

Setting the Standard for Automation™



Preliminary Results of Tests of Cryptographic Modules on Legacy SCADA Systems

EXPO 2005
Chicago, IL

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

This Is The Work Of Several People

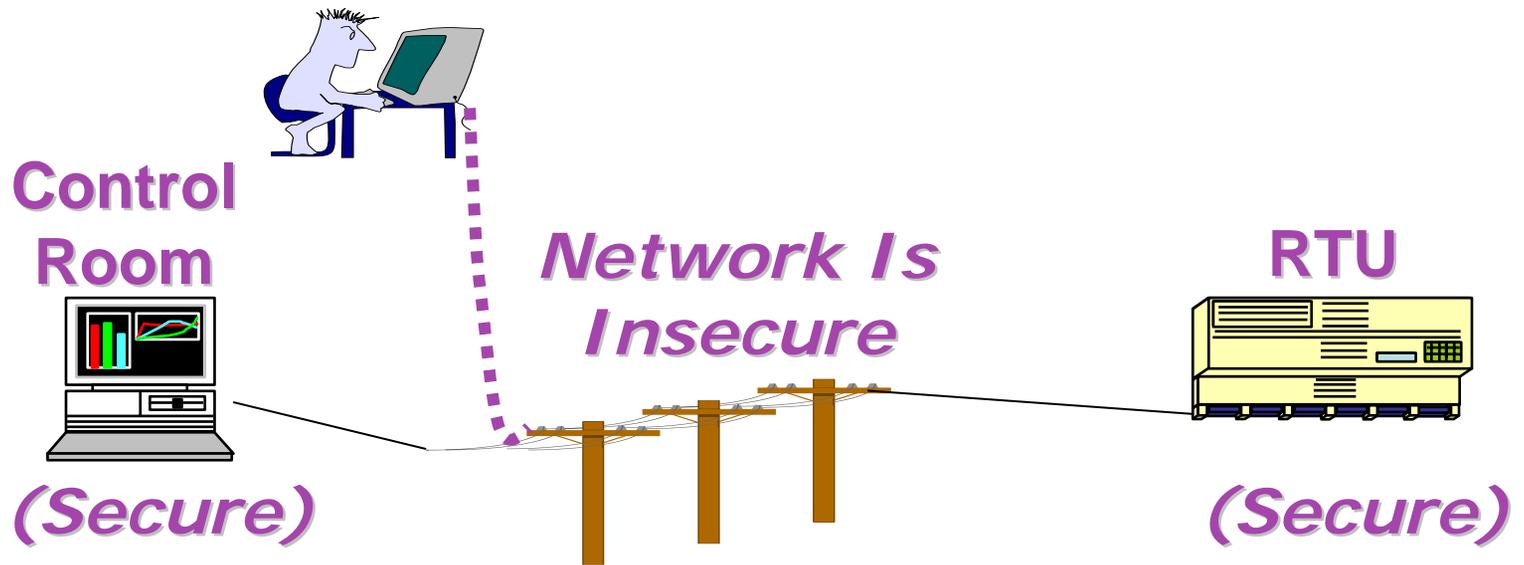
- **Bill Rush (GTI)**
 - Physicist At GTI Since 1978
 - Chair, American Gas Association Encryption Working Group
- **John Kinast (GTI)**
- **Aakash Shah (GTI)**
- **Andrew Wright (Cisco Systems)**

We Will Answer 6 Questions



- 1) **What Does AGA 12 Do For SCADA?**
- 2) **Does It Really Work?**
- 3) **Will It Slow Communications?**
- 4) **Is It Convenient?**
- 5) **Will It Be Expensive?**
- 6) **How Soon Can I Get It?**

AGA 12 Protects SCADA Communication Links



AGA 12 Also Secures RTU Maintenance Ports

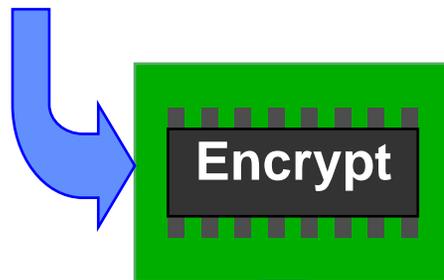
AGA 12 Is A Recommendation For Protecting SCADA Data

