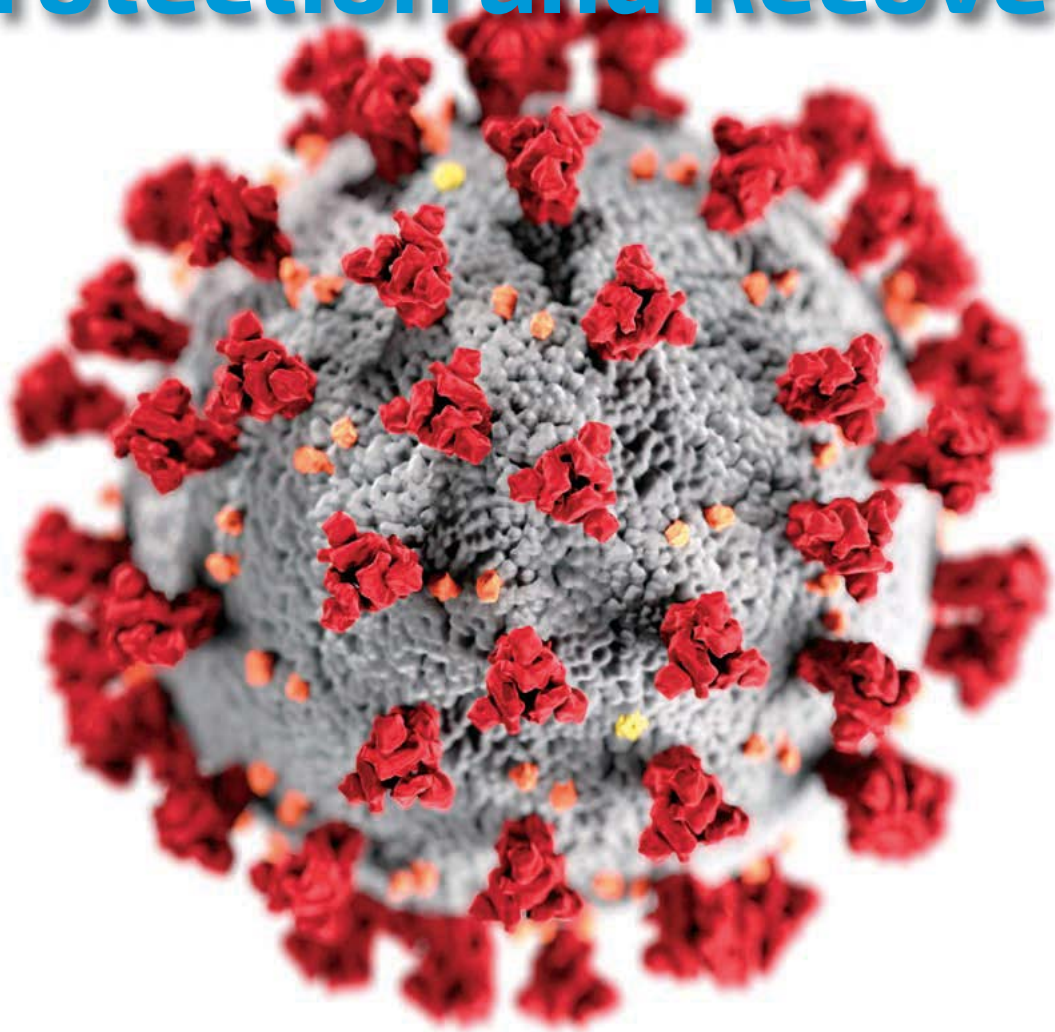


# INSIGHT

This Issue's Feature:  
**Critical Infrastructure  
Protection and Recovery**



**JUNE 2020**  
VOLUME 23 / ISSUE 2



This issue is sponsored by the Lockheed Martin Corporation.

**A PUBLICATION OF THE INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING**





**30<sup>th</sup>** Annual **INCOSE**  
international symposium

Virtual Event  
July 20 - 22, 2020







# Join us for the **30<sup>th</sup> Annual INCOSE International Symposium** and the **1<sup>st</sup> Virtual Edition**

## **SYSTEMS ENGINEERING FOR EARTH'S FUTURE**

Uniting Technology and Grand Challenges through Systems Engineering

### **The Premier International Systems Engineering Conference**

3 Days, 3 Tracks, 3 Keynotes, 70+ Presentations, Panels, and More!

<b>over 70</b>		<b>Papers, Presentations on Systems Engineering</b> Monday - Wednesday	
<b>3</b>		<b>Inspiring Keynote Speakers</b>	<b>Bernie Fanaroff</b> - Former Director Square Kilometer Array (SKA) Project Office <b>Dr. Ronnie S. McKenzie</b> - Managing Director, WRP <b>Jakob van Zyl</b> - Hydrosat, Inc.
<b>25</b>		<b>Countries Represented</b>	Argentina - Australia - Brazil - Canada - China - Finland - France - Germany - India - Ireland - Israel - Italy - Japan - Lithuania - Netherlands New Zealand - Norway - Singapore - South Africa - Sweden - Switzerland Thailand - Turkey - United Kingdom - United States
<b>19</b>		<b>Application Domains</b>	<b>Top Domains</b> Enterprise Systems Engineering - Defense - Aerospace - Academia - IT/Telecom - Environmental Systems - Automotive - Energy - Autonomous Systems - City Planning - Infrastructure
<b>38</b>		<b>Topics Represented</b>	<b>Top Topics</b> Systems Thinking - System Arch/Design Definition - MBSE - Needs and Req Definition - Processes - Systems of Systems - Complexity - Systems Science
<b>4</b>		<b>Panels</b> Monday - Wednesday	Including Topics Like These Discussed With Global Leaders in Systems Engineering <b>Aerospace - Systems Thinking - Defense - Diversity - System Security</b> <b>Teaching and Training - Cybernetics</b>

## **SPONSOR INCOSE IS 2020!**

- 1** Unique brand of recognition and visibility for your organization
- 2** Access to the latest thinking relevant to the practice of Systems Engineering
- 3** Put a spotlight on your organization's competency in Systems Engineering
- 4** Be associated with the highest culture of professionalism and innovation
- 5** Demonstrate organizational support to INCOSE's mission
- 6** Develop sustainable business relationships

**Lots of possibilities to interact with systems engineering communities**

Visit [www.incose.org/symp2020](http://www.incose.org/symp2020) and contact us **TODAY** - The IS2020 Organizing Team

# INSIGHT



A PUBLICATION OF THE INTERNATIONAL COUNCIL  
ON SYSTEMS ENGINEERING

JUNE 2020 VOLUME 23 / ISSUE 2

WHAT'S INSIDE  
THIS ISSUE

JUNE 2020  
VOLUME 23 / ISSUE 2

## Inside this issue

<b>FROM THE EDITOR-IN-CHIEF</b>	6
<b>SPECIAL FEATURE</b>	8
Toward Building a Failsafe Hospital: The Impending Drug Resistant Pandemic	8
Systems Theory Principles and Complex Systems Engineering Concepts for Protection and Resilience in Critical Infrastructure: Lessons from the Nuclear Sector	14
Use of SysML to Generate Failure Modes and Effects Analyses for Microgrid Control Systems	21
Microgrids —A Watershed Moment	32
Defining Critical Communications Networks: Modelling Networks as Systems	36
Emergency Systems and Power Outage Restoration Due to Infrastructure Damage from Major Floods and Disasters	43
Loss of Offsite Power Recovery Modeling in United States Nuclear Power Plants	56

# About This Publication

## INFORMATION ABOUT INCOSE

INCOSE's membership extends to over 18,000 individual members and more than 100 corporations, government entities, and academic institutions. Its mission is to share, promote, and advance the best of systems engineering from across the globe for the benefit of humanity and the planet. INCOSE chapters worldwide, includes a corporate advisory board, and is led by elected officers and directors.

