32nd Annual INCOSE international symposium

hybrid event

Detroit, MI, USA
June 25 - 30, 2022

Mon 27, Jun 15:30 -16:55 ET | INCOSE Telecommunications WG

How to apply a criticality framework to your communications' networks

www.incose.org/symp2022

Background

2018

SESA Telecommunications Working Group established

2019

INCOSE Telecommunications Working Group established

2020

Defining Critical Communications Networks: Modelling Networks as Systems published in INCOSE's INSIGHT magazine

2021

Criticality Framework

A Criticality Framework for Resilient Communications Networks (unpublished)

2022-23

Development and publication of a Telecommunications Primer

Telecommunications Primer

Member link: https://connect.incose.org/Library/InsightMagazine --> INSIGHT_v23-2_0629

Keith Rothschild
Atlanta, Georgia USA
(Cox Communications)

William Scheible
Mineral, Virginia USA
(MITRE Corp)

Thomas Manley
Canberra, Australia
(Decision Analysis Services,
Co-Chair INCOSE
Telecomm WG)

Susan Ronning
Portland, Oregon
(ADCOMM Engineering,
Co-Chair INCOSE
Telecomm WG)

Panel Members (INCOSE Telecommunications WG Members)

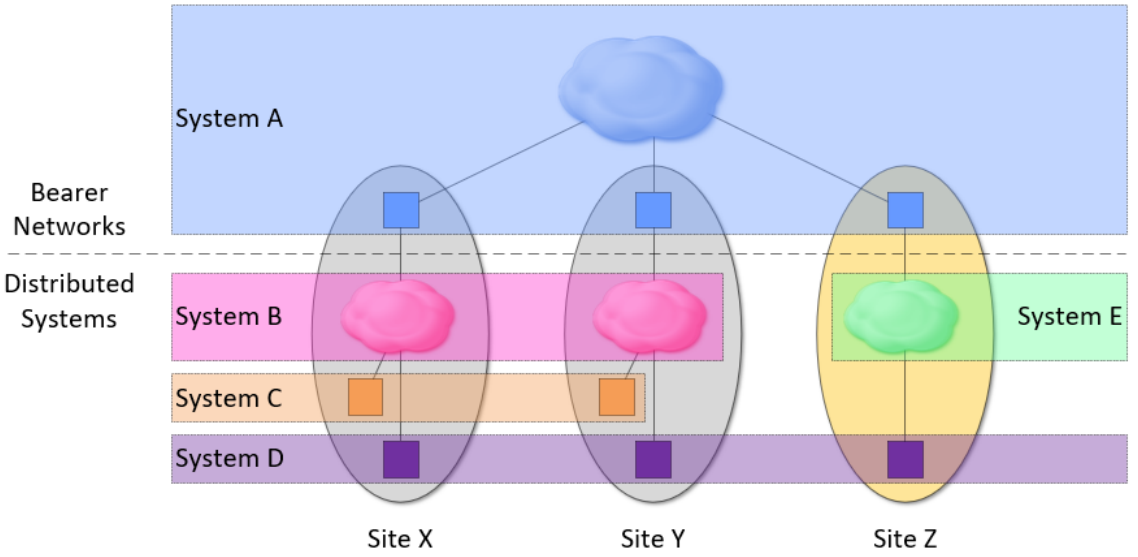
What are Communications Networks?

- **Transfer of information** *between* locations and *within* locations
- Information types:
  - *Voice* (e.g. two-way radio, mobile phone)
  - *Data* (e.g. emergency alert notifications, SCADA, control systems, iOT)
- Location (aka site) types:
  - *Fixed* (e.g. buildings, train stations, control centres)
  - *Mobile* (e.g. rolling stock, vehicles, ships, satellites)
  - *Personal* (i.e. carried by people or animals)
- Two perspectives:
  - those *providing* communications services (e.g. carriers, cloud applications)
  - those *utilizing* them (e.g. enterprise agencies, businesses, end users)

Types of Communication Networks

Bearer Networks – connect locations together (e.g. leased lines, cellular, LMR, Satellite Communications)

Distributed Systems – systems whose elements operate together, irrespective of geographical distribution, or are at least managed as one system (e.g. a corporate LAN, a ticketing system, CCTV as well as Zoom, Teams, web/mobile apps etc)

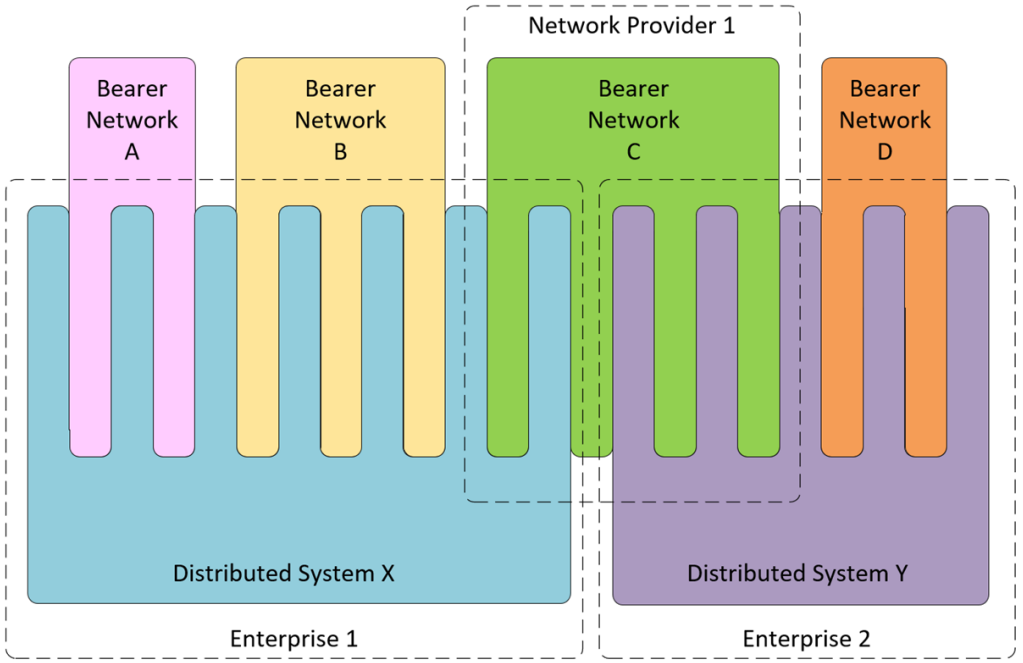


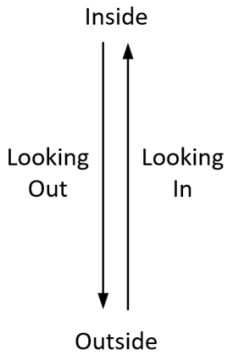
CCTV: Closed Circuit Television
LAN: Local Area Network
LMR: Land Mobile Radio

