GSAW 2006
Automated Systems: What Technology Can (and Cannot) Do

John Urbano
Raytheon Intelligence and Information Systems

Pete Phillips
The Aerospace Corporation

Agenda

1. Svalbard Background
2. The Need
3. The Solution
4. Architectural Elements
5. Results to Date
6. Outage Factors
7. Evolving the System
8. Architectural Implications

Svalbard Background

Svalbard, at 78º N , is an ideal location to support polar orbiting spacecraft

The Norwegian Government, under an agreement with the NPOESS program and NASA, installed an undersea fiber-optic cable to provide a high bandwidth terrestrial connectivity between Svalbard and mainland Norway. The cost and use of this fiber is shared between the NPOESS Program and NASA, both of which have access to it for a 25-year period

The undersea fiber provides an economical data transfer alternative for NASA, NOAA, and DoD missions currently supported at the Svalbard site

What's Needed

Svalbard users needed a high-bandwidth, high-availability network to transfer satellite mission data from Svalbard, Norway to the U.S. with minimal downtime

Customer requirements for this network were as follows:

- Total Bandwidth of 155 Mbps
- Packet latency round trip time of 300 msec or less
- 0.001% packet loss or less
- Support Jumbo Frames (up to 9216 bytes per frame)
- Automatic fail-over restoral time of less than 1 minute
- Capability to identify failures within 20 minutes
- Minimum life-cycle costs
- No dedicated operations and sustainment staff

The Solution

Use commercially-available network equipment — switches, routers, etc.

- 24/7 on-call support and next day replacement where applicable

Use commercial data links to connect Norway to U.S.

Created a fundamentally robust, automated architecture that requires minimal human intervention to maintain required availability

