University of Southern California

15th Annual Conference on Systems Engineering Research

March 23-25 2017, Redondo Beach, CA

Using systems engineering to protect society in the face of potential "Black Sky" hazards

Neil Siegel, Ph.D.
IBM Professor of Engineering Management
Daniel Epstein Department of Industrial and Systems Engineering
USC Viterbi School of Engineering

CSER 2017 15 YEARS
conference on systems engineering research

The need for a survivable emergency communications system

- **Problem:** If a power outage is big enough (and now, there are ways to create such an outage: cyber, cyber/physical, EMP), there is no way quickly to recover
- **Root cause:** Restarting the power grid after a large-scale failure requires real-time communications between sites (e.g., between a generation station and a water-treatment plant) . . . but all of the communications systems will be down
- **With and without:** A panel of industry experts created a simulation of such a "Black Sky" event. The result was catastrophe: years to recover, millions of casualties. When they re-ran the scenario positing the existence of a survivable emergency communications systems, recovery was far faster, and casualties were orders of magnitude less.

The risk to national continuity

- Our Nation is sustained by complex lifeline infrastructures that produce and provide the resources we need to continue as a society – loss of the power grid would cascade through all other societal infrastructures
  - "Loops", e.g., electricity generated by natural gas; natural gas pumped by electricity; communications powered by electricity, but "re-boot" of the electric grid requires communications; and so forth
- Vulnerability significantly increased by the "electrification of everything"

The social architecture

- We performed a social architecture analysis that allowed us to:
  - Identify the users and customers for such an emergency communications system
  - Determine how they define value within their operational context
  - What would they use it to do?
  - Who would they need to talk to?
  - Determine what they believe that they want and need
  - Understand how they perform their mission today, and what they believe are the shortcomings of the tools and procedures they have today
  - Understand the constraints and limits that apply to their operations

CSER 2017 15 YEARS
conference on systems engineering research

Lessons from the social architecture

- People and organizations that need to receive this emergency communications equipment include power companies, but also include critical infrastructure service providers that need electricity (e.g., water, sewage, natural gas, nuclear, etc.), and some set of "first responders", NGOs, and government officials.
- We identified two principle categories of users, who need very different capabilities:
  - Those who are *coordinating and communicating* about the recovery efforts need status information. These personnel need situational awareness data.
  - Those who are *performing* the actual recovery efforts. These personnel need task management software
- The scale of the emergency communications system will reach 100,000 to 200,000 nodes, so cost-per-node is an issue. This is, however, 3 or 4 orders-of-magnitude fewer nodes than commercial communications systems; those solutions do not affordably scale down.
- The emergency communications system will generate more data than can be assimilated manually, so some sort of decision-support automation system will also be required.
- Planning will be essential, but no plan will survive the onset of "black sky" day without requiring adaptation to the actual event.

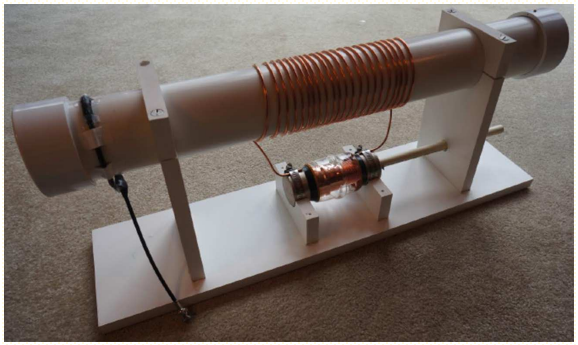
The trade studies

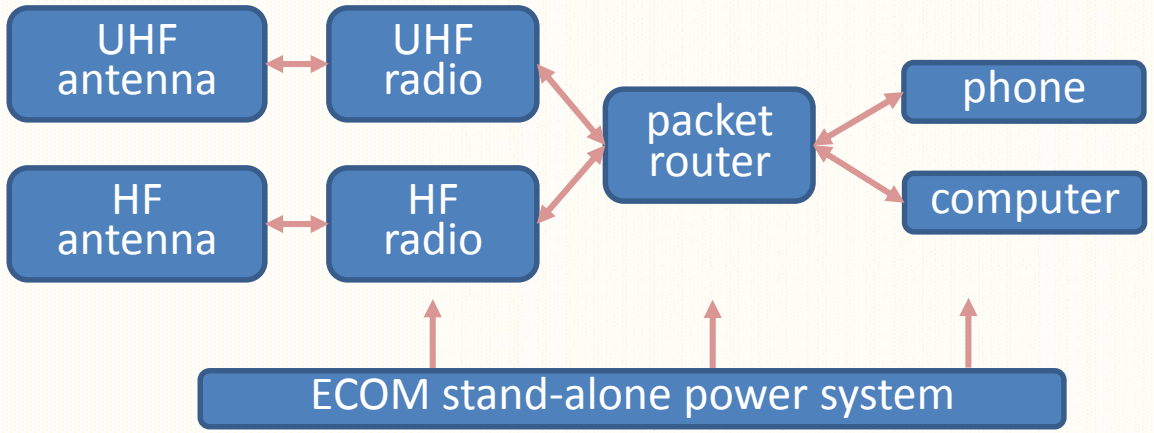
- We next mapped the goals, requirements, and considerations developed in the social architecture into candidate solutions.
- This process involved several steps:
  - Identify candidate communications technologies
  - Create a list of key issues / risk areas
  - Using that list of key issues / risk areas, identify a set of key technical trade studies
  - Create a set of candidate designs, together with methods and metrics for selecting among those candidates designs
  - Make the initial design selection, provide the rationale, and make a preliminary assessment of the feasibility and performance of the selected design