For more information, click here:

[The International Council on Systems Engineering](http://TheInternationalCouncilonSystemsEngineering.com)  
([www.incose.org](http://www.incose.org))

## OVERVIEW

*INSIGHT* is the magazine of the International Council on Systems Engineering. It is published four times per year and features informative articles dedicated to advancing the state of practice in systems engineering and to close the gap with the state of the art. *INSIGHT* delivers practical information on current hot topics, implementations, and best practices, written in applications-driven style. There is an emphasis on practical applications, tutorials, guides, and case studies that result in successful outcomes. Explicitly identified opinion pieces, book reviews, and technology roadmapping complement articles to stimulate advancing the state of practice. *INSIGHT* is dedicated to advancing the INCOSE objectives of impactful products and accelerating the transformation of

systems engineering to a model-based discipline. Topics to be covered include resilient systems, model-based systems engineering, commercial-driven transformational systems engineering, natural systems, agile security, systems of systems, and cyber-physical systems across disciplines and domains of interest to the constituent groups in the systems engineering community: industry, government, and academia. Advances in practice often come from lateral connections of information dissemination across disciplines and domains. *INSIGHT* will track advances in the state of the art with follow-up, practically written articles to more rapidly disseminate knowledge to stimulate practice throughout the community.

## EDITORIAL BOARD AND STAFF

<b>Editor-In-Chief</b> insight@incose.org	William Miller +1 908-759-7110
<b>Assistant Editor</b> lisa@hsmcgroup.biz	Lisa Hoverman
<b>Theme Editor</b> mitchell.kerman@inl.gov	Mitchell Kerman
<b>Advertising Account Manager</b> dnicholas@wiley.org	Dan Nicholas +1 716-587-2181
<b>Layout and Design</b> chuck.eng@comcast.net	Chuck Eng
<b>Member Services</b> info@incose.org	INCOSE Administrative Office +1 858 541-1725

## 2020 INCOSE BOARD OF DIRECTORS

### Officers

**President:** Kerry Lunney, *ESEP, Thales Australia*  
**President-Elect:** Marilee Wheaton, *INCOSE Fellow, The Aerospace Corporation*

### At-Large Directors

**Academic Matters:** Bob Swarz, *WPI*  
**Marketing & Communications:** Lisa Hoverman, *HSMC*  
**Outreach:** Mitchell Kerman, *Idaho National Laboratory*  
**Americas Sector:** Antony Williams, *ESEP, Jacobs*  
**EMEA Sector:** Lucio Tirone, *CSEP, OCSMP, Fincantieri*  
**Asia-Oceania Sector:** Serge Landry, *ESEP, Consultant*  
**Chief Information Officer (CIO):** Bill Chown, *BBM Group*  
**Technical Director:** David Endler, *CSEP, Systems Engineering Consultant*

**Secretary:** Kayla Marshall, *CSEP, Lockheed Martin Corporation*  
**Treasurer:** Michael Vinarcik, *ESEP, SAIC*

**Deputy Technical Director:** Christopher Hoffman, *CSEP, Cummins*

**Technical Services Director:** Don Gelosh, *WPI*

**Director for Strategic Integration:** Tom McDermott,

*Stevens Institute of Technology*

**Corporate Advisory Board Chair:** Don York, *CSEP, SAIC*

**CAB Co-chair:** Ron Giachetti, *Naval Postgraduate School*

**Chief of Staff:** Andy Pickard, *Rolls Royce Corporation*

## PERMISSIONS

\* PLEASE NOTE: If the links highlighted here do not take you to those web sites, please copy and paste address in your browser.

### Permission to reproduce Wiley journal Content:

Requests to reproduce material from John Wiley & Sons publications are being handled through the RightsLink® automated permissions service.

### Simply follow the steps below to obtain permission via the Rightslink® system:

- Locate the article you wish to reproduce on Wiley Online Library (<http://onlinelibrary.wiley.com>)
- Click on the 'Request Permissions' link, under the 'ARTICLE TOOLS' menu on the abstract page (also available from Table of Contents or Search Results)
- Follow the online instructions and select your requirements from the drop down options and click on 'quick price' to get a quote
- Create a RightsLink® account to complete your transaction (and pay, where applicable)
- Read and accept our Terms & Conditions and download your license
- For any technical queries please contact [customercare@copyright.com](mailto:customercare@copyright.com)
- For further information and to view a Rightslink® demo please visit [www.wiley.com](http://www.wiley.com) and select Rights & Permissions.

**AUTHORS** – If you wish to reuse your own article (or an amended version of it) in a new publication of which you are the author, editor or co-editor, prior permission is not required (with the usual acknowledgements). However, a formal grant of license can be downloaded free of charge from RightsLink if required.

### Photocopying

Teaching institutions with a current paid subscription to the journal may make multiple copies for teaching purposes without charge, provided such copies are not resold or copied. In all other cases, permission should be obtained from a reproduction rights organisation (see below) or directly from RightsLink®.

### Copyright Licensing Agency (CLA)

Institutions based in the UK with a valid photocopying and/or digital license with the Copyright Licensing Agency may copy excerpts from Wiley books and journals under the terms of their license. For further information go to CLA.

### Copyright Clearance Center (CCC)

Institutions based in the US with a valid photocopying and/or digital license with the Copyright Clearance Center may copy excerpts from Wiley books and journals under the terms of their license, please go to CCC.

**Other Territories:** Please contact your local reproduction rights organisation. For further information please visit [www.wiley.com](http://www.wiley.com) and select Rights & Permissions.

If you have any questions about the permitted uses of a specific article, please contact us.