- **Protects Communications**
- **Assumes Secure Physical Facilities**
- **Actually, A Suite Of Reports**
- **AGA 12-1 Is Background, Policy, Tests**
- **AGA 12-2 Covers Retrofit Serial Links**
- **Will Develop Embedded & High Speed Recommendations Soon**

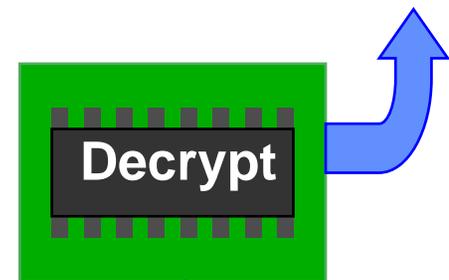
AGA 12 Protects SCADA By Encrypting Messages



“Open A Valve!”



“Open A Valve!”



“^fD%b*m>s#H!j“

***Even Intercepted SCADA Commands Are Secure
Until They Reach Their Destination***

AGA 12-2 Is Thought To Be Cryptographically Secure



- **“Secure” -> Only Brute Force Attacks Work**
- **Uses NIST Approved Algorithms**
- **Submitted To Cryptographic Community**
- **As “Sure As Practical”**
- **Better Bet Than Untested Systems**

Cryptography Raises Speed Concerns



- **Cryptography Takes Time**
- **Added Communication Overhead**
- **More Chance For Errors/Retries**

AGA 12 Includes A Test Program

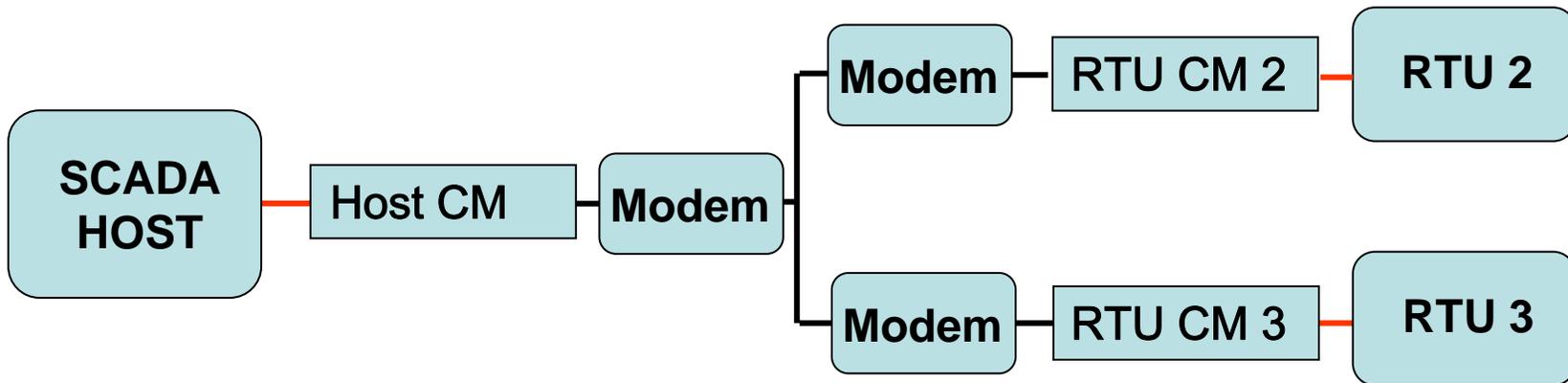


- **Basic Measures Are**
 - Message Throughput Rate
 - Timeouts
 - Message Errors (Corruption)
- **Many Other Tests Not Reported Here**