The design

1. Radios

- Site-to-site communications are provided by HF NVIS radios and UHF radios.
- The disadvantage of large size traditionally associated with HF radio antennas is corrected through the use of magnetic antennas.
- UHF provides very high-quality service, but at a shorter range than HF, and HF can operate beyond line-of-sight.
- Hence we include ***both*** frequencies in the ECOM design.

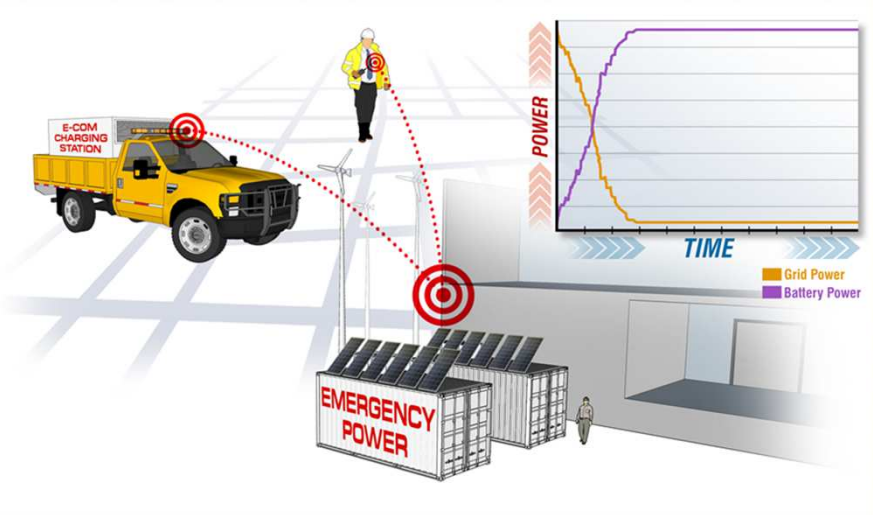




The design

1. Radios
2. Batteries

- 30 days of stand-alone power is provided at each site, through the use of vanadium redox flow batteries.
- In order to be affordable, the size of the stand-alone power array will vary from site to site, driven by a cautious site-specific estimate of ECOM power requirements for 30 days.
- At many sites, the size (and cost) of the battery array can be decreased by the additional of solar panels (and perhaps, wind-power).



The design

1. Radios
2. Batteries
3. On-the-move

- Vehicle-mounted emergency communications configurations are possible, and probably required.
- On-the-move operation will be limited to UHF, due to antenna considerations. HF will be limited to operate at-the-pause.
- Power will be provided by enhanced vehicle alternators.

The design

1. Radios
2. Batteries
3. On-the-move
4. Portable power

- Truck-mounted ECOM battery configurations (e.g., transportable emergency power) are possible, providing a portable power source that can be moved from site to site during an emergency.
- This could power equipment at a site where the battery has been damaged, for example, but could also be used at other sites to provide emergency power.

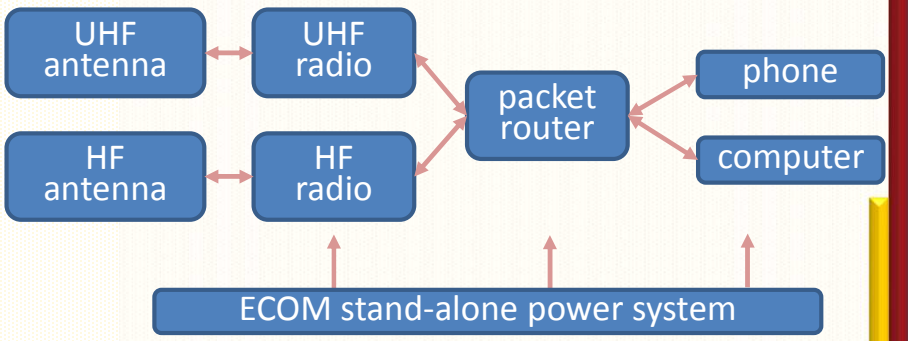
The design

- The single-hop, direct site-to-site communications success-rate native to the radios is not adequate; it must (and can) be improved through the use of error correction coding, and other higher-level communications protocols.
- These functions are implemented in the packet router located at each emergency communications system site.