### Permissions Department – UK

John Wiley & Sons Ltd.  
The Atrium,  
Southern Gate,  
Chichester  
West Sussex, PO19 8SQ  
UK  
Email: [Permissions@wiley.com](mailto:Permissions@wiley.com)  
Fax: 44 (0) 1243 770620  
or

### Permissions Department – US

John Wiley & Sons Inc.  
111 River Street MS 4-02  
Hoboken, NJ 07030-5774  
USA  
Email: [Permissions@wiley.com](mailto:Permissions@wiley.com)  
Fax: (201) 748-6008

## ARTICLE SUBMISSION

[INSIGHT@incose.org](mailto:INSIGHT@incose.org)

**Publication Schedule.** *INSIGHT* is published four times per year.

Issue and article submission deadlines are as follows:

- March 2020 issue – 2 January
- June 2020 issue – 2 April
- September 2020 issue – 1 July
- December 2020 issue – 1 October

### © 2020 Copyright Notice.

Unless otherwise noted, the entire contents are copyrighted by INCOSE and may not be reproduced in whole or in part without written permission by INCOSE. Permission is given for use of up to three paragraphs as long as full credit is provided. The opinions expressed in

*INSIGHT* are those of the authors and advertisers and do not necessarily reflect the positions of the editorial staff or the International Council on Systems Engineering.  
ISSN 2156-485X; (print) ISSN 2156-4868 (online)

For further information on submissions and issue themes, visit the INCOSE website: [www.incose.org](http://www.incose.org)

**ADVERTISE**

**Readership**

*INSIGHT* reaches over 18,000 individual members and uncounted employees and students of more than 100 CAB organizations worldwide. Readership includes engineers, manufacturers/purchasers, scientists, research & development professionals, presidents and CEOs, students and other professionals in systems engineering.

Issuance	Circulation
2020, Vol 23, 4 Issues	100% Paid

**Contact us for Advertising and Corporate Sales Services**

We have a complete range of advertising and publishing solutions professionally managed within our global team. From traditional print-based solutions to cutting-edge online technology the Wiley-Blackwell corporate sales service is your connection to minds that matter. For an overview of all our services please browse our site which is located under the Resources section. Contact our corporate sales team today to discuss the range of services available:

- Print advertising for non-US journals
- Email Table of Contents Sponsorship
- Reprints
- Supplement and sponsorship opportunities
- Books
- Custom Projects
- Online advertising

Click on the option below to email your enquiry to your nearest office:

- Asia & Australia [corporatesalesaustralia@wiley.com](mailto:corporatesalesaustralia@wiley.com)
- Europe, Middle East & Africa (EMEA) [corporatesaleseurope@wiley.com](mailto:corporatesaleseurope@wiley.com)
- Japan [corporatesalesjapan@wiley.com](mailto:corporatesalesjapan@wiley.com)
- Korea [corporatesaleskorea@wiley.com](mailto:corporatesaleskorea@wiley.com)

**USA (also Canada, and South/Central America):**

- Healthcare Advertising [corporatesalesusa@wiley.com](mailto:corporatesalesusa@wiley.com)
- Science Advertising [Ads\\_sciences@wiley.com](mailto:Ads_sciences@wiley.com)
- Reprints [Commercialreprints@wiley.com](mailto:Commercialreprints@wiley.com)
- Supplements, Sponsorship, Books and Custom Projects [busdev@wiley.com](mailto:busdev@wiley.com)

**Or please contact:**

Dan Nicholas, Associate Director – Sciences, Corporate Sales  
 Wiley  
 PHONE: +1 716-587-2181  
 E-MAIL: [dnicholas@wiley.com](mailto:dnicholas@wiley.com)

**CONTACT**

Questions or comments concerning:

**Submissions, Editorial Policy, or Publication Management**

*Please contact:* William Miller, Editor-in-Chief  
[insight@incose.org](mailto:insight@incose.org)

**Advertising—please contact:**

Dan Nicholas, Associate Director  
 Sciences, Corporate Sales  
 PHONE: +1 716-587-2181  
 E-MAIL: [dnicholas@wiley.com](mailto:dnicholas@wiley.com)

**Member Services – please contact:** [info@incose.org](mailto:info@incose.org)

**ADVERTISER INDEX**

June volume 23-2

IS2020	inside front cover
Caltech	7
<i>Systems Engineering Call for Papers</i>	back inside cover
INCOS certification	back cover

*INSIGHT volume 23, no. 2 is sponsored by the Lockheed Martin Corporation.* **LOCKHEED MARTIN** 

**CORPORATE ADVISORY BOARD – MEMBER COMPANIES**

321 Gang, Inc.  
 Aerospace Corporation, The  
 Airbus  
 Airbus Defense and Space  
 AM General LLC  
 Analog Devices, Inc.  
 Analytic Services  
 Aras Corp  
 Australian Department of Defence  
 Aviation Industry Corporation of China, Ltd  
 BAE Systems  
 Bechtel  
 Boeing Company, The  
 Bombardier Transportation  
 Booz Allen Hamilton Inc.  
 C.S. Draper Laboratory, Inc.  
 CACI International, Inc.  
 Carnegie Mellon University Software Engineering Institute  
 Change Vision, Inc  
 Colorado State University  
 Cornell University  
 Cranfield University  
 Cubic Corporation  
 Cummins, Inc.  
 CYBERNET MBSE  
 Defense Acquisition University  
 DENSO Create, Inc.  
 Drexel University  
 Eindhoven University of Technology  
 Embraer S.A.  
 ENAC  
 Federal Aviation Administration (U.S.)  
 Ford Motor Company  
 Fundacao Ezute  
 General Dynamics  
 General Motors  
 George Mason University  
 Georgia Institute of Technology  
 IBM

Idaho National Laboratory  
 ISAE SUPAERO  
 ISDEFE  
 ISID Engineering, LTD  
 iTiD Consulting, Ltd  
 Jacobs Engineering  
 Jama Software  
 Jet Propulsion Laboratory  
 John Deere & Company  
 Johns Hopkins University  
 KBR, Inc.  
 KEIO University  
 L3 Harris  
 Leidos  
 Lockheed Martin Corporation  
 Los Alamos National Laboratory  
 ManTech International Corporation  
 Maplesoft  
 Massachusetts Institute of Technology  
 MBDA (UK) Ltd.  
 Missouri University of Science & Technology  
 MITRE Corporation, The  
 Mitsubishi Aircraft Corporation (Mitsubishi Heavy Industries Group)  
 National Aeronautics and Space Administration  
 National Security Agency - Enterprise  
 Naval Postgraduate School  
 Nissan Motor Co, Ltd  
 No Magic/Dassault Systems  
 Noblis  
 Northrop Grumman Corporation  
 Penn State University  
 Perspecta (formerly Vencore)  
 Prime Solutions Group, Inc.  
 Project Performance International  
 Raytheon Corporation  
 Roche Diagnostics  
 Rolls-Royce  
 Saab AB  
 Safran Electronics and Defence

SAIC  
 Sandia National Laboratories  
 Shell  
 Siemens  
 Sierra Nevada Corporation  
 Singapore Institute of Technology  
 Skoltech  
 SPEC Innovations  
 Stellar Solutions  
 Stevens Institute of Technology  
 Strategic Technical Services  
 Swedish Defence Materiel Administration  
 Systems Engineering Directorate  
 Systems Planning and Analysis  
 Thales  
 TNO  
 Trane Technologies  
 Tsinghua University  
 TUS Solution LLC  
 UK MoD  
 United Technologies Corporation  
 University of Arkansas  
 University of California San Diego  
 University of Connecticut  
 University of Maryland  
 University of Maryland, Baltimore County  
 University of Michigan, Ann Arbor  
 University of New South Wales, The, Canberra  
 University of Southern California  
 University of Texas at Dallas  
 University of Texas at El Paso, The  
 US Department of Defense, Deputy Assistant Secretary of Defense for Systems Engineering,  
 Veoneer, Inc  
 Vitech Corporation  
 Volvo Construction Equipment  
 Woodward Inc  
 Worcester Polytechnic Institute- WPI  
 Zuken, Inc



# Defining Critical Communications Networks: Modelling Networks as Systems

Thomas Manley, [thomas@manley.name](mailto:thomas@manley.name); Susan Ronning, [s.ronning@adcomm911.com](mailto:s.ronning@adcomm911.com); and William Scheible, [wscheible@mitre.org](mailto:wscheible@mitre.org)

Copyright © 2020 by Thomas Manley, Susan Ronning, and William Scheible. Published and used by INCOSE with permission.