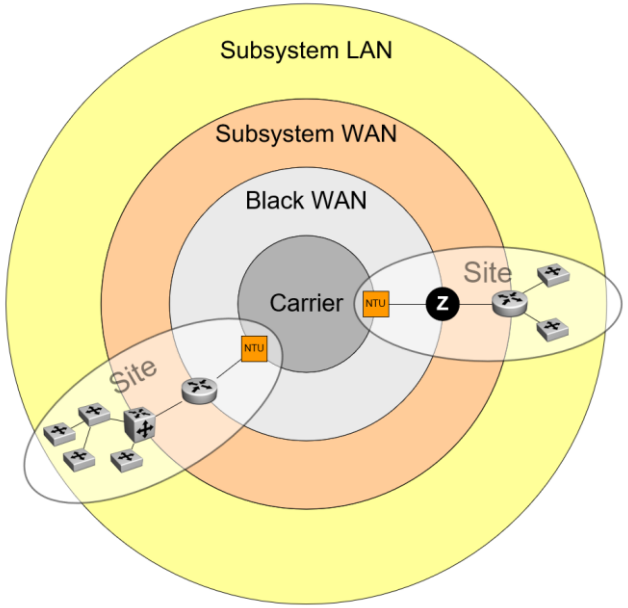
Manley, T., Ronning, S. & Scheible, W. (2020). Defining Critical Communications Networks: Modelling Networks as Systems. INSIGHT, 23(2), 36-42

Relative Perspectives

- *Inside Looking Out* – the perspective of the network provider (carrier)
- *Outside Looking In* – the perspective of the enterprise (service/application)







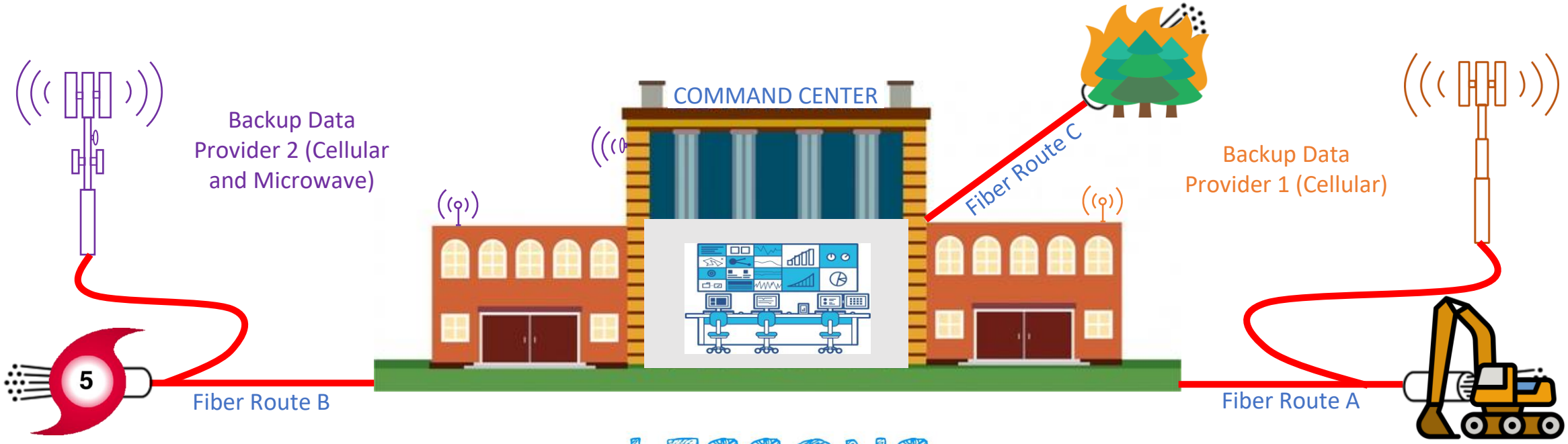
Enterprise Perspective
(Outside Looking In)

Perspective: Network Provider

Keith Rothschild
Atlanta, Georgia USA
(Cox Communications)

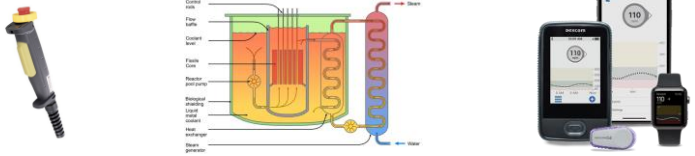
- Dr. Keith Rothschild is the Senior Principal Engineer for Cox Communication's Technology Solutions Engineering organization (Atlanta, GA, USA). His work focuses on solving problems related to complex adaptive systems of systems, including autonomous/machine learning, late-binding/dynamic resource-cost optimization, diverse design as a real-time service robustness strategy, and polymorphic policy adaptation.
- Dr. Rothschild is an IEEE Senior Member with over 20 years' experience in the telecommunications industry, and has over two dozen patents in diverse areas including data storage, Hybrid-Fiber-Coax (HFC) architectures, digital rights management, network-DVR, cloud computing, and content-aware networks.
- He has a BS in Electrical/Computer Engineering from Carnegie Mellon University, an MBA from DeSales University, and his Ph.D. from Northcentral University and is an active member of the INCOSE Telecommunications working group.

Network Provider Perspective: Climate Event



Design Paradigm: Fail To Safe

If it is important enough to design failure mitigation you should also contemplate what happens if it still fails…



https://www.healthline.com/diabetesmine/when-medical-technology-fails

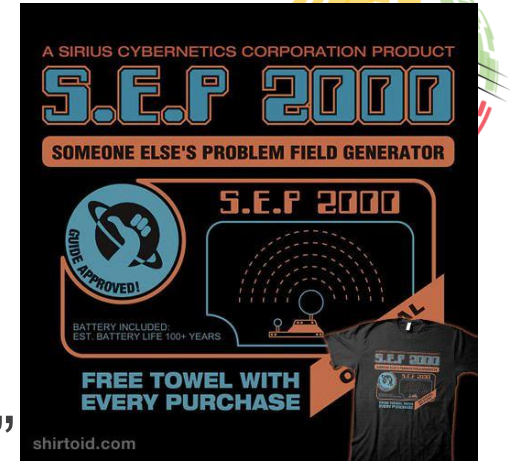
Common-Cause Failure and the need for Diverse Design even in the "IT" Paradigm

