Shifting Decision Perspectives for the System Engineer

Integrating System Security Into the Mix

zefyr Avril

Presented by

Kenneth Kepchar, ESEP CISSP
EagleView Associates LLC

Topics

- Three Case Studies
- The Common Threads
- Common Perceptions of Security
- The Intersection of Security and SE
- Basic principles for Integrating Security into SE decisions
- Considerations for the System Engineer
- Benefits & Conclusions

Intelligent Transportation System

On board sensors

Availability

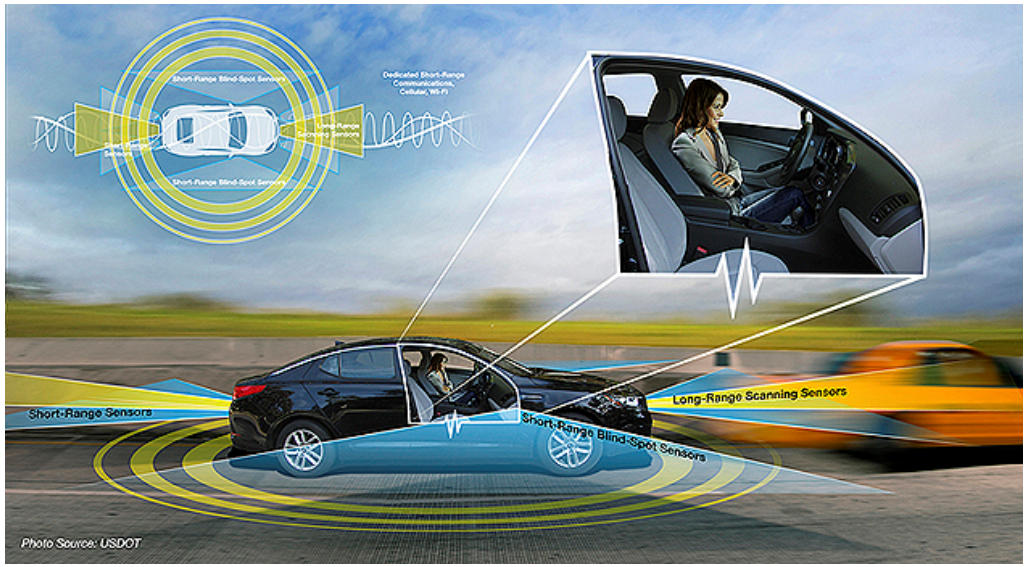
Cameras

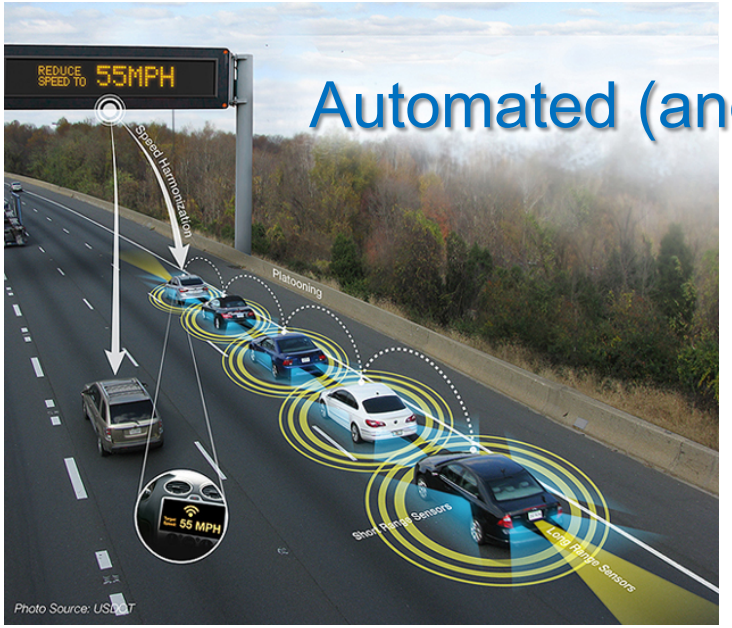
Safety services

Tamper Proof

Integrity

GPS





Automated (and connected) vehicles

Supply chain

PNT

Wireless

Service continuity

Advisory services

Real time data

Data accuracy

Images courtesy of the U.S. Department of Transportation

Aviation - Moving Into the Digital Age

N.J. man fined $32K for illegal GPS device that disrupted Newark airport system

By Steve Strunsky/The Star-Ledger
Email the author | Follow on Twitter
on August 08, 2013 at 4:28 PM, updated August 08, 2013 at 9:33 PM

Print

NEWARK — The Federal Communications Commission has fined a Readington man nearly $32,000 after concluding he interfered with Newark Liberty International Airport's satellite-based tracking system when he used an illegal GPS jamming device in his pickup truck to hide his whereabouts from his employer.