## ■ ABSTRACT

As a society, we have become exceedingly dependent on our communication devices and the infrastructure networks supporting them. Even short duration network outages can result in chaos within public transport systems (air traffic control of commercial flights, traffic signaling of rail networks); disrupt financial systems (electronic payments, stock market transactions); and reduce business productivity (phone and email). It can also have the potential for loss of life: field utility workers communicating remotely with dispatch controllers to de-energize and re-energize lines for repair; law enforcement field personnel communicating needs for crowd control during riots; and alerting the public about dam breaches through emergency notification systems.

This article helps explain what critical communications networks are, where these networks fit within a systems-of-systems context, and what other systems must also be resilient, redundant, and reliable to ensure communication networks can continue to operate as designed. It also introduces systems engineering principles, techniques, and approaches that we can use to aid in the design of critical wireless and wireline communications networks for normal day-to-day operations, and for the protection and recovery of those networks during service disruptions caused by man-made and natural events.

■ **KEYWORDS:** telecommunications; wireless; telephone; 9-1-1; emergency communications; critical infrastructure; PPD-21; networks; voice; data; communications impacts; critical systems design; nodes

## COMMUNICATIONS NETWORKS AS ENABLING SYSTEMS

An enterprise's core business may provide: a market for exchanging stocks (financial); electricity to business and residential customers (utilities); transportation of people or things from one place to another (railways, airplanes); or law enforcement and fire-fighting services (public safety). Communications networks underpin almost every business, government agency, and non-government organization. Networks must transport an exchange of information, be it voice or data, from one location to another to enable performance of the enterprise's core functions.

A given communications network often serves several different types of users in many different capacities. For instance, private citizens typically use the same cel-

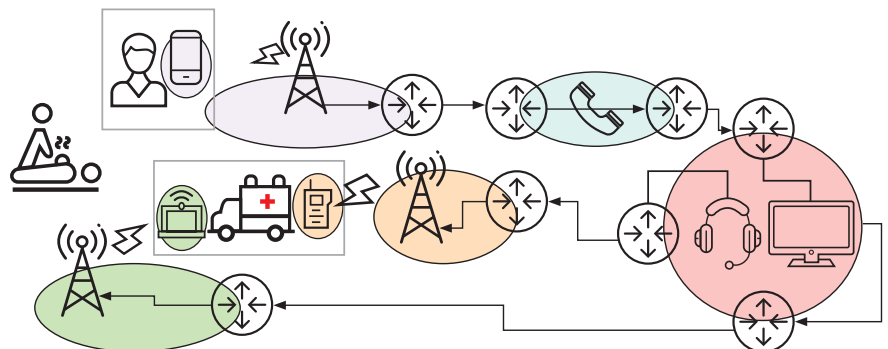


Figure 1. Emergency medical call from mobile phone service via commercial telephone system to public safety answering point to ambulance via voice radio and broadband data networks, demonstrating multibearer networks in everyday occurrence

lular phone services for text messaging that they also use to make emergency calls to request police and fire services; ambulances may use this same cellular phone service

for automated vehicle location mapping to determine the closest ambulance to a casualty (figure 1). Other multiuser examples include satellite-based voice calls made

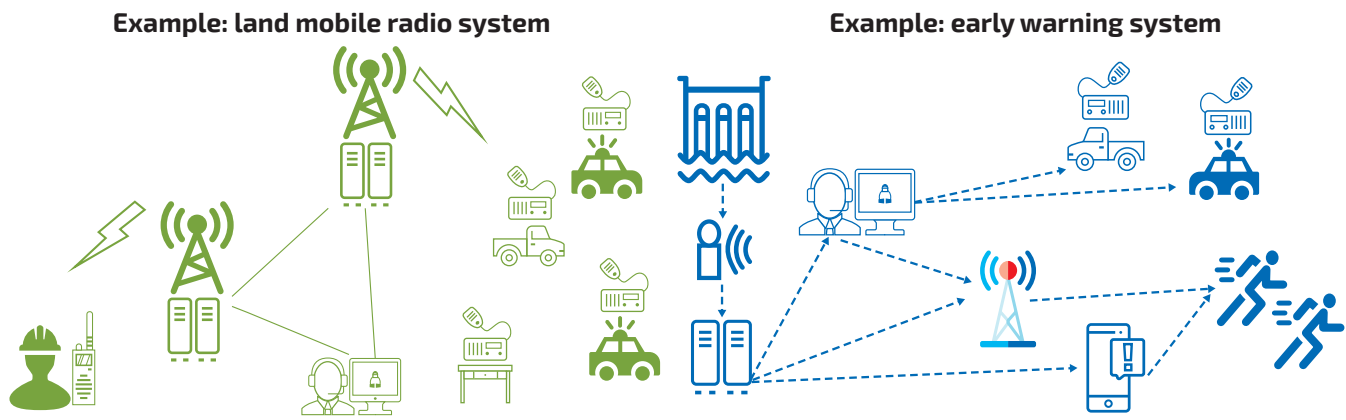


Figure 2. Two different examples of critical communications networks

from a cruise ship to the mainland, line-of-sight simplex radio transmissions between a helicopter and the ground crew guiding a pilot during landing, and a wireless access point providing data communications to multiple wireless devices in a home.

The US Department of Homeland Security's Communications Sector-Specific Plan (CSSP) (2019) states, "Since 2010, the communications sector has evolved rapidly in multiple areas, including mobile broadband, cloud computing, the Internet of Things (IoT), and software-defined networks (SDNs). Voice and data networks have continued to converge, and mobile devices, such as smartphones and tablet computers, have been widely adopted, creating enormous demand for mobile broadband communications." Although this has reduced the number of single purpose networks required, it is now more difficult to understand the criticality of the resulting networks that have replaced them.

#### What is a Communications Network?

A communications network may be made up of a collection of systems, integrated and interacting with one another (figure 2). The communications network system of interest may include mobile and fixed transceiver equipment. Supporting systems can include antennas and filters, primary and/or backup power, physical mounts, routers and switches, device management and alarm notification, end user interfaces, and the transport networks (or links). They can include subscriber devices like handheld cell phones and portable radios; radios installed inside vehicles, airplanes, or satellites; IoT devices; and fixed transceiver units (base stations and their antenna systems) which engineers may install inside buildings, on towers, or on satellites orbiting the earth. They can also include applications running over the network, such as email systems, video conferencing systems, and contact center systems.