Expired Certificates

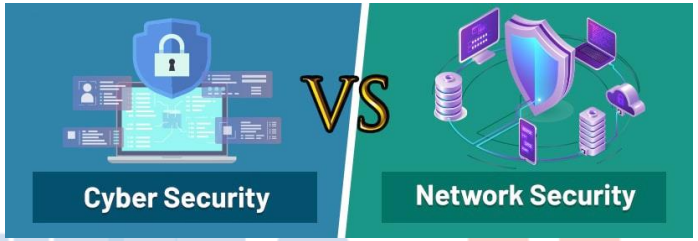
Shared Resources

Common Code Libraries

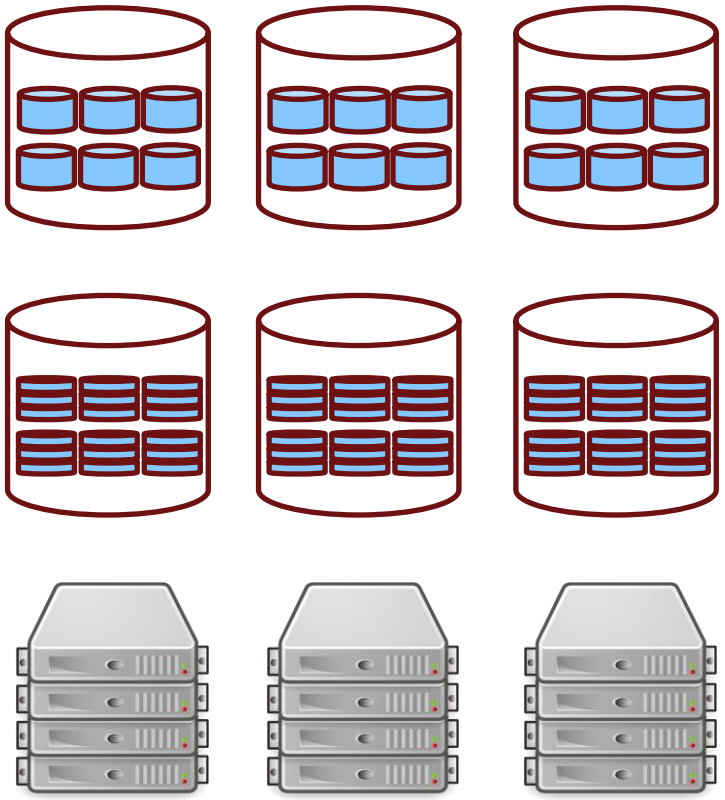
Communication Networks for SEs



- Networks are Layered – there is rarely a single ”network”
- Systems use networks internally and to connect to other Systems
- Networks can be dynamically reconfigured, undergo maintenance, and experience failures – not all interruptions are failures!
  - How do systems respond to different types of network interruptions?
  - How do systems respond after the network interruption has been restored?
  - What is the impact to adjacent systems of the behavior during the network interruption and in response to restoration of the network connectivity?



Technology Advances



As designs become increasingly segmented, the teams responsible for different components (database vs. logical storage vs. physical infrastructure) have designs with completely independent lifecycles.

It is important to consider how each of these are segmented, how the failure zones align with each other, and how they align with network connectivity.

Perspective: Wireless Services

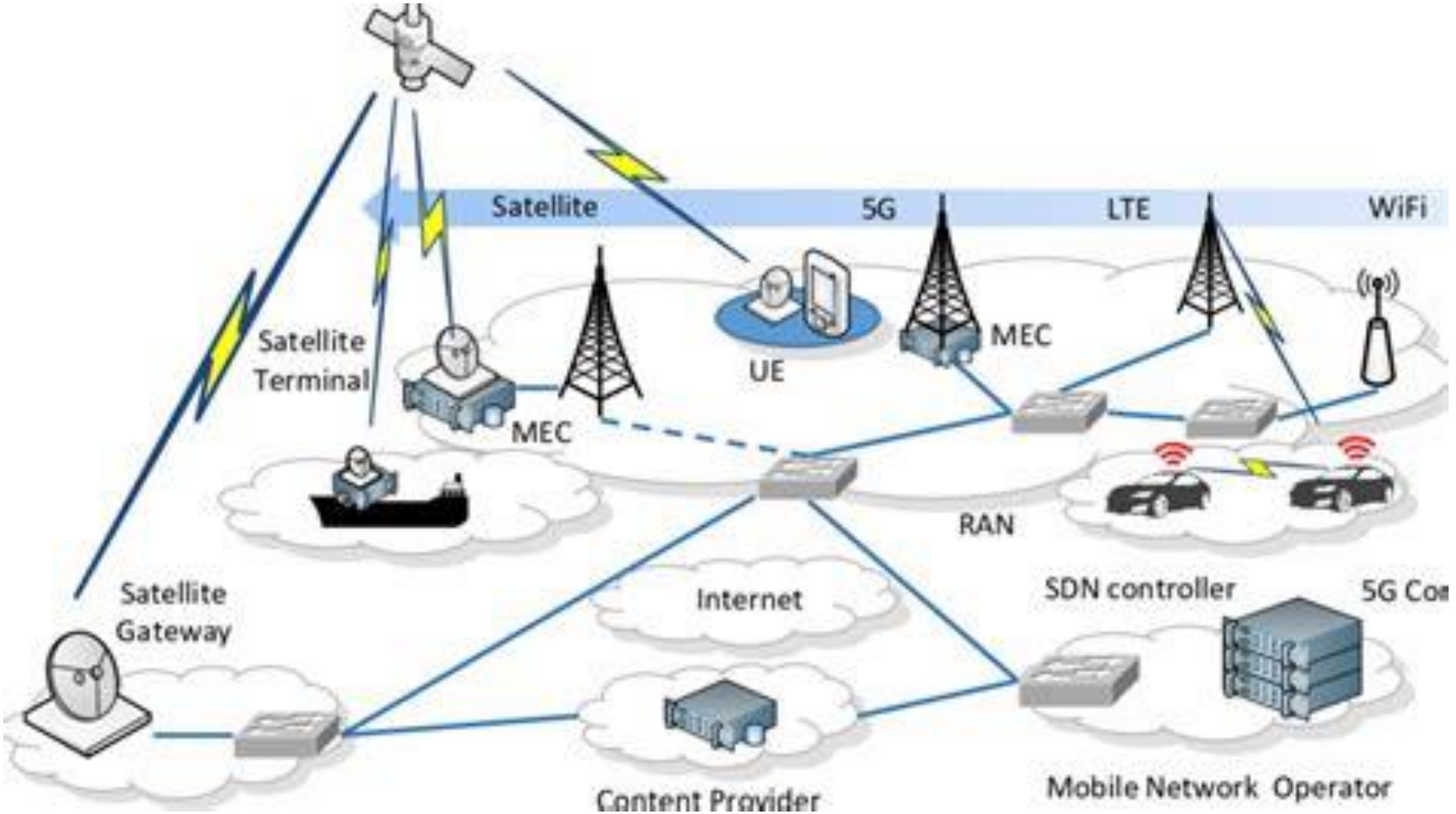
William Scheible
Mineral, Virginia USA
(MITRE Corp)

- Mr. William Scheible is a Principal Network Systems & Distribution System Engineer with the MITRE Corporation (McLean, VA, USA).
- He has over 35 years of both commercial and government experience in all facets of network design, network operations, and systems architecture working with both wired and wireless infrastructures.
- He began his career with Tymshare/Tymnet in Cupertino, CA developing packet switching networks, followed by engagements with several financial, consulting and networking companies before joining MITRE in 2002.
- He holds ESEP and CISSP certifications and is an active member of the INCOSE Telecommunications working group.