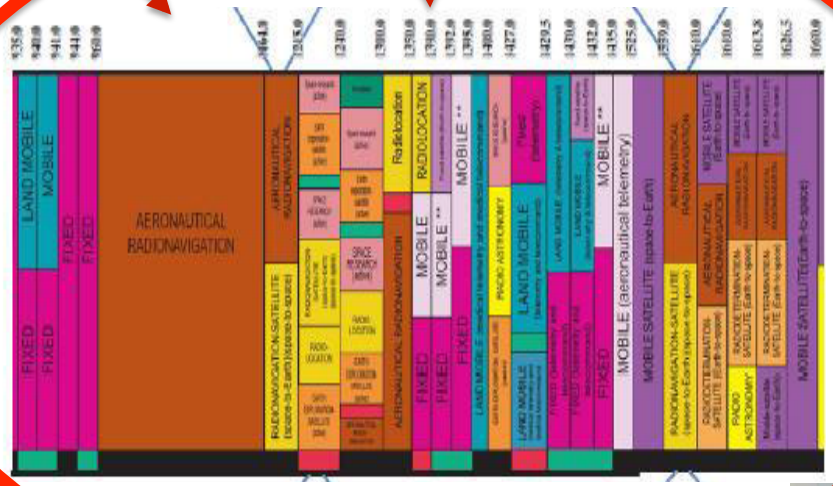
The FCC said an aircraft tracking system at Newark Liberty International Airport experienced interference from a GPS jamming device used by a Readington man who claimed he was simply trying to hide his whereabouts from his employer. The FCC fined the driver $31,875.

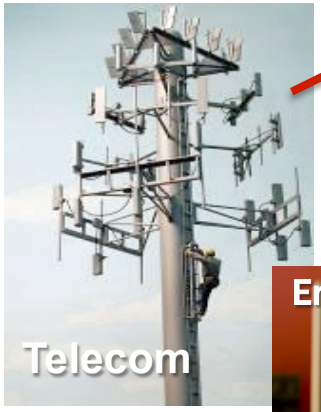
Jennifer Brown/Star-Ledger file photo

Disrupting satellite signals can hinder air traffic controllers' ability to receive accurate information about a plane's location in the air and on the runway.

In what is known as a notice of apparent liability posted on its website last Friday, the FCC imposed the civil penalty on Gary Bojczak, who lives in the Whitehouse Station section of Readington in Hunterdon County.

Spectrum - A Precious Commodity
So Many Demands – So Little Supply





The Common Threads

- **Technology drives the technical decision landscape that System Engineering operates in**
- **System integration involving legacy technologies and systems can be hazardous**
  - ***Benefits (value) usually based on only system of interest***
  - ***Interaction with installed base usually not optimal (It's the unintended consequences that get in the way)***
- **System Engineering must balance more than technical considerations**

California eyes $3 billion RUC scheme to fund maintenance

Two of Cali[illegible]'s biggest transport coalitions have proposed a [illegible] Fund, charging road users to create $3 billion for highway maintenance.

Transport California and the California Alliance for jobs jointly submitted proposals to the California Attorney General, which they reckon if approved by voters, would raise $3 billion annually to fix the Golden State's deteriorating roads, highways and bridges.

The proposed California Road Repairs Act of 2014 would impose a fee of 1 per cent of the market value of the vehicle.