All these systems must work together

in concert to relay the information from one location to another. Engineers must first define, design, procure, and configure each individual system to work within their own domain, and then, when integrated with each other, support the network as a whole. And, engineers must design each—individually and together—to withstand potential failures.

#### APPLYING SYSTEMS ENGINEERING TO COMMUNICATIONS NETWORKS

To apply systems engineering knowledge to the design and support of communications networks, there is a need to model communications networks as systems. Yet, there is very limited guidance as to how to do this. While industries often use the terms system and network interchangeably in relation to communications networks, in practice, it can be very difficult to define system boundaries or the internal and external interfaces of communications networks as the network topology can be constantly changing. As a result, the effects of localized failures are often very difficult to predict, so performing techniques such as failure mode, effects, and criticality analysis (FMECA) can be challenging. This is increasingly the case for critical communications networks as these are often larger and more complex.

If it is possible to describe a network as a system, then we can unlock the tools in the systems engineer's toolkit to add value to both the design and support of the network. FMECA and reliability, availability, and maintainability (RAM) analysis are two such techniques that may assist engineers to assess the resiliency of a communications network qualitatively and quantitatively. Similarly, the ability to identify and label components that we may find in many places across the network, for example, switches and routers, can facilitate configuration management as well as assist in the allocation of requirements and con-

struction of architecture descriptions. What follows is guidance on how to approach the modelling of communications networks as systems. Note that while this is focused on, and intended for, critical communications networks, it is applicable to all communications networks.

#### Nodes and Links

Engineers often represent communications networks graphically as a set of nodes (geographical locations where information communications technology [ICT] services are delivered) connected by links (interfaces between two or more nodes). While this approach obfuscates much of the detail of the network (for instance, it assumes a single homogeneous network where any information can potentially flow from any node to any other node), it does provide a high-level representation of the structure of the network and therefore provides a useful starting point for exploration. Note that a node can itself contain an inner network, which can be comprised of lower level nodes in much the same way a system can be comprised of subsystems. Hence nodal recursion is also possible.

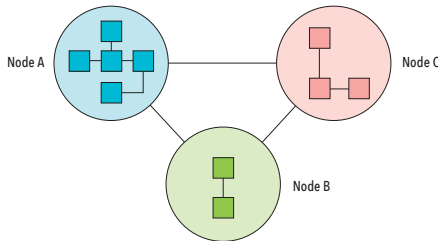
Nodes can be a fixed site, such as a building or university campus. They may also consist of environmental sensors, cellular base stations, geo-stationary satellites, or automated farm gates. Nodes may also be mobile, such as vehicles that move on the ground, under the sea, in the air, or in space. They may also consist of wearable devices on people and animals, or consist of a network of unmanned autonomous vehicles (UAV) that may even include weapons in military applications.

The key is that there may be communication within nodes (intranode) and between nodes (internode) (Syed, Pong, and Hutchinson 2017). In this way, we can think of a large office housing thousands of individuals as a single node connected to other nodes via links, obfuscating the

complexity of the network within the office itself. It is in this context that they are most useful for modelling complex communications networks.

### Nodal Types

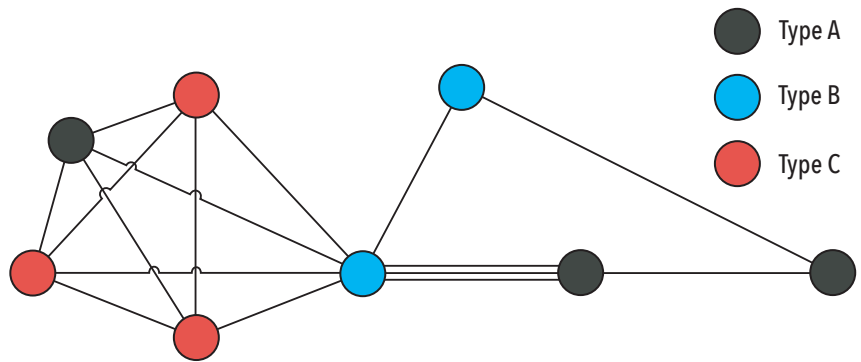
We can treat each node as a distinct nodal system, with external interfaces to other nodal systems and internal interfaces between the system elements within it (see figure 3). For networks with many nodes, though (and particularly those networks with large nodes such as offices), each node would have its own unique internal design and this could quickly become difficult to manage (and support).



**Figure 3.** Example nodes showing internal and external structure with i) internode links/external interfaces and ii) intranode links/internal interfaces

The use of nodal types (where each instance of a nodal type shares a common architecture) can simplify the effort of designing and supporting each node, since this reduces the number of unique nodes and allows for the use of templates (or design patterns), as illustrated in figure 4. We can then place these patterns under configuration control to maintain consistency between each instance of each nodal type.

To create a set of nodal types, we can group nodes together in various ways. While there are many different ways to group nodes, how we group them can affect the degree of difference between nodes within a nodal type and the management effort to support them. Careful selection of the characteristics that define each nodal type is therefore important. For instance, scale is often a distinguishing characteristic, with an organization having offices configured for different office sizes based on the number of employees located there (large, medium, and small). These are candidates for nodal types. However, if the functionality (or services) that each node provides differs in more than the size (a factory may have a similar number of workers to an office, yet very different ICT needs, while a data center may have very few staff or none at all) then functionality may be a more effective characteristic to select. The following proposed principles may aid in defining a useful set of nodal types.



**Figure 4.** Node topology diagram with multiple instances of three nodal types (A, B, and C). In this case, there are three distinct links between the middle blue and black nodes.

### Nodal Type Principles:

1. Functionality is more important than scale in distinguishing nodal types, that is, group nodes with common functionality into a nodal type before size;
2. Engineers should minimize the number of nodal types to reduce operational complexity and configuration management;
3. Nodal types should include sufficient granularity of services such that nodes do not provide services that are not required, such as the minimum required services;
4. Nodal type variants can be used to cater for lower level differences between nodes of the same nodal type including the modular addition (or removal) of supplementary services, for example, a manufacturer can fit the same model vehicle with manual or automatic transmission, or add roof racks.

### SYSTEMS OF SYSTEMS

While systems engineering normally focus on the design of individual systems, the concept of systems of systems engineering (SOSE) was created in part to deal with the complexity arising from the existence of many independent systems interacting with each other for a common purpose, so systems engineers can usefully apply it to networks (Maier, 1998).

From the *Systems Engineering Handbook* (Walden et al. 2015, 8), systems of systems (SoS) tend to have the following characteristics which help distinguish them from ordinary systems:

- operational independence of constituent systems;
- managerial independence of constituent systems;
- geographical systems;
- emergent behavior; and
- evolutionary development processes.

The “Systems of Systems Primer” (INCOSE 2018) expands on managerial

independence by positing that one of the challenges of SoS is that constituent systems “may withdraw (possibly without warning) from the SoS,” implying that this is not an option available to a subsystem of an ordinary system.