Thoughts on Wireless and Critical Infrastructure

• No surprise, but wireless services, especially for end user to host has become the defacto communications solution for entertainment, personal connections and now business.
–Normal business and especially disaster recovery is now being done using wireless services
• 99% of wireless services is carrier or vendor provided.
–To this point, wireless services are a key input to the application of the criticality framework
–For critical applications, you need to know what your carrier can offer to support them.
• Users and IT departments have very little control over the quality and stability of wireless services. (LTE, 3,4 and 5G..not Bluetooth)
–Redundancy, alternate access and awareness of what is being offered locally
–Know the service limitations when applying the framework.
• More alternatives, such as LOE satellites and expanded WI-FI access are available
• Remember these are paid for services and access control(s) can be a dangerous obstacle during a crisis.
• There is usually at least one alternative connection method between two points.
–Be prepared and work though how to support a DIL (Delay, intermittent, low bandwidth)
• Mobility support, as a critical service need, will be continue to be a significant challenge, especially in the world of newer and more powerful applications.

Bearer Network Architecture



Perspective: Military

Thomas Manley
Canberra, Australia
(Decision Analysis Services, Co-Chair INCOSE Telecomm WG)

- Mr. Thomas Manley is a Principal Consultant with Decision Analysis Services Ltd (Canberra, Australia).
- He is a foundation member of the SESA Telecommunications Working Group that became an INCOSE working group
- Mr. Manley has 20 years' experience in network engineering, systems engineering and enterprise architecture, primarily for Defence and ATO, working for Optus, Telstra, Boeing and Thales.
- He holds a CSEP certification and is CPEng. He has a BE/BSc and an MBA from Australian National University and is Co-Chair of the INCOSE Telecommunications working group.

Military Communications Networks – Characteristics

- Distinction between Enterprise and Tactical Networks
- Enterprise Networks tend to be partitioned (e.g. into different security domains) and exist long term
- Tactical Networks tend to be:
  - Mobile / Ad-Hoc
  - Nodal (vehicles incl. unmanned autonomous systems (UAS), dismounted soldiers, satellites)
  - Disconnected, Intermittent and Limited (DIL) scenarios
  - Spectrum is congested, contested, competitive
  - Challenges planning and configuring networks (e.g. crypto keys, channel selection)
  - Increased use of data (IP) over voice
  - Cybersecurity concerns increasingly important
  - Coalition interoperability / Federated Mission Networking (FMN)

Current Ukraine Conflict

- Cyberattack on Viasat satellite capability on 24th Feb blamed on Russia as attempt to disrupt Internet services in Ukraine to “cripple command & control”[1]
- SpaceX has sent ~15,000 Starlink internet kits to Ukraine since the war began on 24th Feb to avoid dependency on terrestrial networks[2]
- “*The strategic impact is, it totally destroyed [Vladimir] Putin’s information campaign*,”: Brig. Gen. Steve Butow, director of the space portfolio at the Defense Innovation Unit[2]
- Russians initially left Ukraine cellular networks functional due to unreliable Russian secure communication systems[3]
- Several Russian generals have been located and targeted through their use of unencrypted cellular phones[3]
- Significant use of lethal and non-lethal Uncrewed Aerial Vehicles (UAV) for surveillance, logistics and combat purposes

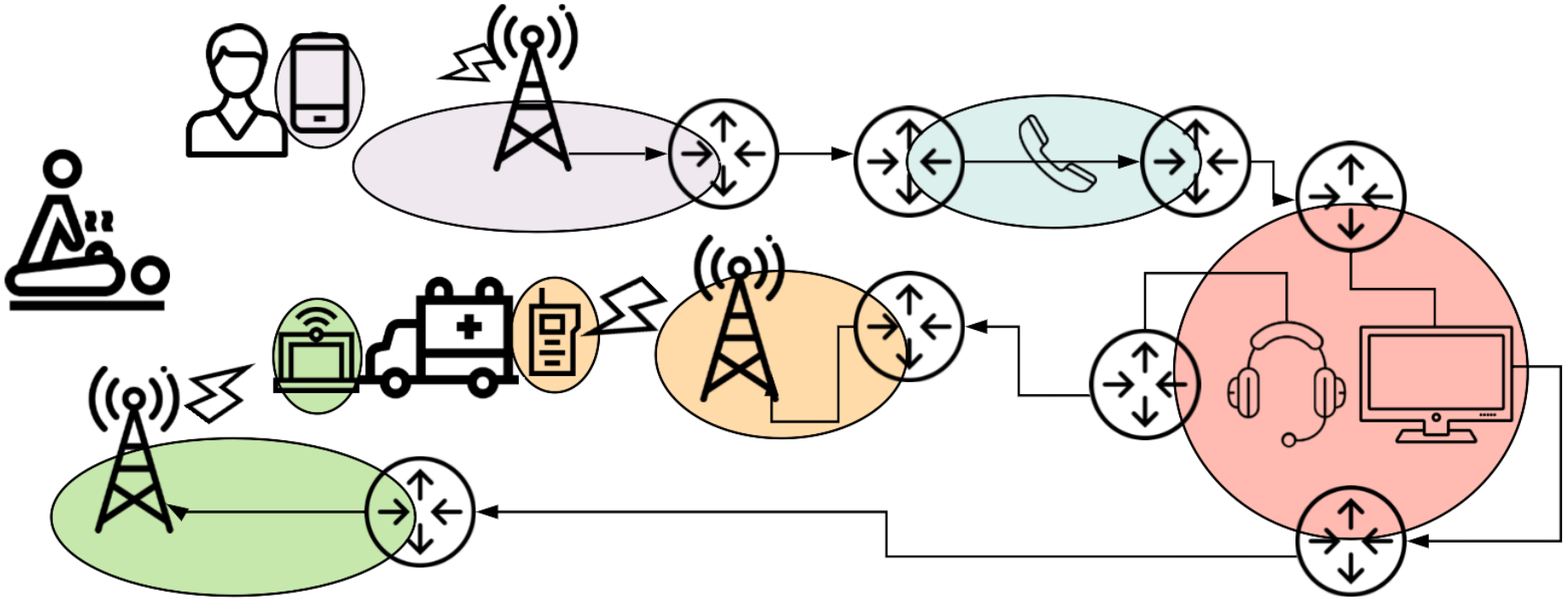
1: https://www.defensenews.com/digital-show-dailies/eurosatory/2022/06/15/how-russia-telegraphed-invasion-of-ukraine-in-space-and-online/?utm_%E2%80%A6
2: https://www.politico.com/news/2022/06/09/elon-musk-spacex-starlink-ukraine-00038039
3: https://www.newscientist.com/article/2315553-russia-and-ukraine-are-both-weaponising-mobile-phones-to-track-troops/

Perspective: Emergency Services

Susan Ronning
Portland, Oregon
(ADCOMM Engineering, Co-Chair INCOSE Telecomm WG)

- Ms. Susan Ronning is Owner and Principal Engineer of ADCOMM Engineering LLC (Sandy, Oregon, USA), a critical communications consultancy.
- She has over 20 years' experience in the telecommunications industry in the public safety, emergency management, utility, and transportation markets.
- She was a project engineer for Motorola and Tait Communications, led the operations and maintenance for City of Glendale, California, and consulted on multiple large-scale implementation projects across the United States.
- Ms. Ronning is a registered professional engineer in multiple states, a longtime member of IEEE, and Co-Chair of the INCOSE Telecommunications working group.