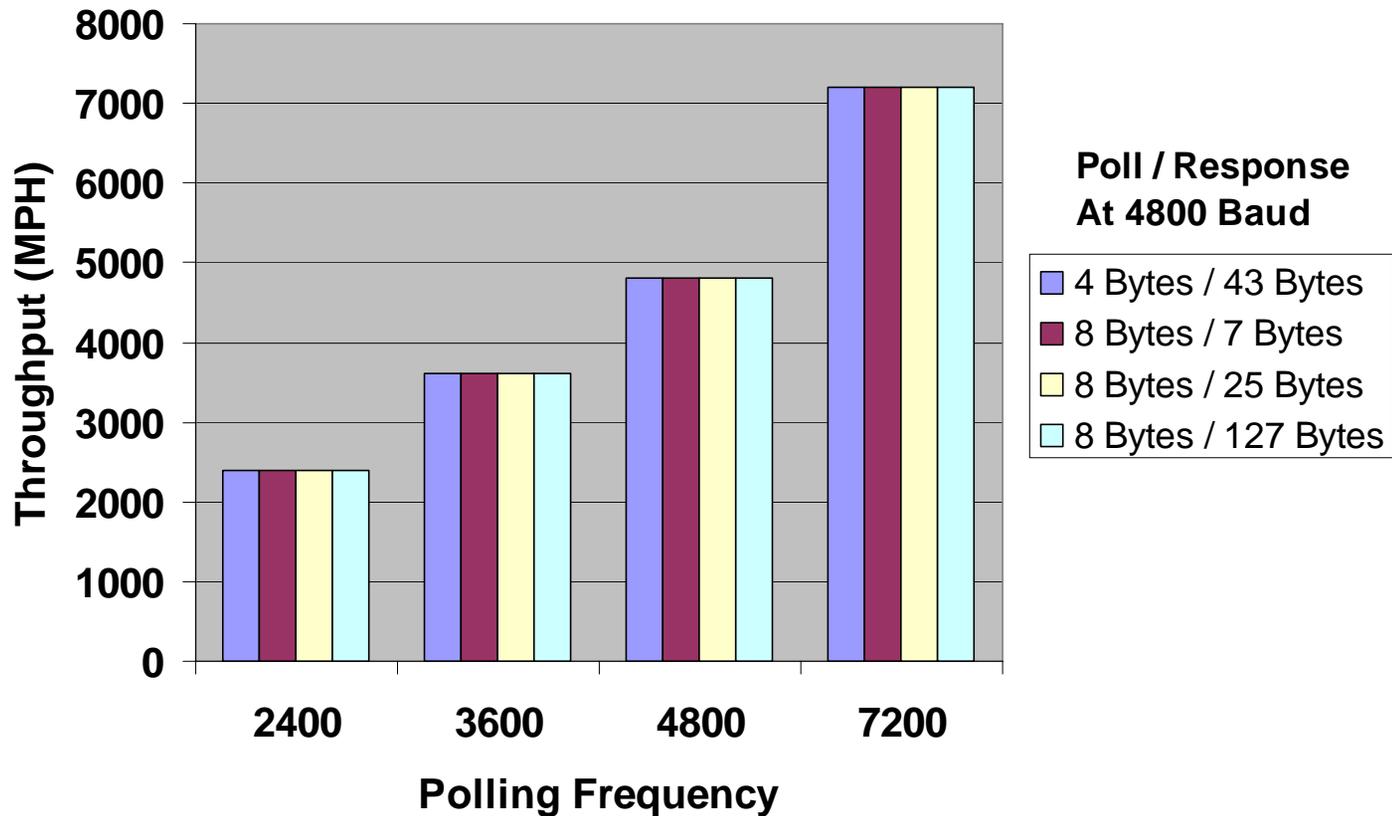
GTI Tested AGA 12 Modules In The Laboratory



- Measure Throughput, Timeouts, Errors
- With And Without Cryptography
- Measure Difference
- Tests At 4800 & 9600 Baud, Modbus
- Tested Mixed Mode And Broadcast