We can think of communications networks as SoSs where nodes are systems that can (in theory at least) join or leave the network at will. Communications networks, however, are a special case of SoS and also tend to exhibit the following set of proposed characteristics. Additional characteristics of communications networks include:

- common purpose, that is, to facilitate communication within and between nodes;
- commonality of architecture (many nodes may be instances of the same node type and therefore share the same design);
- strong interdependence of constituent systems (certain failures within a particular node may cause other nodes to become isolated/disconnected);
- large in scale (hundreds, or even thousands of nodes); and
- a strong focus on traffic flows through a network rather than the interfaces within it.

### DUAL NATURE OF SOLUTION ELEMENTS

The problem then arises when we share technology solutions between nodal types; in other words, where the engineer reuses a solution element (being simply an element of a solution) as a building block in multiple nodal type designs. How does the engineer manage these solution elements, given that they may be part of multiple nodal type designs, and changing the design for one may necessitate changing it for all other instances of it?

Another problem is that due to the deliberate logical separation of certain downstream networks, often involving encryption, different network domains may



be transported over a common wide area network (WAN). This gives rise to functional systems that engineers can overlay on top of a subset of nodes, either as:

- bearer networks (those functional systems whose main purpose is to connect nodes, for example, a WAN); or
- distributed systems (systems whose elements operate together irrespective of geographical distribution, or are at least managed as one system).

The implication is that solution elements (as building blocks of a nodal system) may simultaneously be a subsystem of a node as well as a subset of a functional system. This dual nature of a solution element is a unique property of communications networks that requires new thinking.

We demonstrate these constructs in figure 5 where section A illustrates a generic network topology of three sites (A, B, and C) that we then refine to section B through the allocation of solution elements to various bearer networks and distributed systems and the identification of nodal types (X and Y). We show the resulting simplified system block diagram in section C. Note that while there are two instances of nodal type X, only one is shown in the system block diagram.

Interestingly, nodal systems appear to meet the SoS criteria of “operational independence of the components” that Maier proposed (1998), since the network as a whole can survive the losses of some nodes; we cannot necessarily say the same for functional systems. For instance, distributed systems may be critically dependent on bearer systems. As such, we can think of nodal systems as forming SoSs, yet this may not be true for functional systems.

#### Links Belonging to Different Networks

Since it is possible for a node to contain multiple downstream functional systems, it is also possible for links to belong to distinct bearer networks to distinguish them from the broader network construct. A node, therefore, could connect to multiple different bearer networks using a different link for each, though the node may or may not function as a gateway between two bearer networks. That is, there may still be isolation between bearer networks, meaning that data cannot flow between them. This is often the case with commercial or military vehicles that can use multiple networks operating in different parts of the electromagnetic spectrum, for example, high frequency (HF) for beyond line of sight (BLOS), very high frequency (VHF) or ultra-high frequency (UHF) for line of sight (LOS), and satellite communication (SATCOM). While all bearer networks may

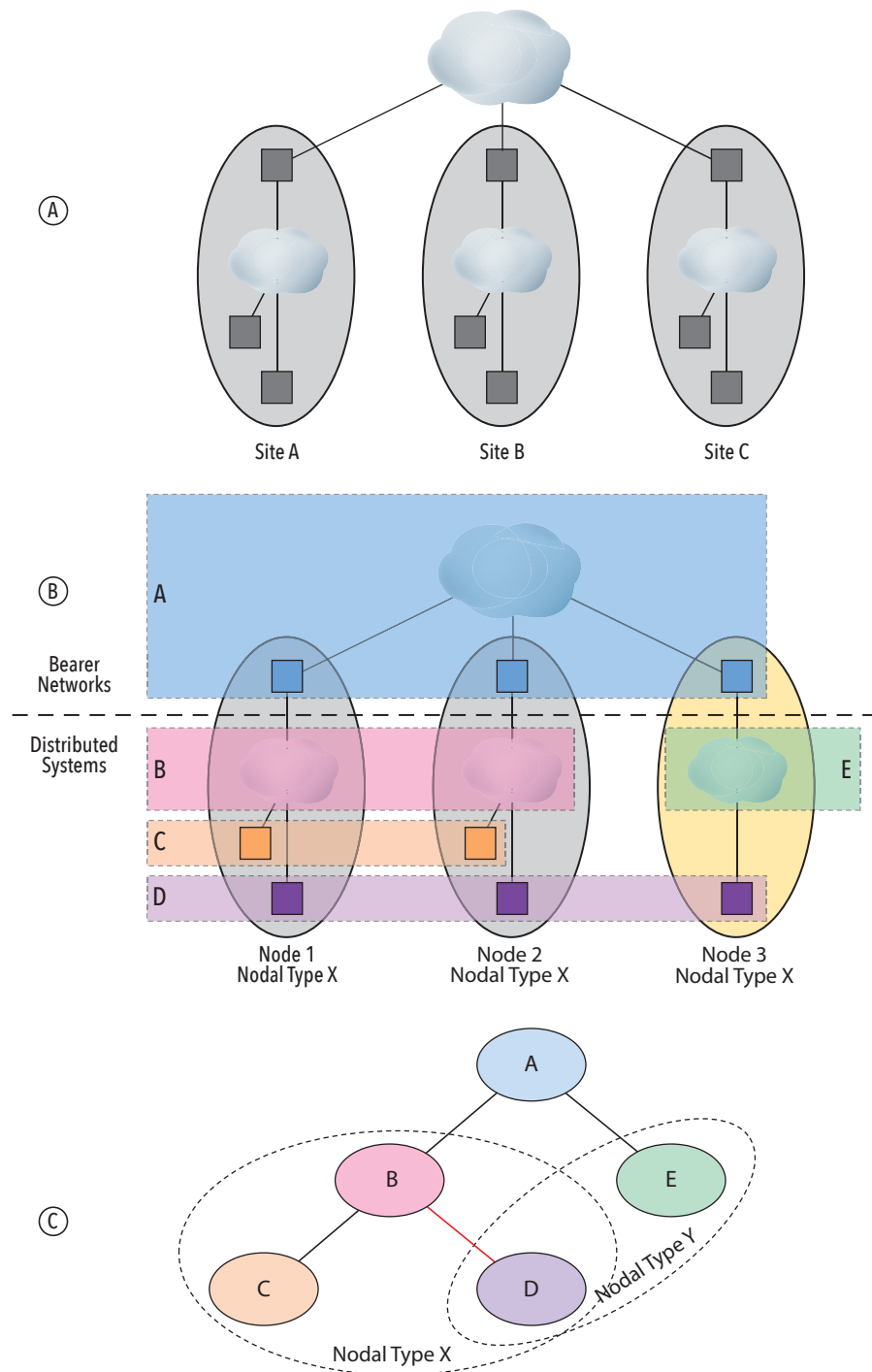


Figure 5. A) a generic network topology of three sites (A, B, and C); B) the same topology allocating components to bearer networks and distributed systems and distinguishing nodal types; and C) the resulting simplified systems block diagram

be available for use at any time (assuming they are not out of range), they may not all be used at the same time. For instance, we might only use voice communications when required, since it could be difficult to listen to multiple voice networks at the same time. Geographical location and the bearer networks that the other party/parties (that the user needs to talk to) have available to them (civilian emergency services

networks) may determine the selection of which bearer network to use (and when).