Emergency Services: Public Safety



Emergency Medical Services Communications Network

Manley, Thomas, Susan Ronning, and William Scheible. "Defining Critical Communications Networks: Modelling Networks as Systems."*INSIGHT*23, no. 2 (2020): 36-42

Example:

Emergency medical call from mobile phone service via commercial telephone system to public safety answering point to ambulance via voice radio and broadband data networks – This demonstrates multi-bearer networks in everyday occurrence

Emergency Services:
Wildland Fire - Public Notifications

Criticality Framework

Why use a Criticality Framework?

- Increased focus on making critical infrastructure (CI) more *resilient*
- Communications systems are *critical* for all CI

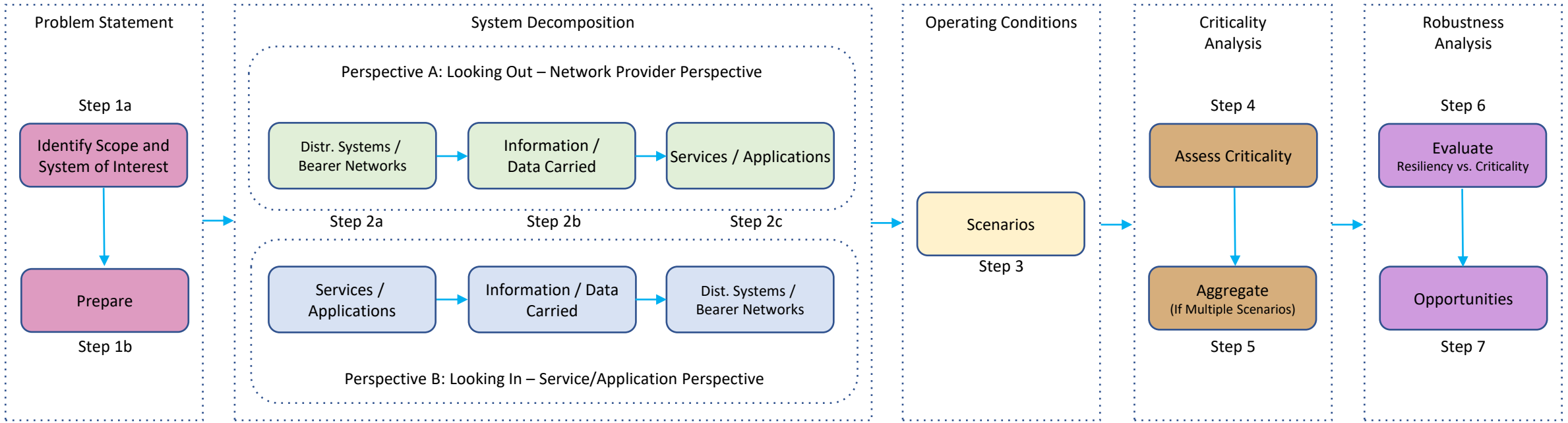
> U.S. efforts shall address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect this infrastructure's interconnectedness and interdependency. This directive also identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors. PPD-21

- Communications Networks are increasingly *complex*
- Need for guidance to model Communicans Networks (CN) as *systems*
- Need for guidance to drive *effective* investment decision making for improved resilience

Presidential Policy Directive -- Critical Infrastructure Security and Resilience (PPD-21)
https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

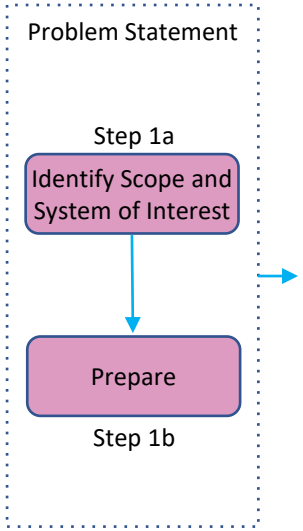
CN: Communications Network

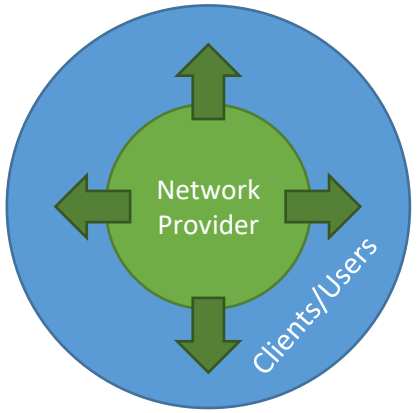
Criticality Framework



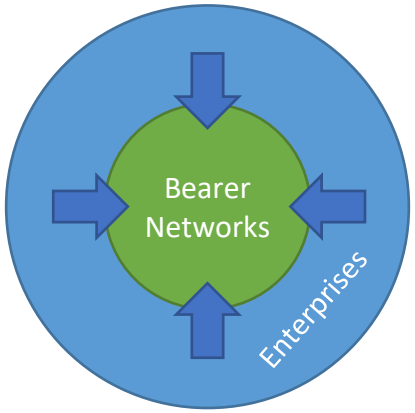
Applying the Framework – Step 1

- Problem Statement
  - **Step 1a:** Identify Scope and System of Interest
  - **Step 1b:** Determine Perspective (Network Provider = Looking Out, Enterprise = Looking In)

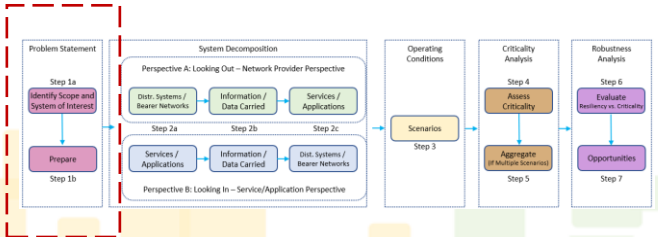




Network Provider Perspective
(Looking Out)