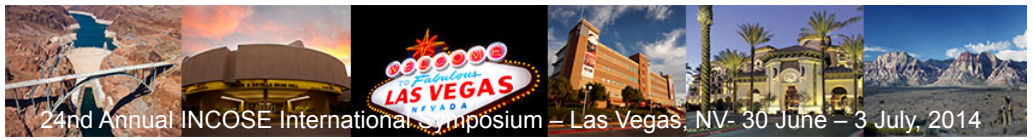
Will Kempton, former head of Caltrans who leads the non-profit advocacy group Transport California, said the initiative would ask voters as early as November 2014 to gradually increase vehicle registration fees [illegible] years.

Pointing to California's impending financial crisis for road works, the proposal declared that poor road conditions cost Californian drivers more than $600 each year in vehicle maintenance, and that worsening congestion costs motorists an estimated $18.7bn every year in lost time and fuel – not to mention environmental pollution.

It presented the idea that every dollar of maintenance work that is put off, will end up costing $50 in more expensive replacements and repairs later on. And it represented findings according to a recent report by the California Transport Commission, that 58 per cent of state roads need improvements.

- **Compliance technology based on GPS**
- **Road User Charging Motivates Jamming**
  - **Fraud Detection is Essential**
  - **Detected Jamming Should Raise Red Flags**

Based on National Space Based PNT Advisory Board Presentation ***6****-3-14*

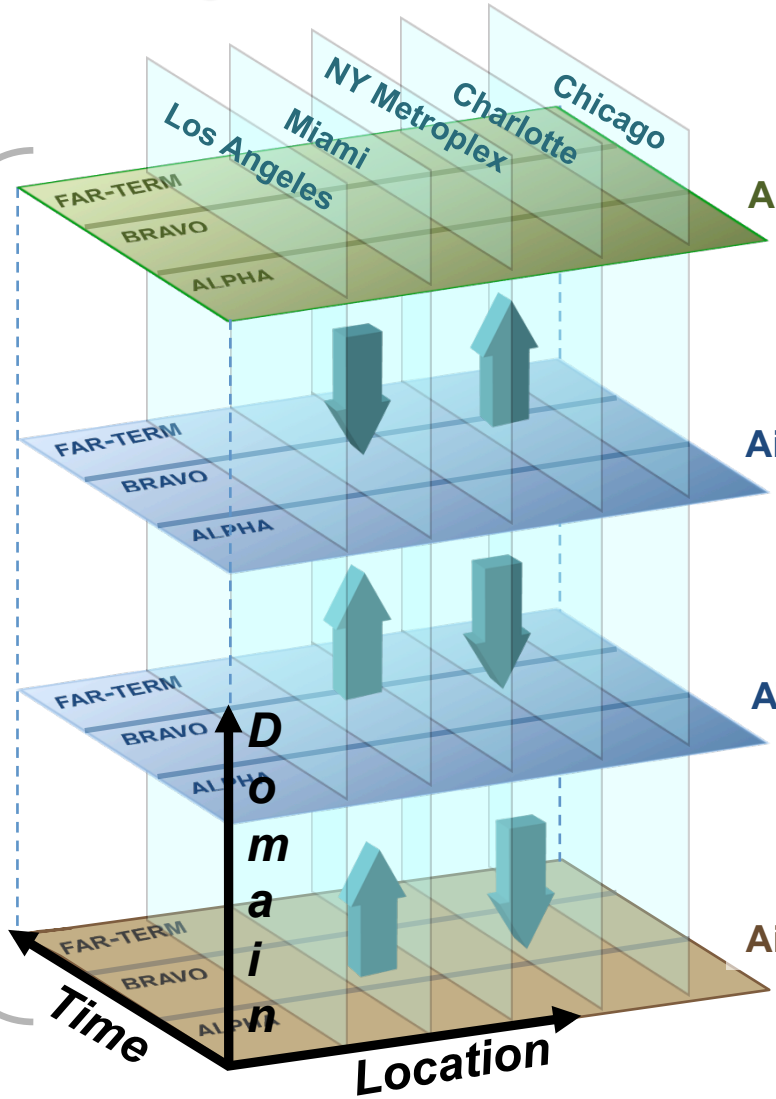


NextGen Operations

An Integrated Framework

Cross-Cutting Factors

- Environmental
- Safety
- Information Security
- Economic
- International
- Regulation



Enablers

- People
- Procedures
- Technology
- Data/Information
- Policy

Legend:

- Private Sector
- FAA (USG)
- Local entities

Common Perceptions of Security

"It's an Issue of Priorities!"