The implication of different links on the same node belonging to different bearer networks is that a physical node may actually be the collocation of multiple virtual nodes (where there is little or no connectivity between the virtual nodes). This is evident in figure 6 where the red and blue nodes (A) are physical nodes that

consist of four and three virtual nodes respectively (B). Because the virtual nodes do not interconnect, there are effectively four distinct networks (green, yellow, purple, and orange), and each link belongs to only one of these bearer networks (C). Traffic cannot flow between these networks without some form of interconnection, for example, a gateway.

**Matrix Approach**

We can treat bearer networks, nodes, and functional systems as systems each in their own right (figure 7), and they can coexist as independent conceptual constructs. However, they each have different frames of reference, and therefore we should take care when considering interfaces between them. For instance, nodes interface externally to bearer networks (and through them other nodes) whilst building blocks (solution elements of functional systems) form a part of a node. Building blocks have interfaces to other building blocks within the same node and may also have logical interfaces across nodes forming a common functional system, for example, a wireless LAN controller (WLC) on one node may control the wireless access points (WAP) at a different node.

**CRITICAL OR NOT?**

Today’s systems engineers are well advised to consider the impact of critical

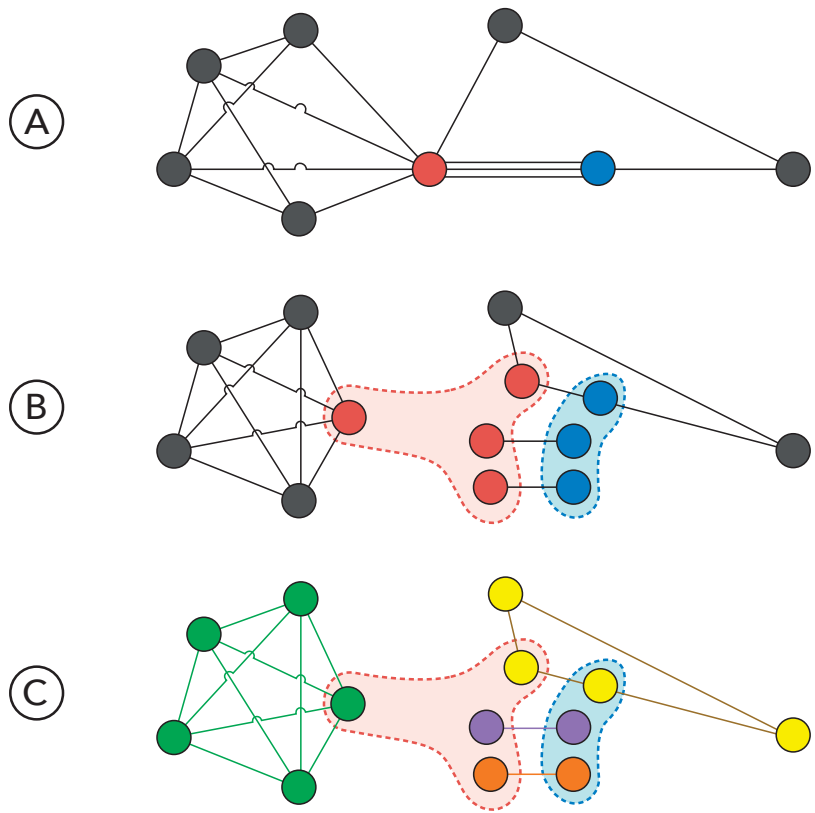


Figure 6. A) is a typical nodal topology diagram that assumes full homogeneity. B) illustrates how the red and blue nodes may be comprised of separate virtual nodes, each with their own discontinuous links. C) illustrates how the set of nodes may represent a set of discontinuous networks (yellow, green, purple, and orange)

		Nodal Systems (location-based)					Representative Network
		Type A	Type B	Type C	Type D	Type E	
Functional Systems (functionality-based)	Bearer Network X	✓	✓	✓	✗	✓	
	Bearer Network Y	✗	✗	✗	✓	✓	
	Distributed System α	✓	✓	✓	✓	✓	
	Distributed System β	✓	✗	✓	✗	✓	
	Distributed System γ	✓	✗	✗	✓	✓	

Figure 7. Nodal systems (location-based) versus functional systems (functionality-based). While the columns (nodal systems) are nodal types comprised of (or built from) elements from the rows, we can also consider these rows, when aggregated together, to be a functional system, either a bearer network (clouds) or a distributed system (boxes); representative network diagrams are shown on the right, where type E represents a data center (DC).

communications and the supporting communications infrastructure in their analysis, design, and support of systems.

The US Department of Homeland Security (2019) identifies “16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.” Presidential Policy Directive 21 specifically calls out the communications sector as critical because it provides an “enabling function” across all critical infrastructure sectors (PPD 2013).

Similarly, the Australian Government’s definition of critical infrastructure (2015) is, “those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia’s ability to conduct national defence and ensure national security.”

We define critical communications networks, with respect to this paper, to be those communications networks that:

- are themselves considered critical infrastructure in their own right (for example, networks used for public safety alerts or by the military); or that
- other critical infrastructure systems depend on for communications services (for example, air traffic control, New York Stock Exchange, utilities, and transportation systems); as well as those networks that
- are relied upon during emergencies, crises, or disasters.

Further, systems that rely on communications networks may be comprised of elements that several different organizations own and manage, preventing the underlying network from having a single owner. For instance, the Australian tsunami warning system relies on constituent elements provided by the Australian Bureau of Meteorology, Geoscience Australia, and the Department of Home Affairs as well as multiple different carriers serving each agency (Australian Government 2020). This greatly increases the complexity of these multi-organization networks.

A myriad of international and domestic vendors and companies provide today’s communications infrastructure. While a communications company can promise to deliver a service, they often have little control over the infrastructures that they use (leased antennas or towers, or virtual channels on a shared fiber link). As several

recent natural disasters have shown, the entire communications infrastructure of a country, state, or area can be damaged to the extent that no existing communications services are available for days or weeks.

### *Levels of Criticality*

In the current era, the importance and criticality of having stable and always available communications is unquestioned. The importance of having and maintaining a communications infrastructure however, is seldom presented or addressed as a stand-alone consideration. In most government and business considerations, the criticality of communications and the need to maintain and protect the infrastructure that delivers communications services is left to the individual critical infrastructure sectors.

The US Department of Homeland Security uses four factors to determine criticality: fatalities, economic loss, mass evacuation length, and degradation of national security (Clarke, Seager, and Chester 2018). The highest level of criticality is the possibility of loss of life. A lack of communications would not directly take a life, but its impact based on the use case might. Examples may include: the inability to perform train signaling functions within a network of high-speed railways; the inability to effectively manage power distribution due to paralyzing impacts from storms or man-made events; the loss of radar managing aircraft within a Class A airspace; and the inability to communicate to field personnel during national emergencies. All such and similar events could remove or seriously degrade the efforts to coordinate responses and awareness to save lives.