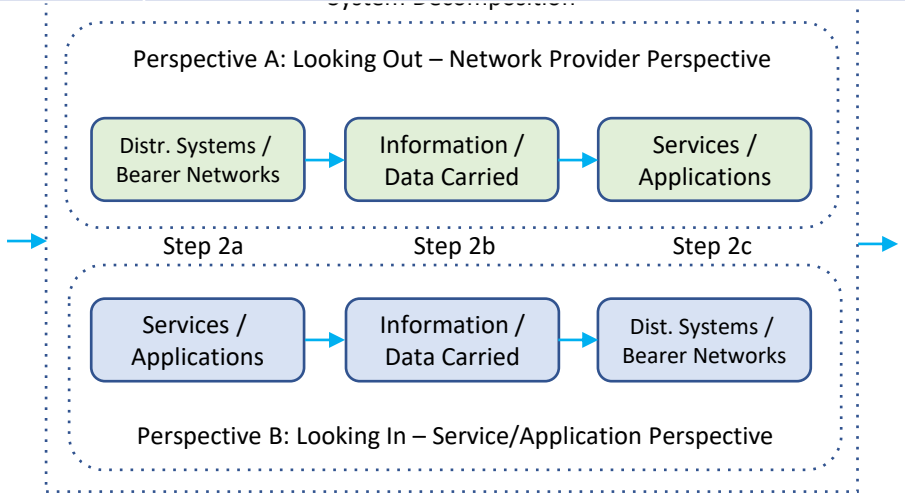


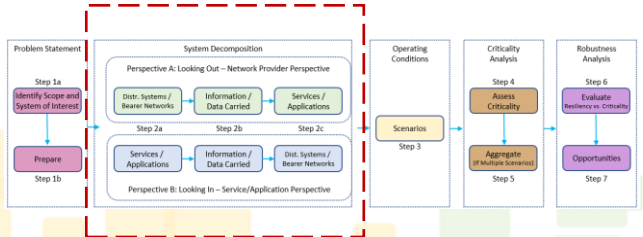
Enterprise Perspective
(Looking In)



Applying the Framework – Step 2

System Decomposition	Looking Out (Network Provider Perspective)	Looking In (Enterprise Perspective)
Step 2a	Identify each CN (BN/DS)	Identify each Service/Application
Step 2b	Identify Information/Data Carried (Information Exchanges)	Identify Information/Data Carried (Information Exchanges)
Step 2c	Determine Dependent Services/Applications	Determine Dependent CNs





(Looking Out) Step 2a → Step 2b → Step 2c

CN	Information Exchanges	Services/ Applications

Step 2c ← Step 2b ← Step 2a (Looking In)

BN: Bearer Network
DS: Distributed System

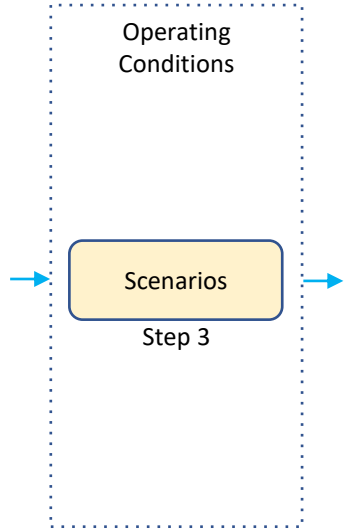
Applying the Framework – Step 3

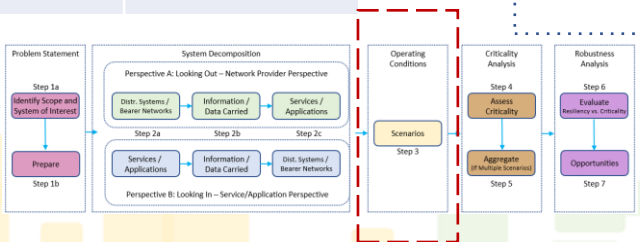
Operating Conditions:

- **Step 3:** Identify potential scenarios / operating conditions (*e.g. business as usual, emergency state, …).* While not all scenarios are predictable, a good set of diverse scenarios helps assess overall resiliency of larger system.

Step 3

CN	Scenario A	Scenario B	Scenario C	Scenario D
1				
2				
3				
4				





Transport scenarios:
fire/life safety incidents,
security incidents,
special operations events,
weather events, …)

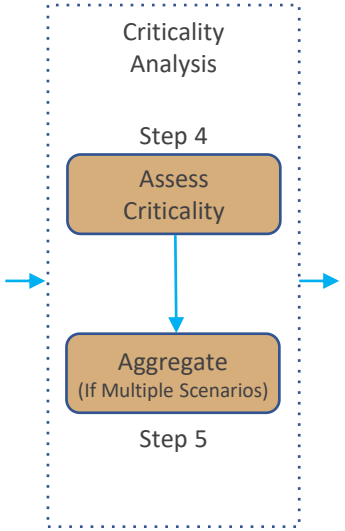
Applying the Framework – Steps 4 & 5

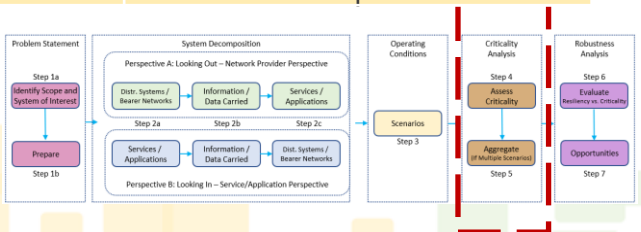
Criticality Analysis

- **Step 4:** Determine a criticality rating for each CN under each scenario. Note that the criticality of a CN is a function of the applications/services that are dependent upon it.
- **Step 5:** Aggregate the criticality ratings for each CN (*e.g. using a weighted average based on the likelihood of each scenario*)

Step 4 | Step 5

CN	Scenario A	Scenario B	Scenario C	Scenario D	Aggregate
1	5	5	5	5	5
2	1	1	1	1	1
3	2	3	2	1	2
4	4	3	3	3	3



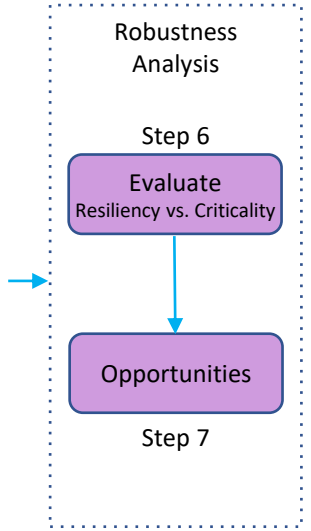


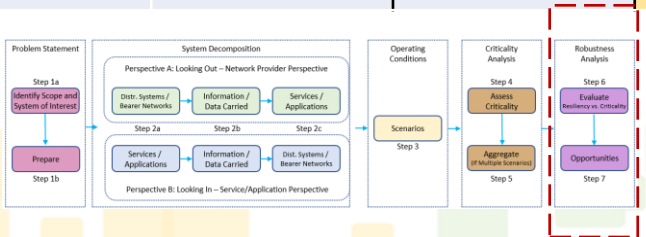
Applying the Framework – Steps 6 & 7

- Robustness Analysis
  - **Step 6:** Use systems analysis techniques (*e.g. FMECA, RAM*) to assess the degree of resilience of the CN and then compare that to the criticality of the CN.
  - **Step 7:** A heat map analysis can identify CNs that are insufficiently robust for their given criticality, and these can be considered as candidates for investment opportunities.