- It's a (major) constraint to system performance
  - *It's not a positive influence or benefit*
- Security only drains my budget
  - *AND I never get budget for it!*
- It's strictly the purview of the an expert
  - *Not part of the SE scope*
- Consideration should wait until the design has stabilized
  - *We only get to commit the resources once – Why not wait so we have a better chance of being right?*
- It should not influence performance decisions
  - *Performance? Either the system is secure or …*
- (Security) technology is out of date before the product is delivered
  - *Threat environment is evolving rapidly – and accelerating*

The Intersection of Security and SE

System Engineering (SE) is responsible to look at the system as a whole *(and beyond)*

Security System Engineering (SSE) ensures the security aspects are:

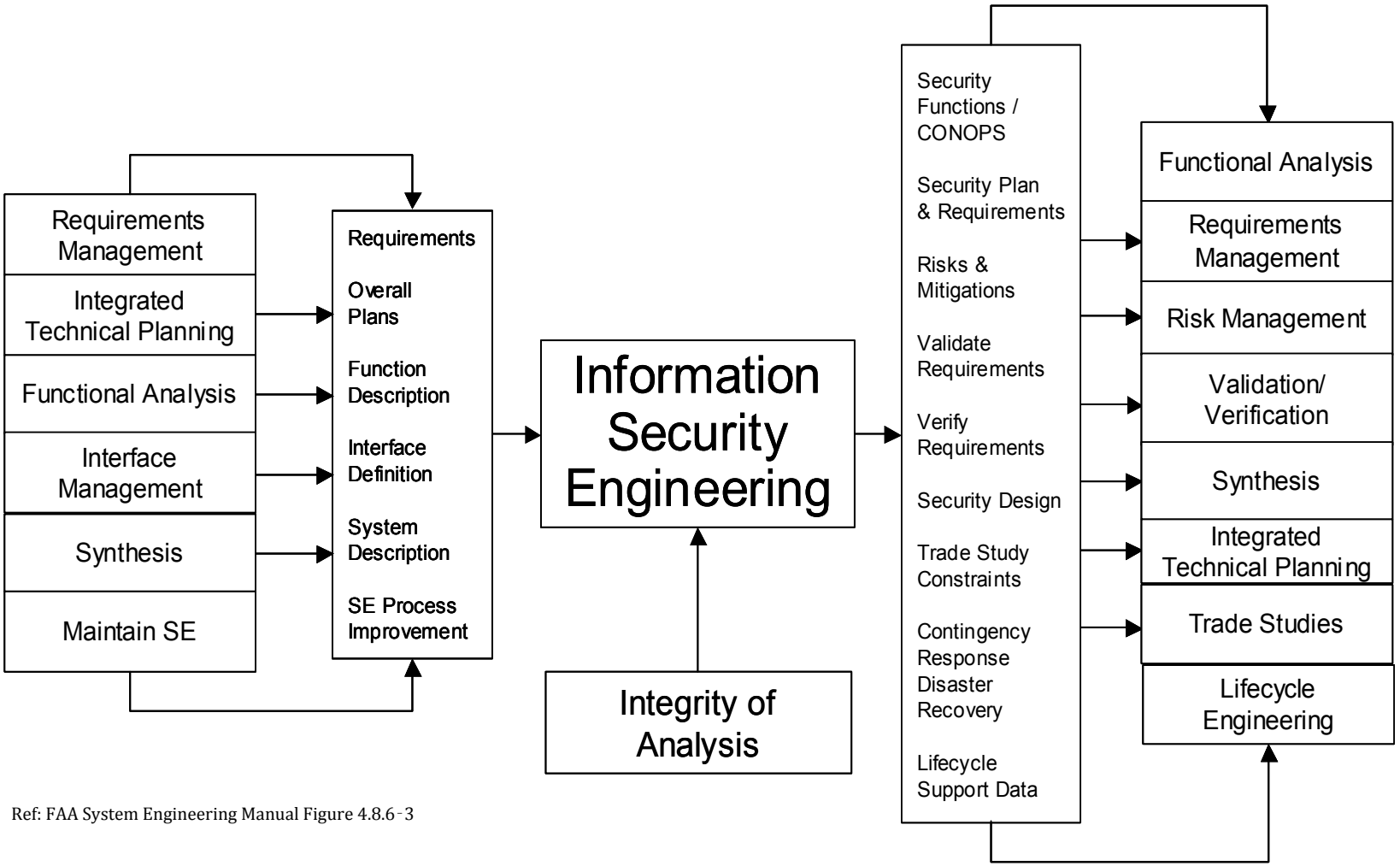
- ***Understood***
- ***Factored in Technical decisions affecting the outcome – i.e. the system***

