Architectural Impacts And Net-Centric Opportunities Using Network-Based Crypto Devices

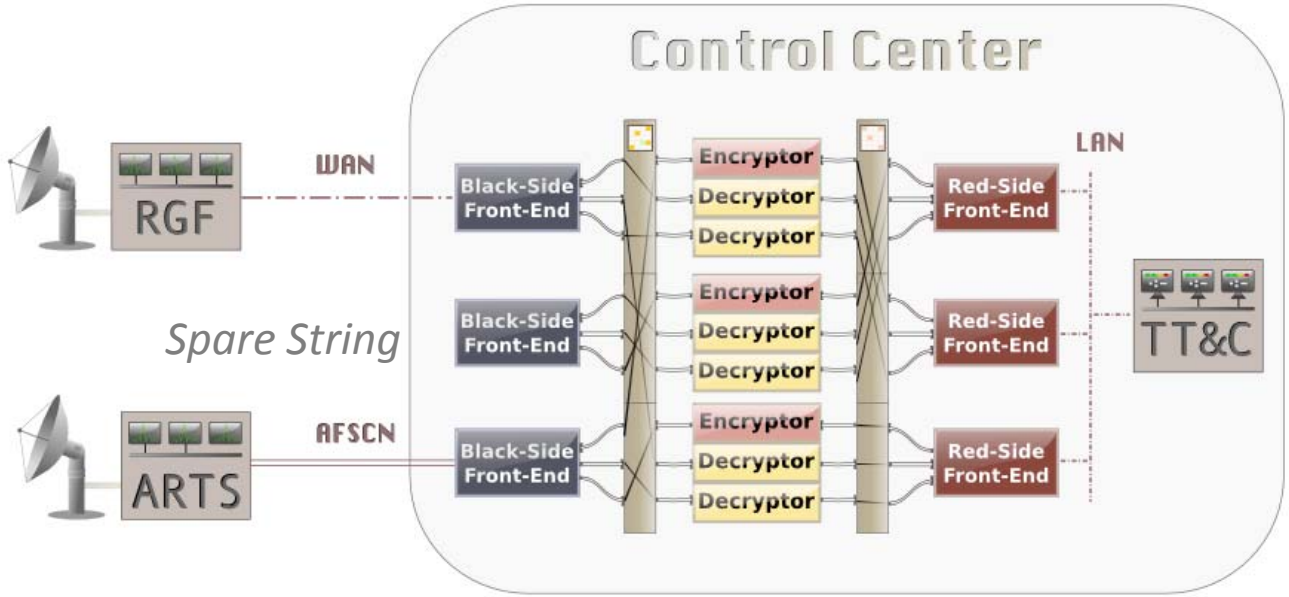
Rob Andzik
AMERGINT Technologies
GSAW 2010

Overview

- **A New Telemetry & Command Crypto: KS-252**
  - How will this impact ground system architectures?
  - What benefits might we realize?
- **Impact Of The Crypto On Current Architectures**
- **Implementation Opportunities Of The New Crypto**
- **Other Considerations**