Step 7

CN	Scenario A	Scenario B	Scenario C	Scenario D	Aggregate	Resilience
1	5	5	5	5	5	3
2	1	1	1	1	1	2
3	2	3	2	1	2	2
4	4	3	3	3	3	2





FMECA: Failure Modes Effects & Criticality Analysis
RAM: Reliability, Availability, Maintainability

Network Provider Perspective: Pandemic

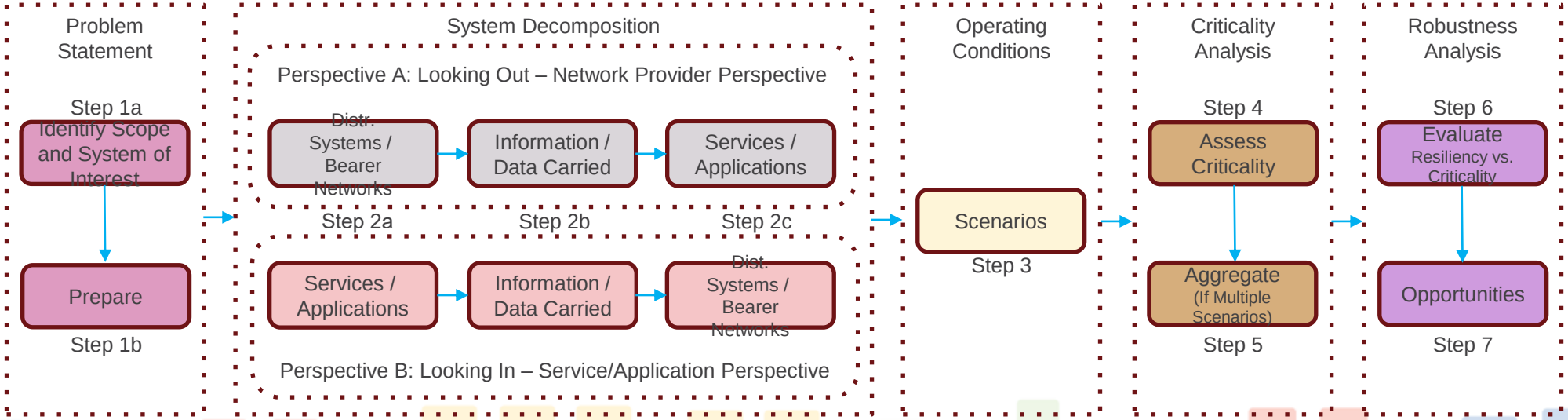
As a network provider, Internet service was not a critical service for residential customers before the pandemic... if the Internet went out, they had alternatives...

During the Pandemic, people couldn't leave their homes... and relied on their Internet for work, school, medical appointments, and socialization...

We saw an additional year worth of traffic growth overnight

Network demand increased at the same time it became critical for customers.

It was immediately clear that we needed to make sure we could quickly address congestion.



Application to Transport

Tailoring to Transport – Observations

- New services/applications e.g.
  - wireless Internet (Wi-Fi) for passengers
  - real-time access to rail information via 3rd party apps / websites
  - virtual/digital tickets (e.g. smartphones)
- Ongoing OT/IT convergence
- Increased reliance on multiple CNs (inc. Internet, public 4G/5G)

OT: Operational Technology

IT: Information Technology

Tailoring to Transport – Example Services/Applications

Fares
- Ticket sales
- Entry/Exit authorisation (e.g. access gates)
- Tag on/off

Customer Information
- Public announcements
- Electronic signage
- Route planner
- Real-time train schedules

Voice
- Emergency calling (e.g. distress buttons)
- Emergency services radio retransmission (e.g. in subway stations)
- Radio voice communication

Video

Security closed circuit television (CCTV)
Operational CCTV (e.g. train door closing)

Monitoring
- Location monitoring (e.g. bus location)
- Sensor monitoring (e.g. rail temperature)
- Intrusion detection (e.g. unauthorised entry into tunnels)

Supervisory Control and Data Acquisition (SCADA)
- Fire/Ventilation

Train Control
- Signalling
- Interlocking
- Automatic train protection (ATP)
- Automatic train operation (ATO)

Tailoring to Transport – Example Distributed Systems

- Ticketing System
- Customer Information System (e.g. Public Announcements, Electronic Signage)
- Location Monitoring System
- CCTV System(s)
- Intrusion Detection System
- Help Point Intercom
- Emergency Voice System
- Emergency Services Broadcast System
- Train Control System
- Enterprise-wide IP Network (i.e. interconnected Local Area Networks (LAN))
- Wireless LAN (WLAN) (e.g. local Wi-Fi access in stations or in trains)

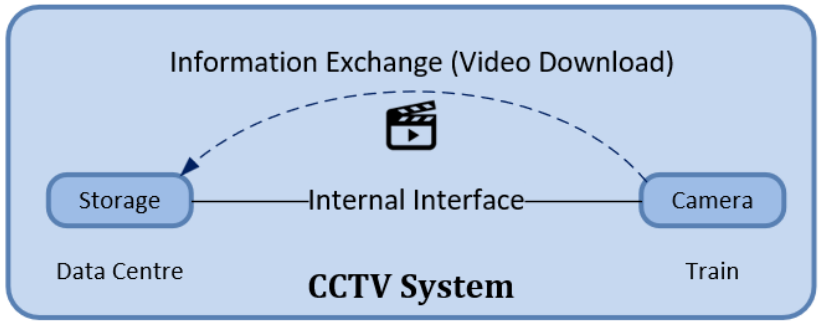
Tailoring to Transport – Example Bearer Networks

- Land Mobile Radio (RF)
- Public 3G/4G/5G Carrier Network(s)
- Agency-Owned Cellular (e.g. GSM-R, FRMCS)
- IPVPN
- Enterprise Wide Area Network (WAN)
- Optical Fibre Network
- Leased Lines (e.g. point-to-point carriage links)

FRMCS: Future Rail Mobile Communication System
IPVPN: Internet Protocol Virtual Private Network
GSM-R: Global System for Mobile Communications – Railway
RF: Radio Frequency