The design

1. Radios
2. Batteries
3. On-the-move
4. Portable power
5. Single-hop reliability
6. Communications diversity

- At each site, there are 2 independent radios, on different frequency bands, utilizing different modulations.
- This provides a basic type of *communications path diversity*, and thereby improves system reliability.
- The router at each site determines which radio to use for each transmission attempt (whether voice or data), based on its radio "visibility" to adjoining sites.
- No manual action is required by the emergency communications system user in order to select the best radio for each transmission.

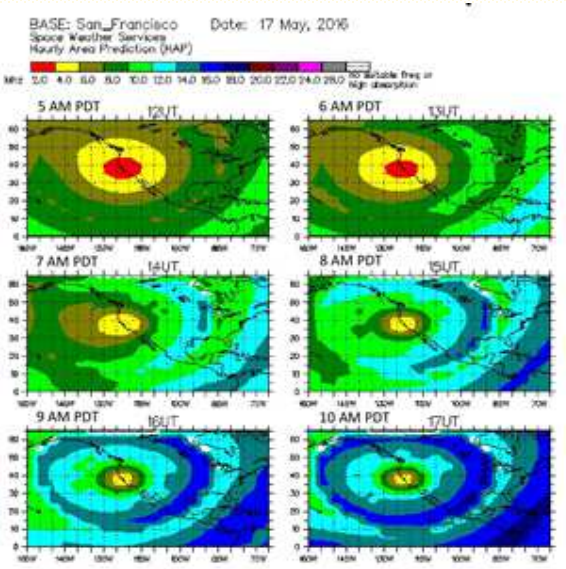


The design

- The packet router also uses a "visibility" algorithm to implement multi-hop communications for both voice and data – a communications link need not be "direct"; I can talk to you through a set of links where the data are in fact routed through other ECOM sites.
- The finding and utilization of such paths is automatically accomplished by the packet routers.
- No manual action is required by the ECOM user to find and implement such multi-hop paths.

The design

- Frequency selection, especially for HF, is based on time-of-day, atmospheric conditions, and other factors.
- A device called the "intelligent director" controls and coordinates this process, providing direction to the packet routers, which in turn command the radios to use the appropriate frequencies and other radio settings.
- No manual action is required by the ECOM user to account for day / night frequency preferences.



The design

- The over-all policy for frequency utilization must be coordinated with regional and national civil officials.
- This is implemented in the intelligent director, located at a regional reliability coordination center or other similar senior command center.
- Policy direction is input into the intelligent director software; it generates the detailed technical commands to all of the packet routers, which in turn command the radios.
- No manual action is required by an ECOM user in the field to comply with radio-frequency policy.

The design

1. Radios
2. Batteries
3. On-the-move
4. Portable power
5. Single-hop reliability
6. Communications diversity
7. Multi-hop communications
8. HF frequency selection
9. Frequency policy management
10. Data processing

- Analysis indicates that the communications system will generate more data than can be assimilated manually by humans, so some sort of data processing system will be required to store, sort, process, prioritize, display, and forward these data
- This software will perform planning / re-planning, situational awareness, task management, and other functions for the recovery personnel
- There are significant software capabilities that are "invisible" to the users, such as authentication, security, and network management. These actually form some of the more-difficult and more important portions of the software.