The System Security Engineering role:

- **No different than the SE role, but with "security" as it's bounds**
- **Provides expertise to support effective SE outcomes by portraying both benefits and limitations of security solutions**
- **Determines system security capability effectiveness**
- **Liaison with stakeholders specifically on security**
- **Support V&V or Operational assessments**

Keys to success involve an ongoing robust dialogue, common mindset for success, and a common understanding of terms and concepts

Security Engineering Relationship to Other System Engineering Processes



Ref: FAA System Engineering Manual Figure 4.8.6-3

Basic principles for Integrating Security into SE decisions

- **Establish a sound security policy as the foundation for design.**
  - ***Driven by the value and state of the information involved***
  - ***Affects system (and organizational) performance objectives***
- **Reduce risk to an acceptable level to limit or contain known vulnerabilities.**
  - ***External systems are assumed insecure until proven otherwise***
  - ***NO security solution is foolproof*** *(maybe today, but probably not tomorrow)*
  - ***Plan (and design) for degraded operations***
  - ***Pay particular attention to interfaces***
- **Good practices in security solutions go beyond the technical architecture of the system itself.**
  - ***Focus on the human component in the equation – It is the most unpredictable.***
  - ***Strike a balance between protection and ease of use***
- **Architect security to allow flexibility to adopt new technology, including a secure and logical technology upgrade path.**
  - ***THE one constant in the security equation – Threat landscape is always changing and faster than you can react***
  - ***System behavior should include addressing damage as well as continued operations.***

Considerations for the System Engineer

("My Mental Checklist")

- ✓ **Understand the contributions a security expert can make**
- ✓ **Integrate security into the system engineering effort.**
- ✓ **The operational integration challenges involved are constantly in flux.**
- ✓ **Security risks are included in project risk efforts and register.**
- ✓ **Tools and techniques are essential**

✓ Integrate security into the system engineering effort.

Legend
ISE Risk Management Process aligned with AMS
Numbered items correspond to AMS Life Cycle diagram numbers, above

a. Integrate Initial Security Needs and Threat Stipulation into MNS
b. Develop Preliminary ISSP including Basic Security Policy
c. Develop CONOPS and Preliminary Security Requirements
d. Develop Preliminary Vulnerability and Risk Assessment
e. Update Vulnerability & Risk Assessment
f. Update CONOPS and Security Requirements
g. Integrate Security Requirements with System Requirements
h. Integrate Security Architecture & Design
i. Update ISSP
j. Develop Security Test Plans & Procedures
k. Develop Users Guides, Training, and Contingency Plans
l. Conduct Security Testing
m. Create Final Security C&A Documents
n. Obtain Security Authorization/ Accreditation
o. Prepare for Tech Refresh & Upgrade

Ref: FAA System Engineering Manual Figure 4.8.6-4

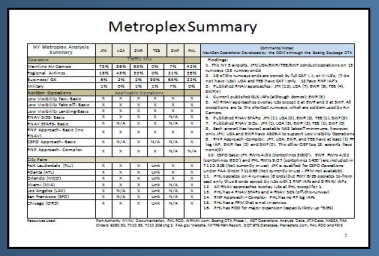
Integrate the Security artifacts into the appropriate SE artifacts as well.

✓ The operational integration challenges involved are constantly in flux.