GTI Tested Different Sizes & Rates Of Messages w/o Crypto

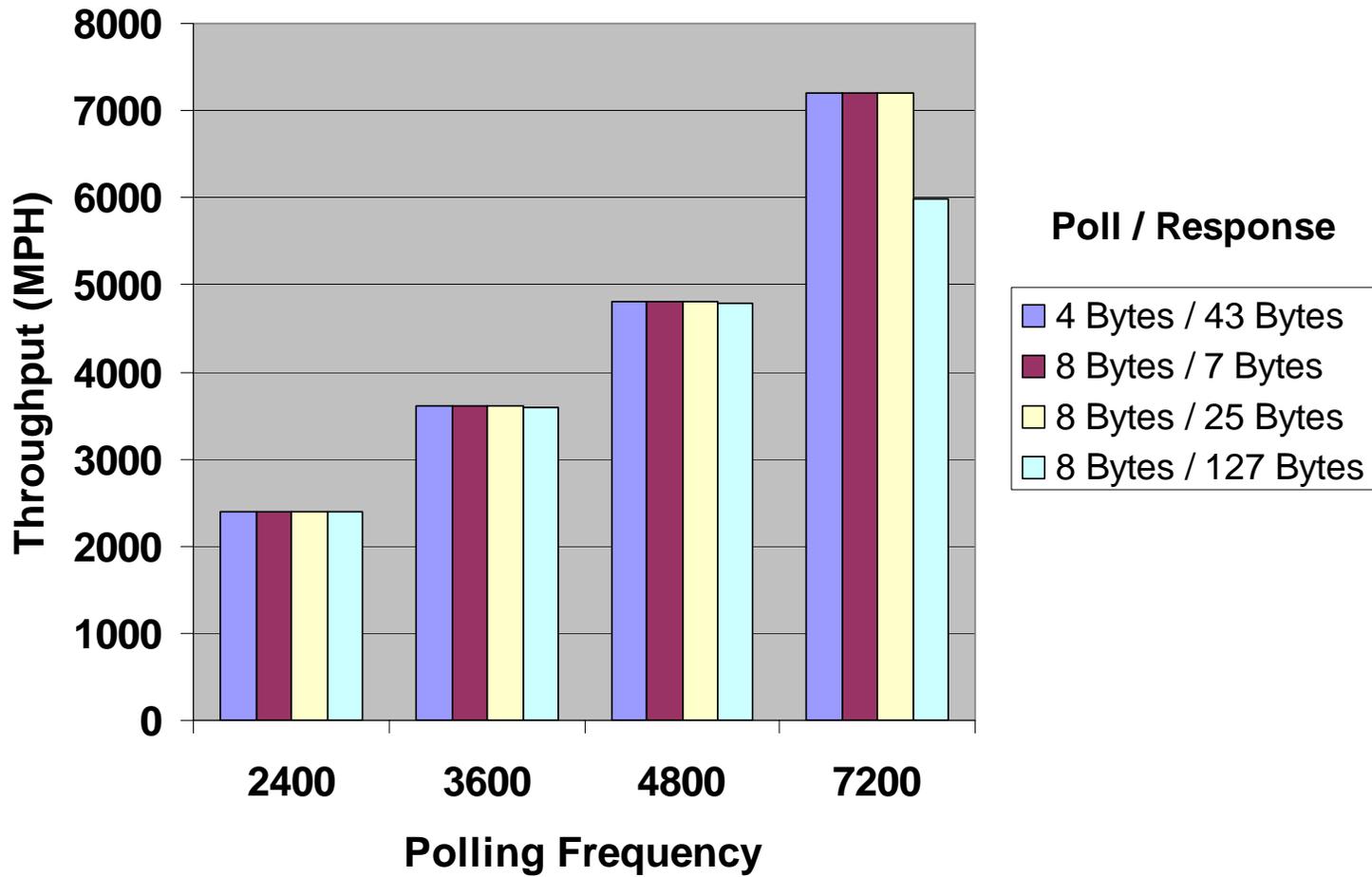


Without Crypto, Modbus Works As Expected

Errors And Timeouts Are Small At 4800 Baud

- **Errors From Corruption: Zero**
- **Minor Timeouts:**
 - Under 0.4% For 8 Byte Poll / 127 Byte Reply
 - Zero For All Other Messages Tested