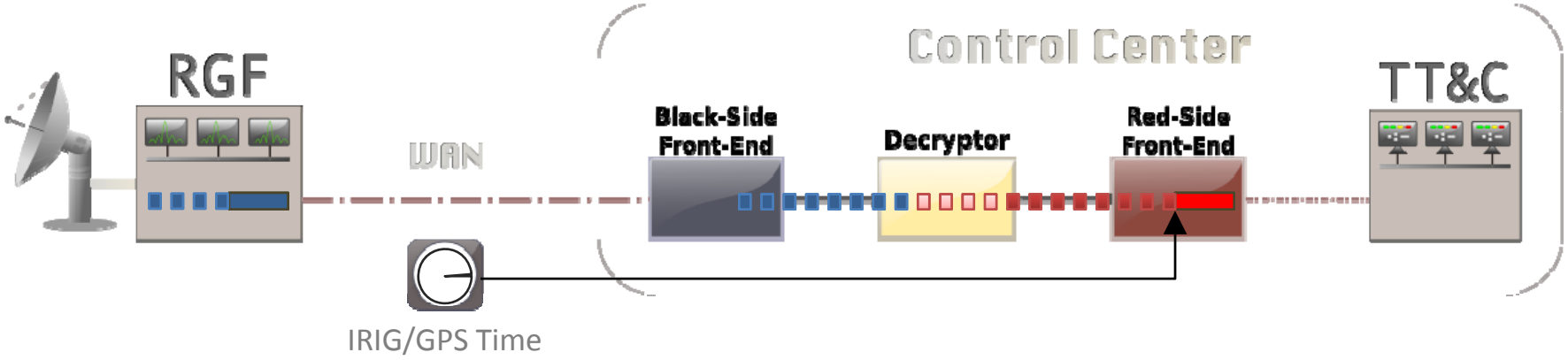
Current State Of Affairs

- **Control Centers Contain Numerous Cables and Devices**
- **The Interface With The Crypto Drives Much Of This Complexity**
- **Cost Impacts**
  - Unique Serial Protocols Prevent Use Of Commodity COTS Solutions
  - Complex & Expensive Software, Hardware & Cabling Required
  - Patch Panels & Switches Necessary For High Availability



How The Crypto Impacts CONOPS

- **Serial Data Transfer Is Inherently Deterministic**
  - Often A Requirement For Timestamps & Time-Critical Commanding
  - Timestamps & Time-Release Are Handled On The Red-Side
- **Combining Packet & Serial Communication Is Challenging**
  - Deterministic Timing Requires Added Latency At Several Points
    - Serial-To-Packet: Must Accumulate A Full Packet Before Transfer
    - Packet-To-Serial: Buffering Reduces Under Flows
  - Non-Deterministic Packet Transfers Impact Timestamps