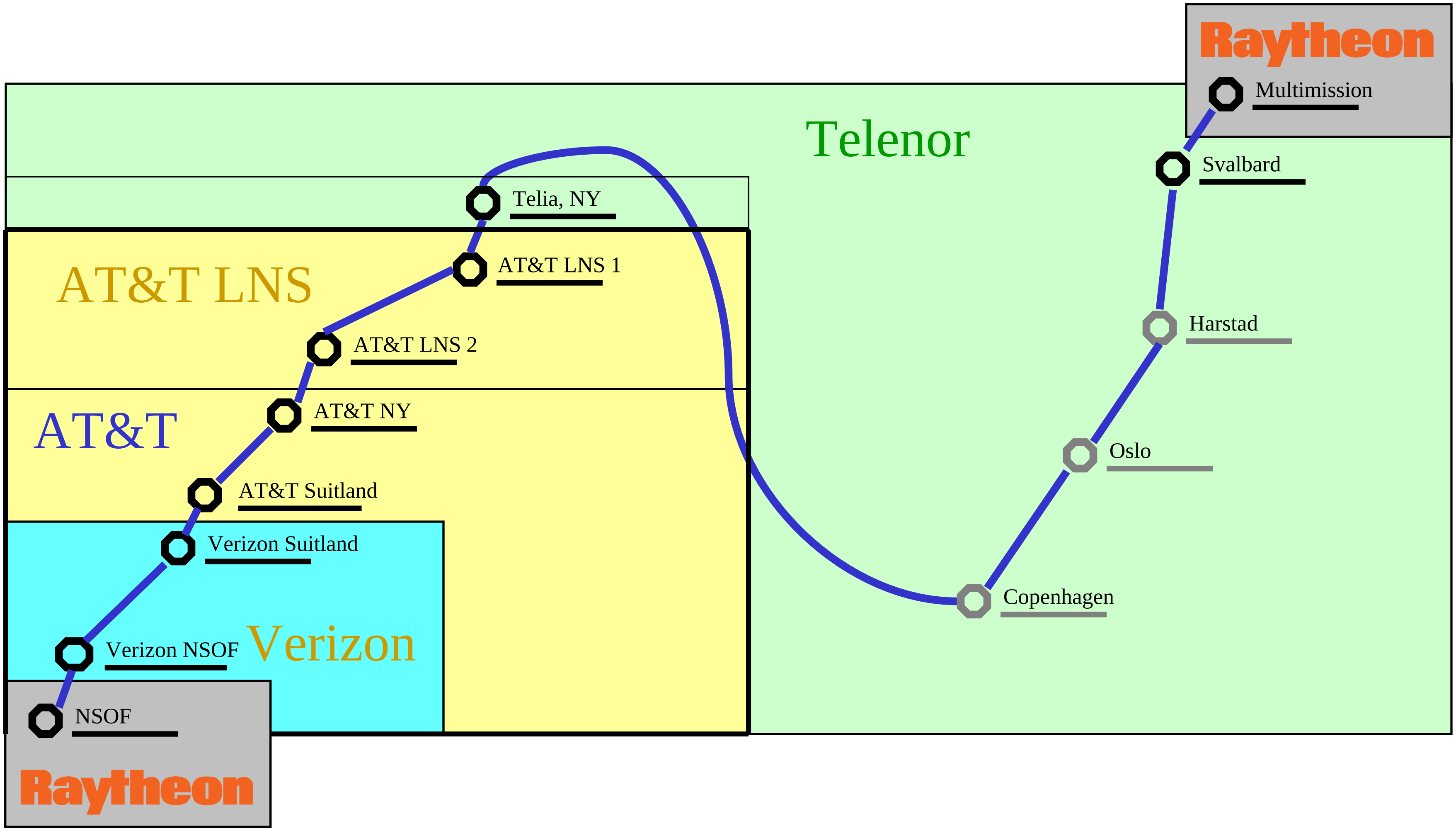
Architectural Elements

- CE Routers
  - APS 1+1 Configuration (Non-Revertive)
  - Remote Manageability (Out-of-Band)
  - Maintenance Support:

24/7 On-Call	IPO Watch Officer
9/5 On-Call	Raytheon Engineering

  - High MTBF Numbers for deployed hardware
- Carrier
  - Diverse Routes
  - Single Circuit with Failover Capability (APS 1+1)
  - 24/7 On Call Support (AT&T AGSEMC and Telenor)

The Network



Raytheon
Multimission
Telenor
Svalbard
Telia, NY
AT&T LNS
AT&T LNS 1
Harstad
AT&T LNS 2
AT&T
AT&T NY
Oslo
AT&T Suitland
Verizon Suitland
Copenhagen
Verizon NSOF
Verizon
NSOF
Raytheon

Operational Results to Date

Network Became Operational in Spring 2004

- The Svalbard link successfully supports the various NASA missions in use over Svalbard (NASA EOS Mission being the largest user)
- The Navy Coriolis WindSAT mission is currently supported via the link taking X-band blind orbit passes over Svalbard
- Supported the POES launch of the NOAA N spacecraft capturing boost-tip data over Svalbard. In addition, POES is currently ramping up to take L and S band blind orbit passes over Svalbard
  - December 2005 – Successfully tested GAC, LAC, and HRPT capability

Operational Results to Date (Continued)

Results to Date:

Number of Outages = 15

Total Downtime in Hours = 48.75

- Comprehensive review of each failure produces improvements to hardware configurations and/or operations procedures

- Network Failures have resulted in minimal actual data losses due to OPSCONS

- Sources of Network Failures were Both Technological and Human

The Technological Factors

- It is difficult, if not impossible, to have a “fully redundant” system. Examples:

- Embedded software is typically the same in redundant devices, and therefore NOT redundant
  - E.g. we experienced an outage due to a Cisco operating system software bug, which was corrected by an upgrade

- Although redundant, our Cisco Customer Edge (CE) router had a partial hardware failure which caused an extended outage
  - The Supervisor Module monitors both primary and redundant routers, and is therefore NOT redundant
  - Due to a partial failure of the supervisor module, the circuit did not failover
    - Had to manually shutdown the interface to force a failover and reboot the router
  - This failure was attributed to infant mortality, module was replaced and is working nominally

The Human Factors

Instances of Human Error:

- Communications service provider “non-interference” infrastructure enhancements that inadvertently interrupted our network
  - Many of the human error outages fall in this category

- Communications service provider scheduled work that was not well coordinated with all stakeholders and end-users

