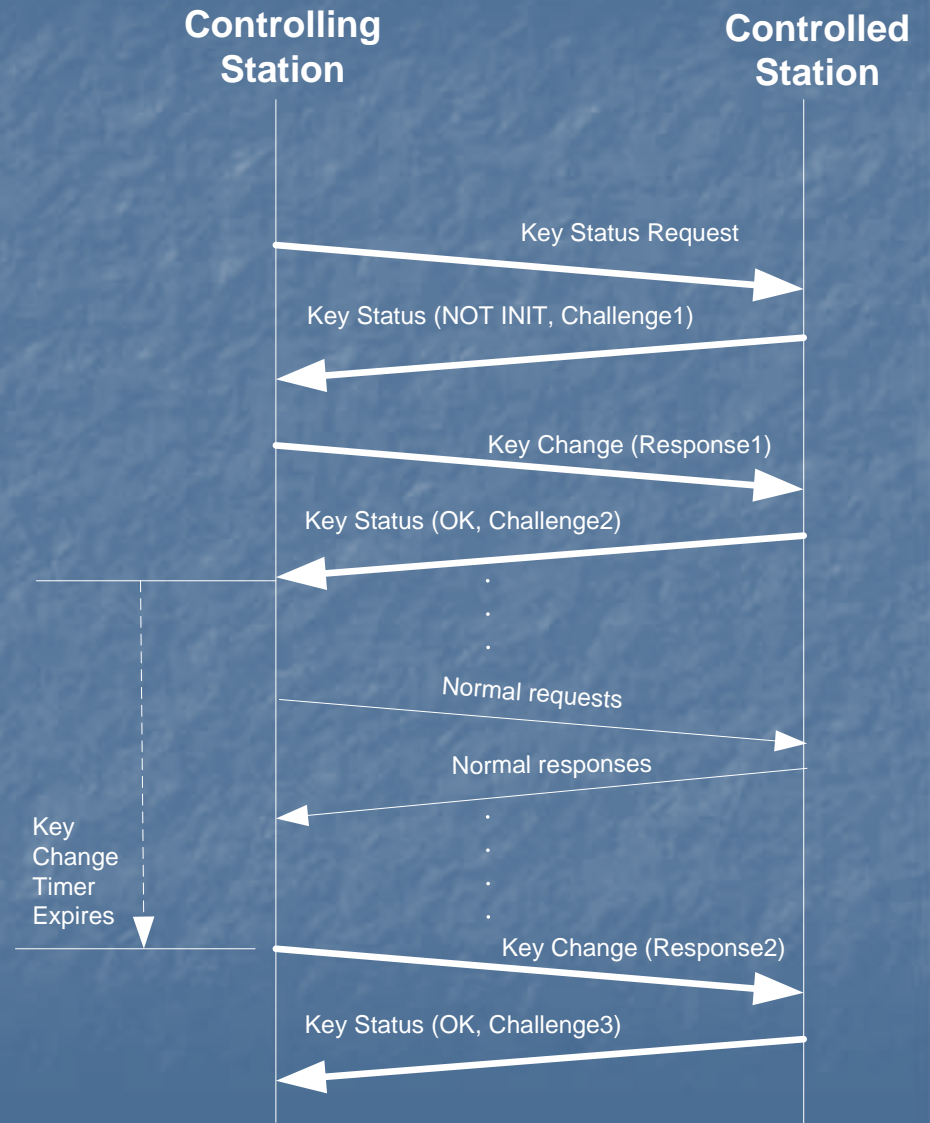
“Aggressive Mode”

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



Key management

- Uses 128-bit keys minimum
- Two types of keys
- Session key
 - 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



Implementing IEC 62351-5 in DNP3

IEC 62351-5 Message	DNP Function Code	DNP Obj	DNP Var	DNP Name
Challenge	0x81 Response 0x82 Unsolicited Response	120	1	Authentication Challenge Object
Response	0x21 Authentication Reply	120	2	Authentication Reply Object
Aggressive Mode Request	As sent by master	120	3	Authentication Aggressive Mode Request Object
Key Status Request	0x22 Key Status Request	-	-	(none)
Key Status	0x81 Response	120	4	Key Status Object
Key Change	0x02 Write	120	5	Session Key Object

Next Steps

- IEC 62351-5 is in 2nd Committee Draft (2CD) stage
- Two more steps, *minimum* 3 months each:
 - Committee Draft for Vote (CDV)
 - Final Draft International Standard (FDIS)
 - International Standard (IS)
- Mapping to DNP3 is in front of the DNP Tech Committee
- Goal is to be completed by early 2007
- Pilot projects in the meantime?



References

Proven techniques

- Challenge-Response from the *Challenge-Handshake Authentication Protocol* (RFC)
- 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