### *What Design Criteria Should Be Incorporated Based on Level of Criticality?*

The level of criticality of these networks is subject to interpretation. The Community Emergency Response Team (CERT) motto is “doing the greatest good for the greatest number of people” (Marion County, US, OR 2019). In the case of critical communications networks, there are no standard levels of design criteria, but there are design principles to support an overarching goal that any potential failure should do the least amount of damage to the least number of users, nodes, or systems. Failures occur. Wherever possible, we should identify and avoid single points of failure. The actual levels of criticality are likely to be sector (or context) specific, and therefore we only have access to general guidance.

Best practice is to evaluate nodes based on their impact with respect to the effect of failures on a localized versus system-wide basis. Data centers tend to be more critical than core/hub sites (those sites that provide

connectivity to other sites); and core/hub sites tend to be more critical than edge/spur sites (those sites that do not). Edge/spur sites tend to be the least critical in the overall network architecture although they may be critical to the users in that region. In areas where communications require higher levels of availability, we may consider multiple layers of communications technology. For example, cellular services may overlap the same geographic region as a public safety land mobile radio system which line-of-sight satellite services may also serve. Or, we may consider redundant power and transport systems for network operation centers.

While each node may have its own unique criticality level, it may be simpler to assign criticality levels to nodal types. Similarly, each functional system may have its own individual criticality level since they each serve different purposes and users. Understanding who these users are and their needs is critical to developing a useful set of criticality levels. From this set of data, dependencies are easily identifiable, and we can therefore mitigate failure modes. For instance, if a nodal type with a high criticality level has a single connection to a bearer network, we may provide a second connection to remove the single point of failure. Similarly, we would ideally design a distributed system with a high criticality level with a high degree of redundancy.

Clarke, Seager, and Chester (2018) refer to the concept of minimum essential infrastructure as well as distinguishing urgent and important infrastructure. In the event of a disaster (the third category of critical communications networks, figure 2), the minimum essential infrastructure should remain operational, or be restored as quickly as possible, and we could classify this type of critical infrastructure as urgent. Outside of a disaster, though, we may require a different (perhaps expanded) set of critical infrastructure(s) to remain operational nonstop, and we could classify this type of critical infrastructure as important. On that basis, it is probable that bearer networks are more likely to be urgent, whilst some distributed systems and many bearer networks are likely to be important, and as such, the model may assist in assigning different criticality levels to different parts of a critical communications network.

### **SUMMARY**

As described, the need, use, and understanding of critical communications is key to successful and on-going systems engineering efforts due to its impact as an enabling system to so many other critical sector systems. Acknowledging and addressing critical communications should

be part of any systems engineering effort, especially during the early understanding, requirements, and architecture definition and analysis phases.

Modelling networks as systems can be difficult because each node in the network is invariably different from all other nodes, and yet each node is comprised of common elements that together may form a functional system extending across many nodes. Without the concept of nodal and functional systems, it is difficult to efficiently identify system boundaries and interfaces,

and then to place these under configuration control as configuration items.

When determining levels of criticality for critical communications networks, assigning levels of criticality separately to each nodal and functional system will assist in identifying which specific solution elements are most critical overall. This will also help provide context to the effect of failure modes and enable resiliency (including redundancy and recovery) that systems engineers need to appropriately design in to minimize the impact of failures on society.

We hope that this guidance will assist in modelling complex communications networks as systems, and in so doing, enable the application of traditional systems engineering techniques to critical communications networks. ■

## ACKNOWLEDGEMENT

The authors contributed this article under the auspices of INCOSE's Telecommunications Working Group of which they are members.

## REFERENCES

- Australian Government. 2015. "Critical Infrastructure Resilience Strategy: Policy Statement." <https://cicentre.gov.au/document/P505023>.
- Australian Government, Bureau of Meteorology. 2020. "Australian Tsunami Warning System" <http://www.bom.gov.au/tsunami/about/atws.shtml>.
- Clarke, S., T. Seager, and M. Chester. 2018. "A Capabilities Approach to the Prioritization of Critical Infrastructure." *Environment Systems and Decisions*. doi:10.1007/s10669-018-9691-8.
- INCOSE. 2018. "Systems of Systems Primer." <https://www.incose.org/products-and-publications/sos-primer>.
- Maier, M. 1998. "Architecting Principles for Systems-of-Systems." *Systems Engineering* 1(4): 267-284. doi:10.1002/(SICI)1520-6858.
- Marion County, US, OR. 2019. "Community Emergency Response Team." <https://www.co.marion.or.us/PW/Emergency-Management/CCC/Pages/cert.aspx>.
- PPD (Presidential Policy Directive). 2013. PPD-21. *Directive of Critical Infrastructure Security and Resilience*. Washington, US-DC: PPD, Administration of Barack Obama.
- Syed, M., P. Pong and B. Hutchinson. 2017. "Battlespace communications network-of-networks interface modelling," 2017 Annual IEEE International Systems Conference (SysCon) 1-6. doi:10.1109/SYSCON.2017.7934706.
- US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. 2019. "Critical Infrastructure Sectors." <https://www.cisa.gov/critical-infrastructure-sectors>.
- Walden, D., G. Roedler, K. Forsberg, R. Hamelin, and T. Shortell. 2015. "Systems Engineering Overview." In *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. 4th ed., 5-24. San Diego, US-CA: Wiley.

*Approved for Public Release; Distribution Unlimited Case 20-0893*

## ABOUT THE AUTHORS

**Mr. Thomas Manley** is a principal consultant with Downer Defence (Braddon, AU) working in the Land Network Integration Centre (LNIC) and Land Command, Control, Communication, and Computers (C4) Program within Army Headquarters (AHQ). He is a foundation member of the SESA Telecommunications Working Group that became an INCOSE Working Group. He has 20 years' experience in telecommunications, primarily for Defence and Australian Taxation Office (ATO), working for Optus, Telstra, Boeing, and Thales.

**Ms. Susan Ronning** is owner and principal engineer of AD-COMM Engineering LLC (Woodinville, US-WA). She has over 20 years' experience in the telecommunications industry with a focus on critical wireless voice and data communications networks for public and private agencies in the public safety, emergency management, utility, and transportation markets. Ms. Ronning is co-chair of the INCOSE Telecommunications Working Group.

**William Scheible** is a principal network systems and distributed systems (Sys&Dist) engineer with the MITRE Corporation (McLean, US-VA). 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, US-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 a member of the INCOSE Telecommunications Working Group. The author has provided affiliation with The MITRE Corporation for identification purposes only, and does not intend to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author. ©2020 The MITRE Corporation. All rights reserved.

## Baker continued from page 35

- McDonald, J. 2019. "Microgrid Series." T&D World.
- Smith, R. 2014. "US Risks National Blackout from Small-Scale Attack." *The Wall Street Journal*, 12 March.
- Ton, D. T., and M. A. Smith. 2012. "The US Department of Energy's Microgrid Initiative." *The Electricity Journal* 25 (8): 84-94. <http://dx.doi.org/10.1016/j.tej.2012.09.013>.
- Wood, E. 2019. "Microgrid Policy: What Really Needs to Be Done?" *Microgrid Knowledge*. <https://microgridknowledge.com/microgrid-policy-really-needs-done/>.

## ABOUT THE AUTHOR

**George H. Baker** is a professor emeritus, James Madison University and director, Foundation for Resilient Societies.