Tailoring to Transport – Step 2 Examples

- Service = CCTV Video Download

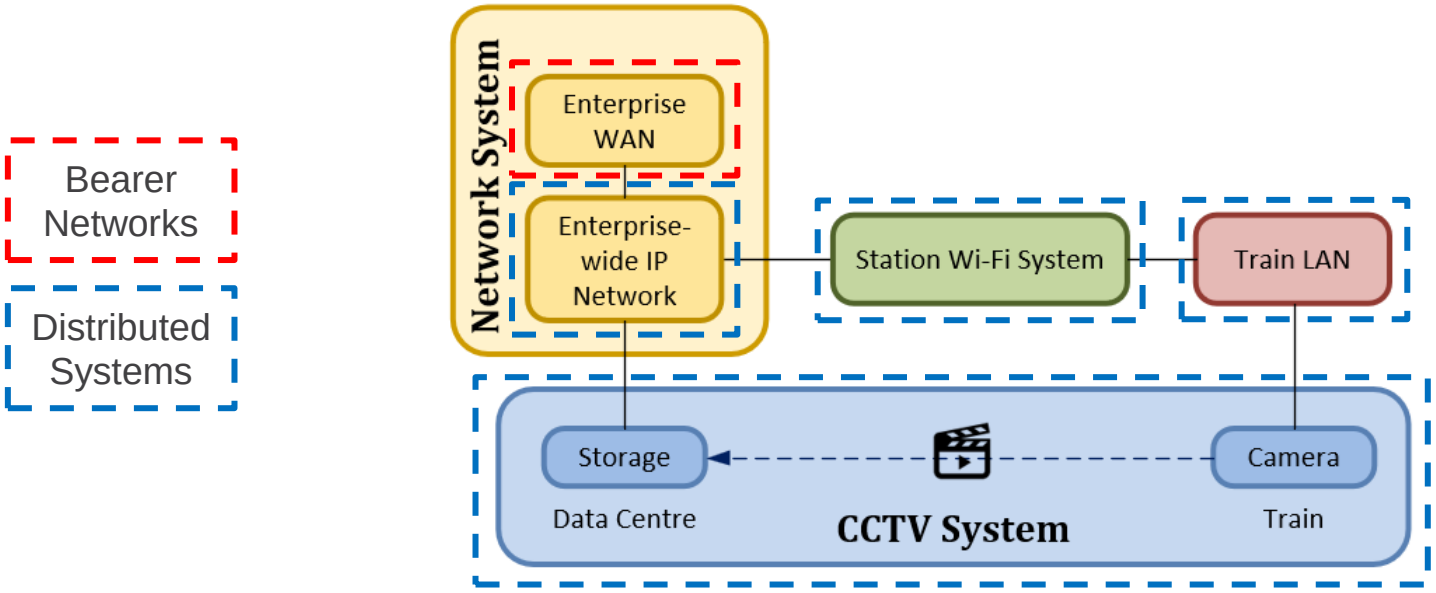


CCTV System Architecture

CCTV System Network Architecture

Tailoring to Transport – Step 2 Examples

- Service = CCTV Video Download

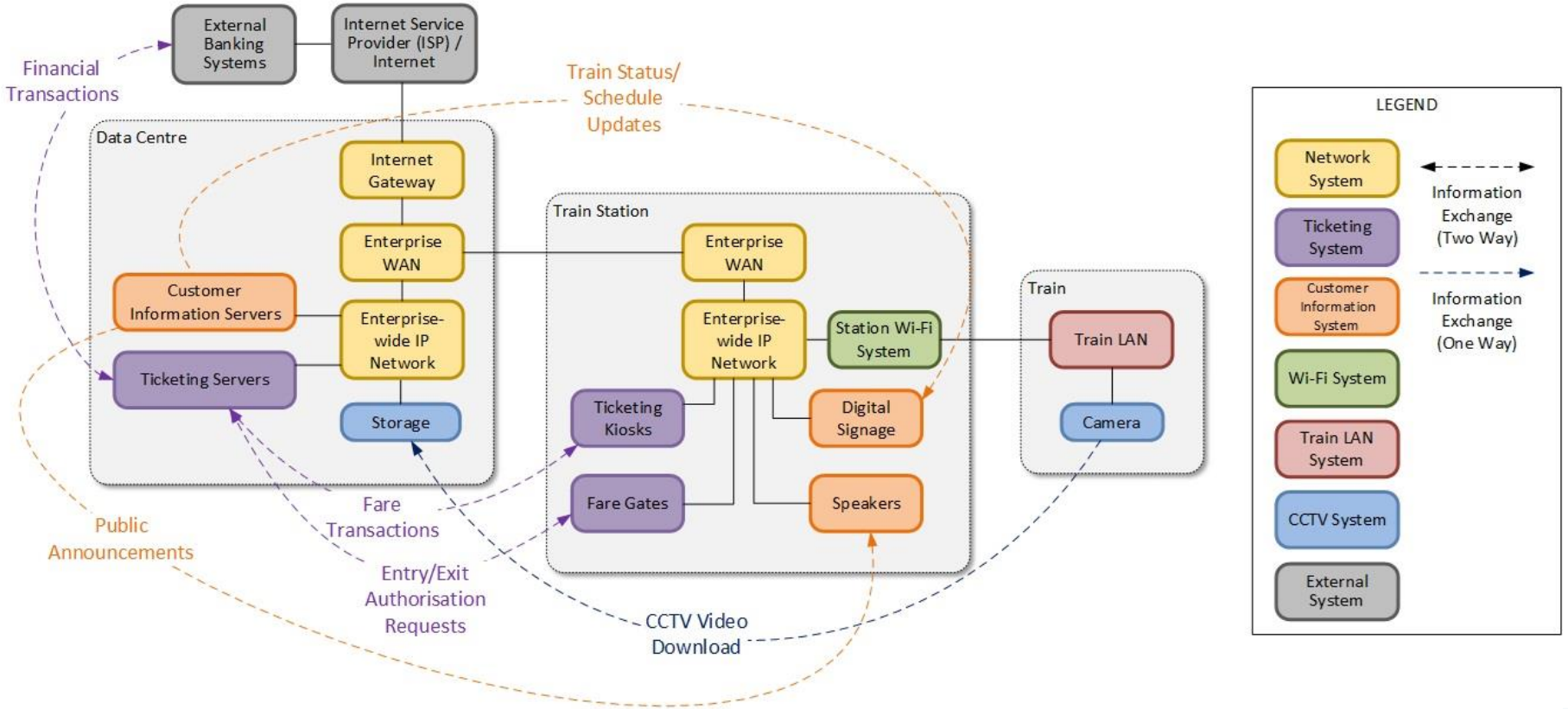


CCTV System Network Diagram

CCTV System Block Diagram

Tailoring to Transport – Step 2 Examples

- Information Exchanges – All



Reminder: 15:30 Tuesday Room 252
Communications Systems Primer: A Systems Engineer's Guide to Communications Networks: Modeling Networks as Systems

Discussion / Q&A

32nd Annual INCOSE international symposium

hybrid event

Detroit, MI, USA
June 25 - 30, 2022

www.incose.org/symp2022