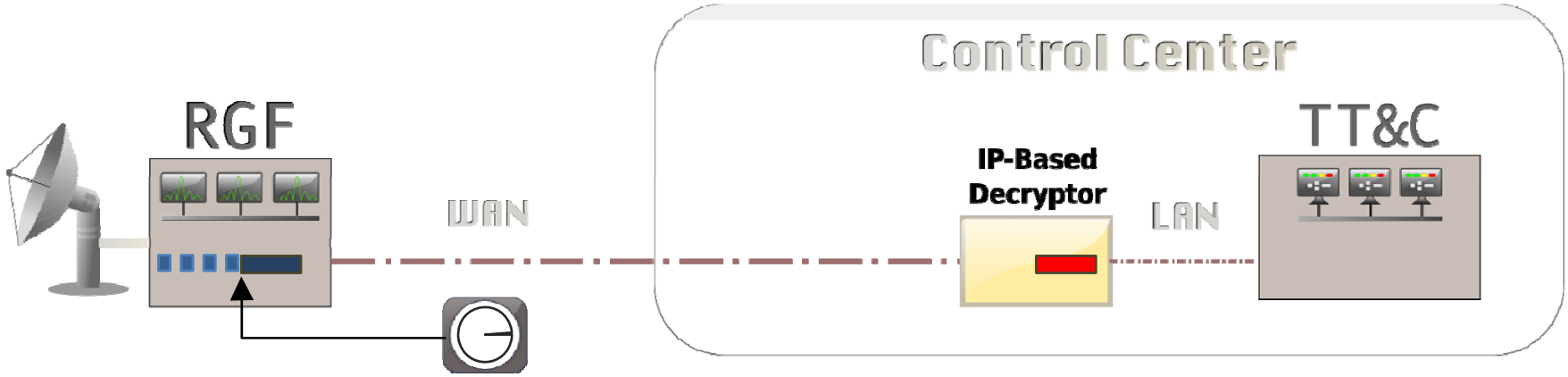


Impact Of A Crypto With Network I/O

- **What Happens If We Switch To A Packet-Based Crypto?**
  - Can We Remove The Complex Nest Of Cables And Devices?
  - Will The New Crypto Impact My CONOPS?
  - What Risks And Challenges Will My Program Face?
- **Enter The KS-252**
  - IP-Based Transfer Of Telemetry & Command Data
  - Support For Multiple Algorithms In A Single, One Rack Unit (1U) Box
  - Supports Both Encrypt/Decrypt and Web-Based Control & Status
- **How Can We Take Advantage Of This?**
  - Potential For Significant Cost Savings!
    - The Crypto Itself Is Less Than 50% The Cost
    - Dramatic Reduction In Cabling & Hardware Complexity
    - Sparing & Pooling Become Practical And Cost Effective
  - Potential For A Net-Centric Ground System Architecture
    - Network-based Switching & Routing
    - Eliminates Much Of The Need For Specialized Hardware
    - The Crypto Could Become A ‘Service On The Network’

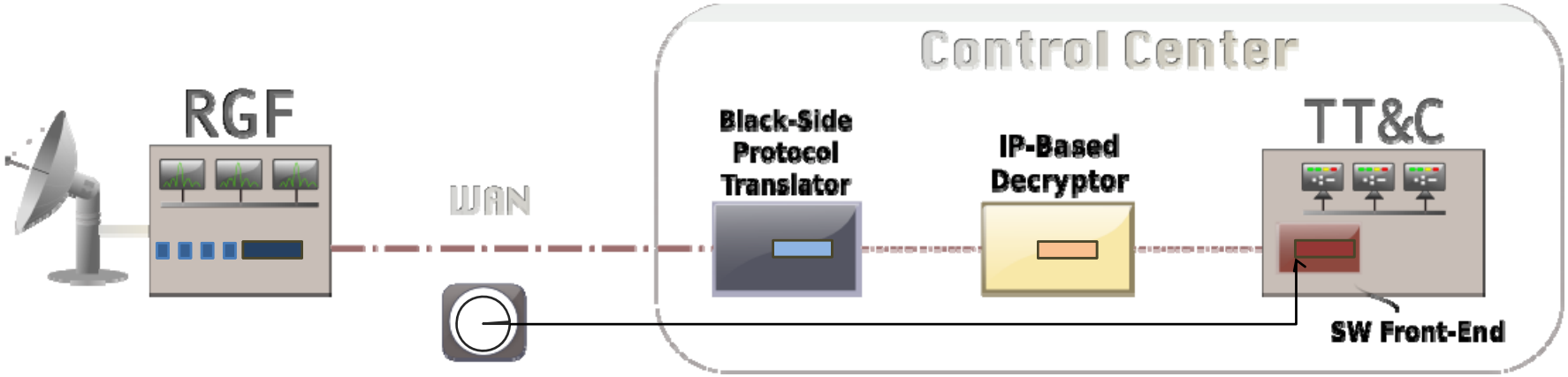
Packet Processing In A Perfect World

- **IP-Based Crypto Dramatically Simplifies The Architecture**
  - All Interfaces Are Ethernet
  - Actual Data Rate Only Impacts Latency At The RGF
  - Ideally We Would Have:
    - The Modem (Or Space Vehicle) Apply Timestamps To The Packets
    - Timestamps Travel With The Packets Through The Crypto
    - No Need For Custom Front-End Hardware
    - Frame Synchronization & Command Processing Move To Software