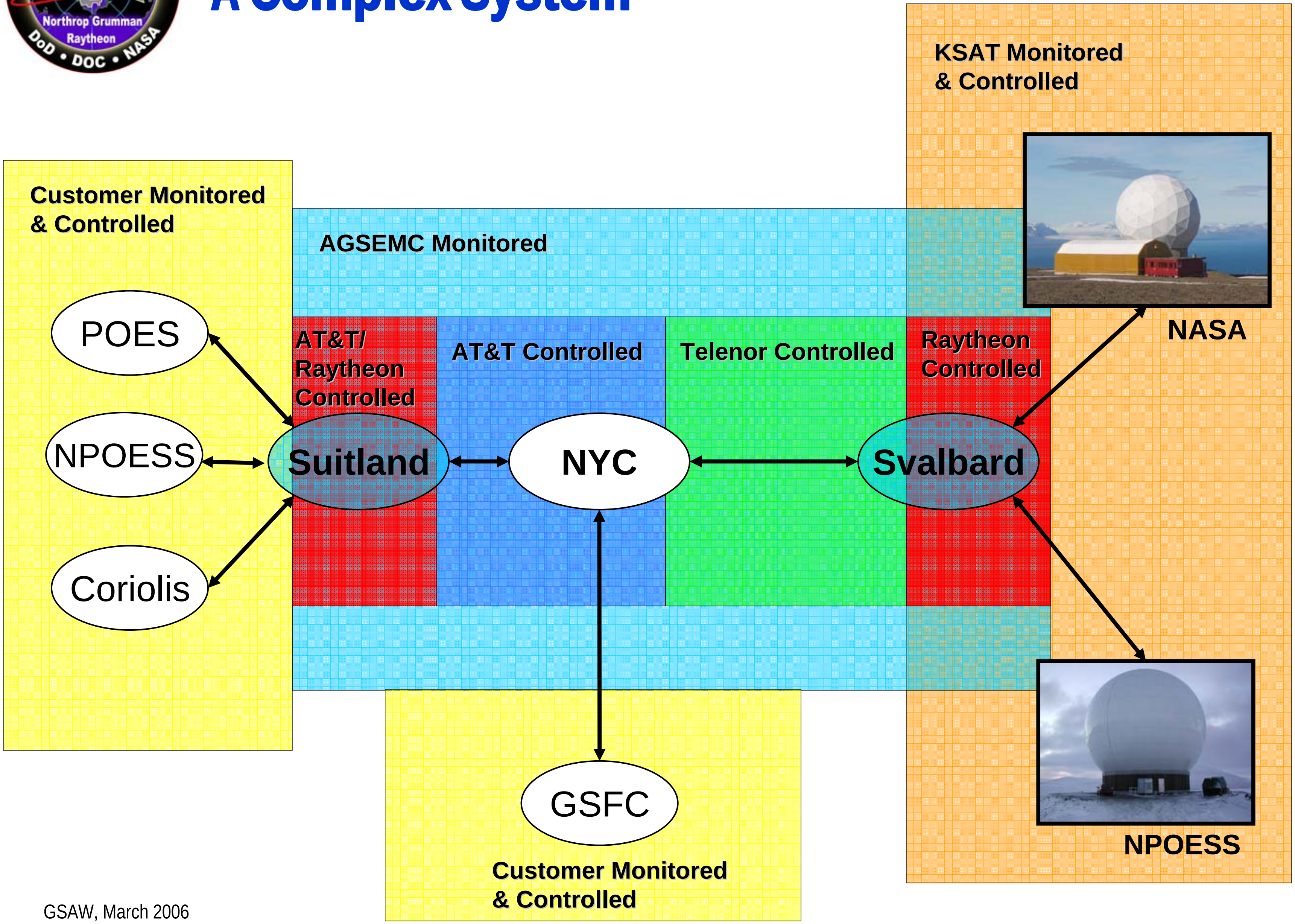
- Difficulty in contacting on-call personnel in a timely manner increased duration of some technology-related outages

The "X-Factors"
Age and Complexity

- Even with extensive testing, systems are more likely to fail in early operations than later on
  - "Infant mortality" is still an issue with technology-intensive systems
  - Human error is also more likely early on

- Increased complexity represents an increased risk to system availability
  - Complex systems are more likely to fail than simple systems
  - The more hardware and humans that are added to a system, the more complex the system
  - With a circuit that spans from CONUS to Svalbard, Norway, there are 4 different telecommunications providers, and multiple interface nodes, that can contribute to outages

A Complex System



KSAT Monitored
& Controlled

Customer Monitored
& Controlled

AGSEMC Monitored

POES

NPOESS

Coriolis

AT&T/
Raytheon
Controlled

AT&T Controlled

Telenor Controlled

Raytheon
Controlled

Suitland

NYC

Svalbard

NASA

NPOESS

GSFC

Customer Monitored
& Controlled

Evolving the System

- System Characterization
  - Each outage is treated as a learning experience and we take positive actions to minimize probability of recurrence
  - For every outage, an outage report is generated and forwarded to all parties (Service Providers, IPO, and Customers)
    - Service providers provide a summary RFO (reason for outage) by next business day and a more detailed explanation of the outage within 5 business days
    - Raytheon in turn generates the outage report and forwards information to the customers and the service providers
  - Raytheon convened “6Sigma” project with entire stakeholder community to look at outages from a system perspective and determine if any architectural changes were needed
    - Technological and Human Factors evolved based on findings and recommendations

Evolving the System (continued)

- Technological Evolution
  - Addressed “infant mortality” by replacing faulty hardware and upgrading to newer versions of embedded software
  - Reviewed overall architecture with vendors
    - Vendors assured us our baseline was sufficient to meet customer requirements
    - Investigated alternate configurations with vendor but told regardless of the configuration, additional internal redundancy would not have prevented our problems
    - Informed the only true redundant architecture for our application would be two active circuits
  - Since any possible changes would add complexity to an already complex system, no major changes were made to fundamental technology or architecture

Evolving the System (continued)

- Human Factors Evolution
  - Primary changes were to improve synergies between human and technological elements
  - Updated troubleshooting procedures for on-call personnel based on lessons learned from system outages
  - Improved communications channels among on-call personnel
  - Increased operations discipline

Architectural Implications

- To be effective, an architecture for automated operations should:
  - Adhere to the simplicity paradigms of “Less is More” and “KISS” —adding more equipment or staff adds more complexity, which increases the number of failure modes and likelihood of system failure
  - Describe required synergies between human and technological elements
  - Identify the technological limitations in redundant modules— single-point failures can, and do, exist even in “fully redundant” designs
  - Be robust to failures during early operations—technology and/or human error can cause the unexpected