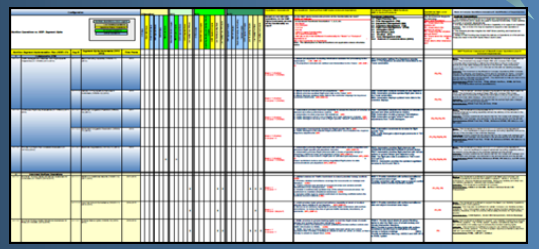
NextGen Stakeholder Equities

- Where does the air transportation community want to go?
- What is needed to achieve the NextGen vision?
- What do we have today that we can leverage for the future?
- How can we implement NextGen capabilities?

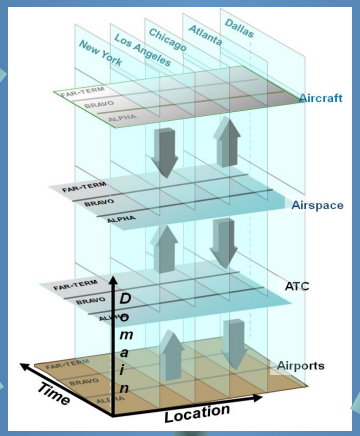
Mid-Term Operations

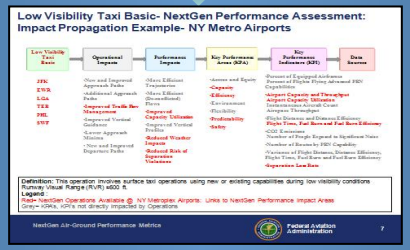


Metroplex Analysis

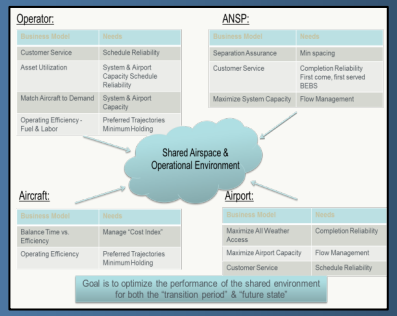


NSIP Alpha vs Operations (Portfolios)