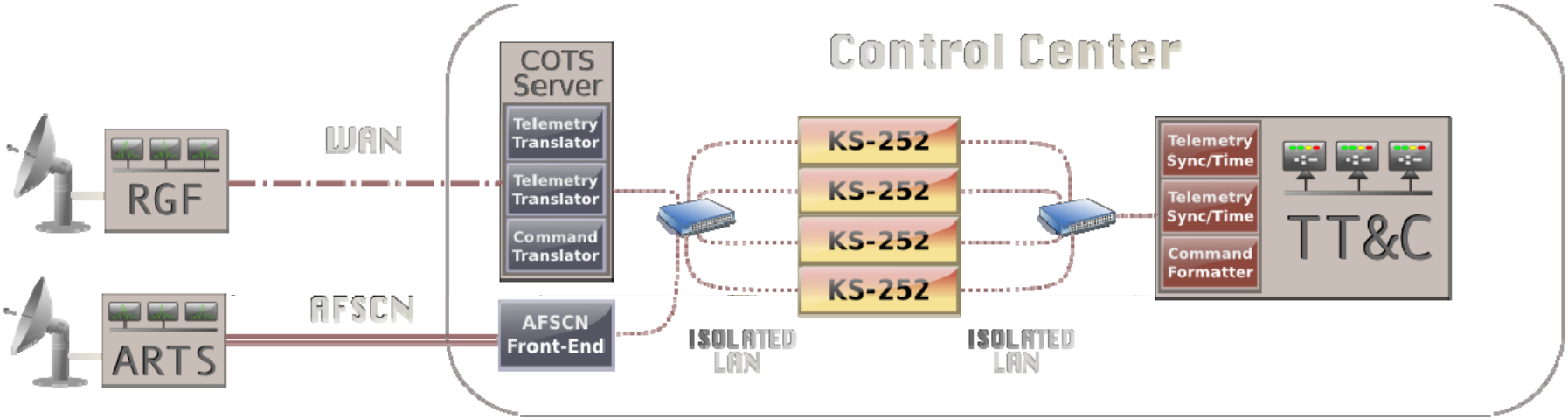


Now For A Dose Of Reality

- **TLM/CMD Requirements Allocated To Front-Ends Still Exist**
  - Synchronization, Barker Codes, Command Spacing, etc.
  - The KS-252 Does Not Pass Timestamps Through With The Packets
- **We Must Also Consider The Impact Of The Network**
  - WAN Jitter Can Vary Packet Delivery Time By Seconds
  - The New Crypto Uses Raw UDP Packets For Data Transfer
  - The AFSCN Is NOT (Yet) Net-Centric
- **As A Result**
  - Some Red/Black Front-End Capabilities Are Still Required
  - Red-Side Timestamps Are Difficult To Calculate Accurately



Modernized Hardware Architecture



- **With The KS-252 The Hardware Architecture Changes**
  - 1U Form Factor Crypto
  - Standard Network Switching & Cables
  - Each KS-252 Can Perform Either Encrypt Or Decrypt
  - Improves Device Pooling, Switching Etc
  - Front-End Systems Can Become Software Applications Or Libraries
    - NOTE: AFSCN Connectivity Still Requires Specialized Hardware

Path Forward

- **Some Might Consider 'Wrapping' The KS-252 With Serial**
  - Allows For Reuse Of Expensive Front-End Equipment
  - In Reality This Adds Unnecessary Complexity
    - IP-To-Serial Conversion Is Tricky
    - Adds Additional Systems: Switches, Hardware, Software etc.
- **Others Will Embrace The Net-Centric Possibilities**
  - Requires Hardware / Software / CONOPS Modifications
- **Timestamps Must Be Solved For Existing Satellite Programs**
  - No Small Task, But Solutions Already Exist
- **Consider Opportunities For Improvement**
  - Virtualization & Platform Independence
  - Sparing & Pooling Of Resources
  - Complete Software-Based Solutions
    - High Performance Software-Based Front-Ends Exist Today

Summary

KS-252 Testing Conducted To Date

Packets To/From Serial Telemetry Conversion	✔
All Telemetry Algorithms	✔
Automated Telemetry Invert (No Control Needed)	✔
Accurate Telemetry Time-Tagging	✔
Interoperability With Current/Legacy Telemetry Crypto	✔
Parallel Telemetry Processing for > 100 Mbps	✔
Packets To/From Ternary Command Conversion	✔
All Commanding Algorithms	✔
Binary/Ternary Commanding	✔
Interoperability With Current/Legacy Command Crypto	90%

Special Thanks To:
- CPSG
- ViaSat

Testing Conducted By:
- CPSG
- AMERGINT

Questions?