At 4800 Baud, AGA 12 Hardly Affects Throughput



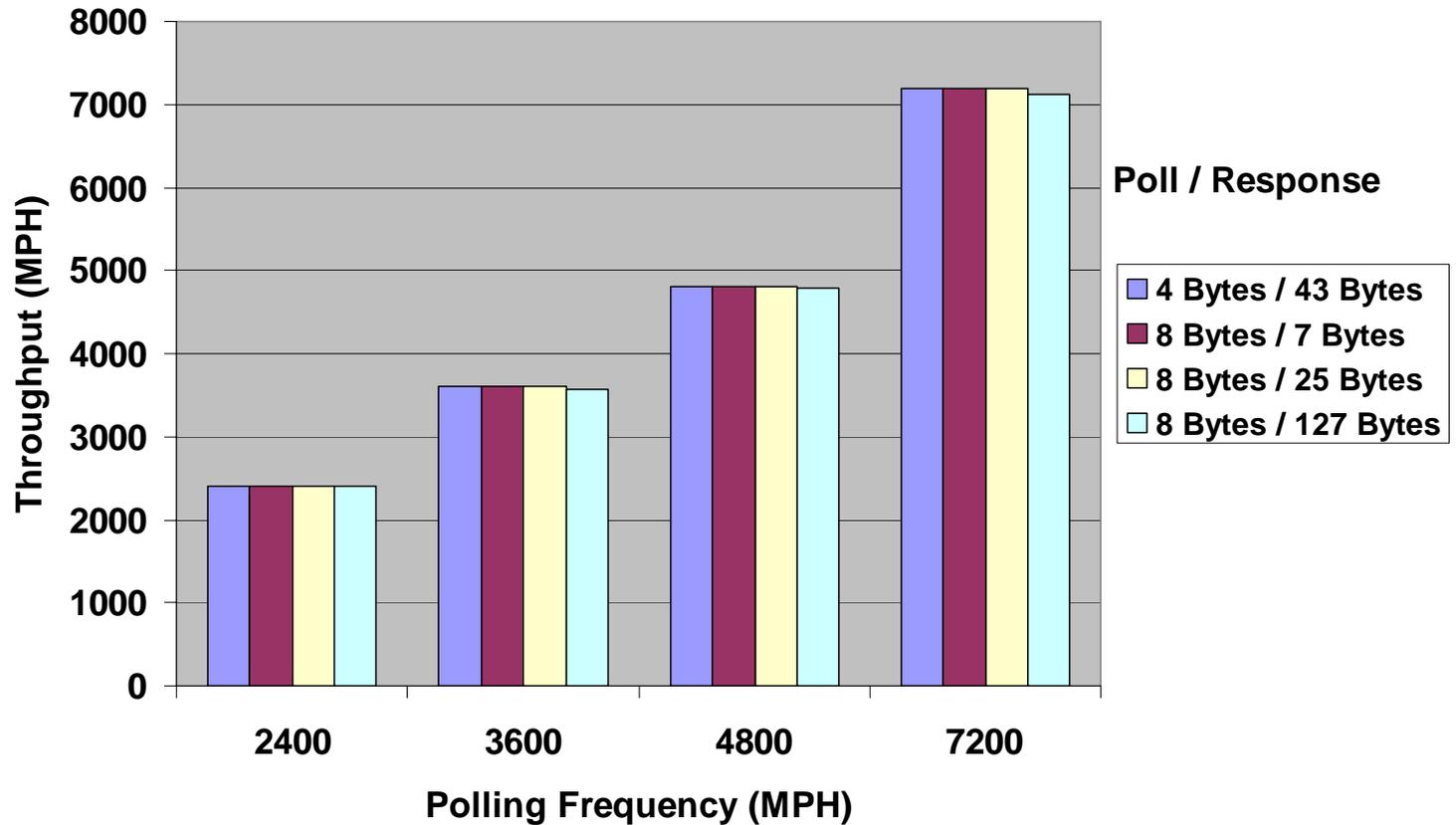
Drop 17% ONLY @ 7200 Polls/Hour

Errors And Timeouts Are Small At 9600 Baud



- **Errors From Corruption: Zero**
- **Minor Timeouts:**
 - Under 1.5% For 8 Byte Poll / 127 Byte Reply, 7200 Polls/Hour
 - Negligible For All Other Messages Tested

At 9600 Baud, Throughput Dropped Less Than 2%



AGA 12 Is Utility Friendly



- **Can Specify A Standard**
- **Interoperability (Limited)**
- **Plug In Retrofit Installation**
- **Retrofit Compatible With Embedded**
- **Reduce Negligence Risks**
- **No Known Back Doors**

- **ANYONE Can Build To AGA 12**
- **JAVA Code On Cisco Web Site**
- **Open Standard Fosters Competition**
- **Options For Product/Feature Competition**

AGA 12 Compliant Products Will Be Available Soon



- **Passed AGA 12 Balloting Procedures**
- **GTI Lab Tests Complete**
- **Now Entering Field Tests**
- **National Labs Testing**
 - Performance (PNNL)
 - Security (Sandia)
- **Manufacturers Producing Prototypes**

Use AGA 12 For Practical, Cryptographic Protection For SCADA Communications

- **Secure**
- **Fast**
- **Convenient**
- **Low Cost**
- **Available Soon**

AGA 12 Introduces Only Negligible Delays