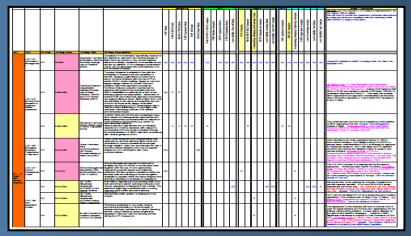




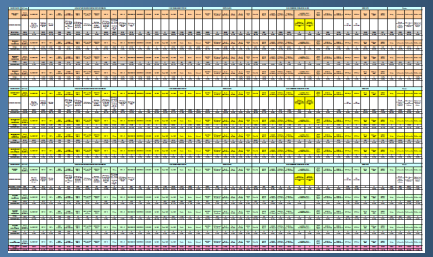
Operations to Benefits Metrics



Business Case Factors



NextGen/SESAR Harmonization



OEM Projected Equipage Statistics

V 1.0

✓ Tools and techniques are essential

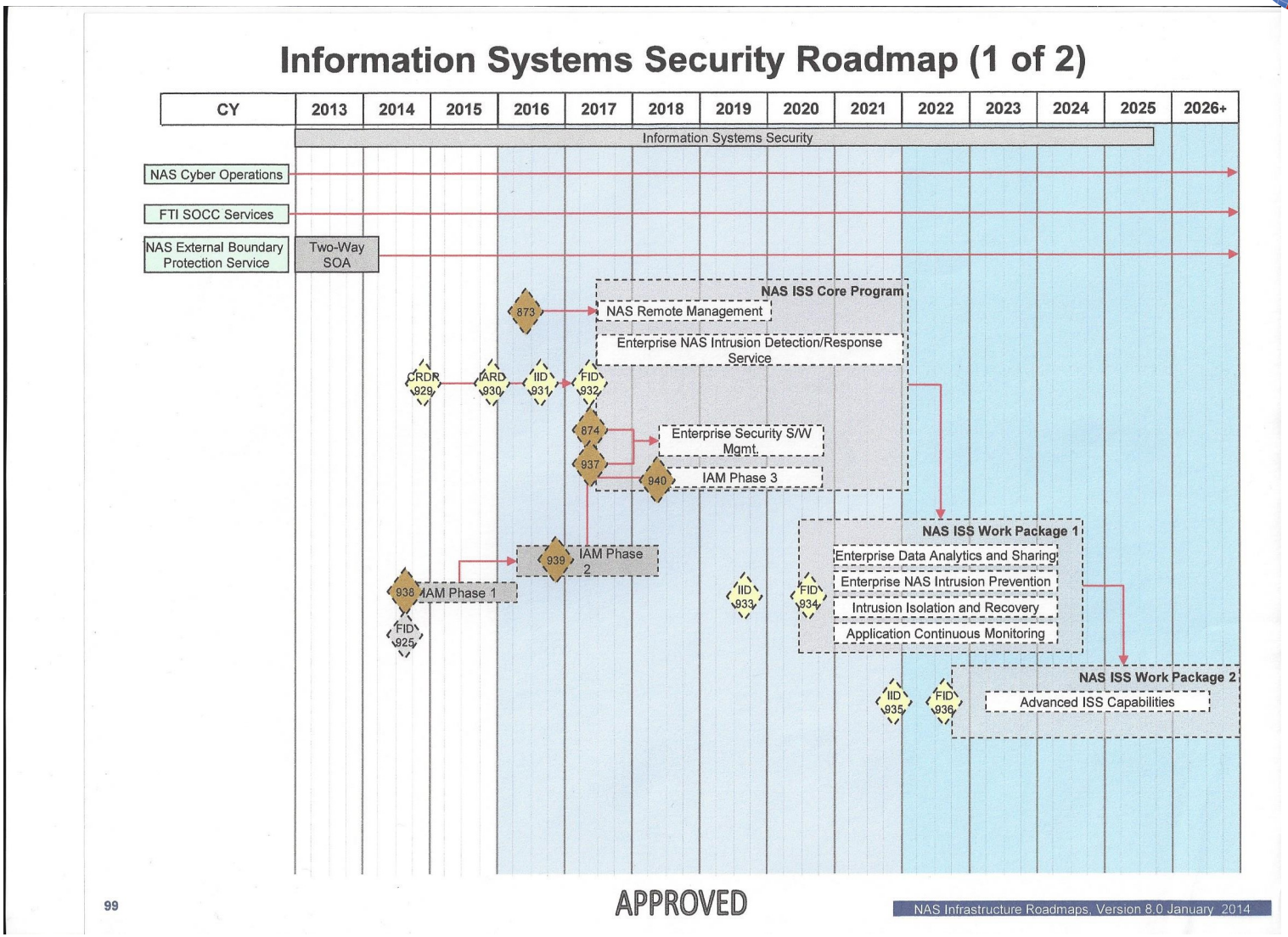
Effective Communication is the key, especially for complex systems or Systems of Systems

- Example of a “System Security Roadmap”
- Portrays security capabilities envisioned
- Shows when they would be available
- How they support planned system capabilities
- Technologies involved
- Highlights which program decisions involve security and when they need to be made

Tools of this nature involve time, resources, and commitment

Benefits realized include the security aspects considered in the same dialogue with all the other technical factors bearing on the decision.

Sample Roadmap Content



Benefits

- **Integrating security into SE deliberations doesn't have to be a binary choice of performance vs security**
- **Integration is not only possible, but can even be straight forward**
- **Integration has happen early and often**
- **Key ingredients to be successful include:**
  - ***Effective communications***
  - ***Shared view of system value, risks, and utility***
  - ***Shared perspectives without barriers of language and terminology***

In the process we can bury some of those myths that have haunted us.

Pragmatic Perceptions of Security

- It's a (major) constraint to system performance - *It's not a positive influence or benefit*

  Architect security as a system function or service

- Security only drains my budget - *AND I never get budget for it!*

  Like any other system function, allocate the appropriate resources

- It's strictly the purview of the an expert - *Not part of the SE scope*

  SE needs to seek expertise and balance their contributions

- Consideration should wait until the design has stabilized - *We only get to commit the resources once – Why not wait so we have a better chance?*

  Architecting is iterative, just like design. The earlier, the better the fit

- It should not influence performance decisions – *Both performance and secure?*

  The answer is how you architect the security features & trades involved

- (Security) technology is out of date before the product is delivered - *Threat environment is evolving rapidly – and accelerating*

  Architect a robust service based on proven security practices

Questions

Ken Kepchar

EagleView Associates LLC

eagleview2@cox.net