CSER 2017 15 YEARS
conference on systems engineering research

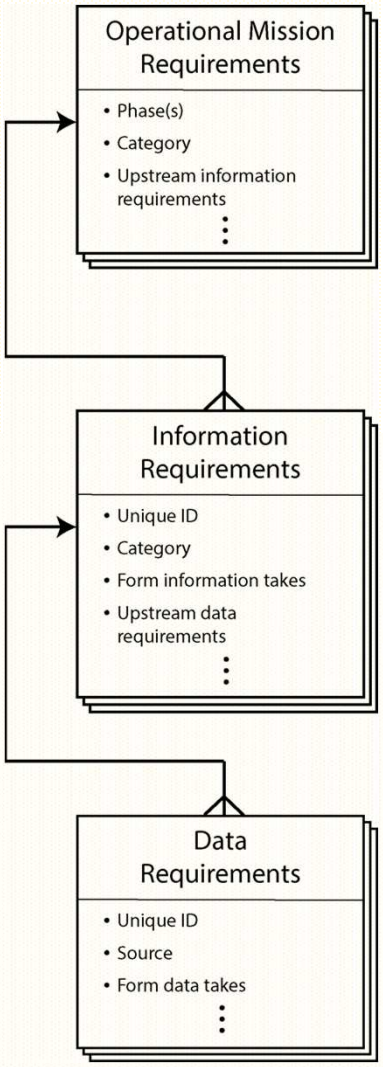
Black-Sky data needs

- Bandwidth is limited for BSX → Need analysis of Black Sky information requirements
  - What **operational missions** will matter most on Black Sky day?
  - What **information** will be needed to guide those missions?
  - What critical **data** must be available to provide that information?

(with thanks to Ellie Graeden, Ph.D. and Joel Thomas, Ph.D.)

Method for analyzing the data

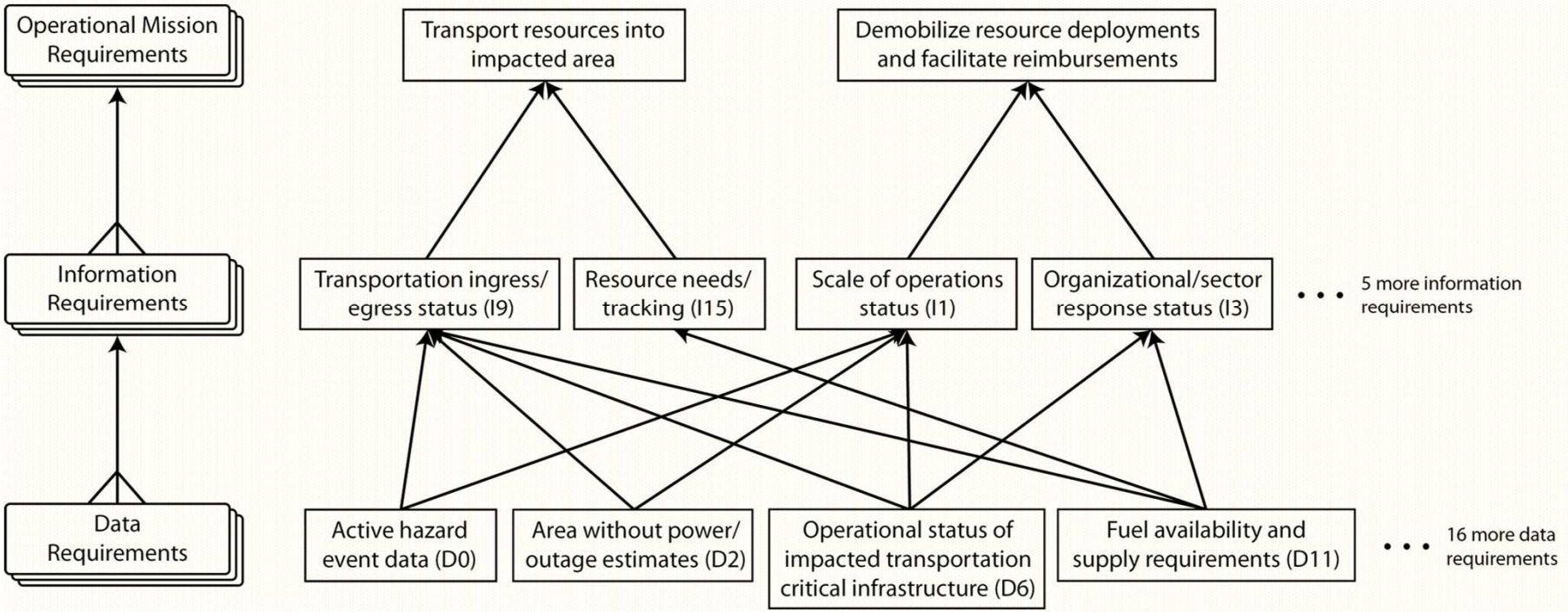
- **Systems-level framework and database**
  - Describes and links requirements
  - Based on prior energy sector analyses
- **Operational mission requirements**
  - Phase-specific actions coordinating entity takes
  - Derived from ~220 requirements from "Virtual USA"
- **Information requirements**
  - Integrate data requirements to give essential context
  - Derived from 350+ essential elements of information from "Virtual USA," and previous analyses
- **Data requirements**
  - Granular, raw data to meet information requirements
  - Derived from 350 interviews across federal interagency emergency management community, and IMIS-SC work



(with thanks to Ellie Graeden, Ph.D. and Joel Thomas, Ph.D.)

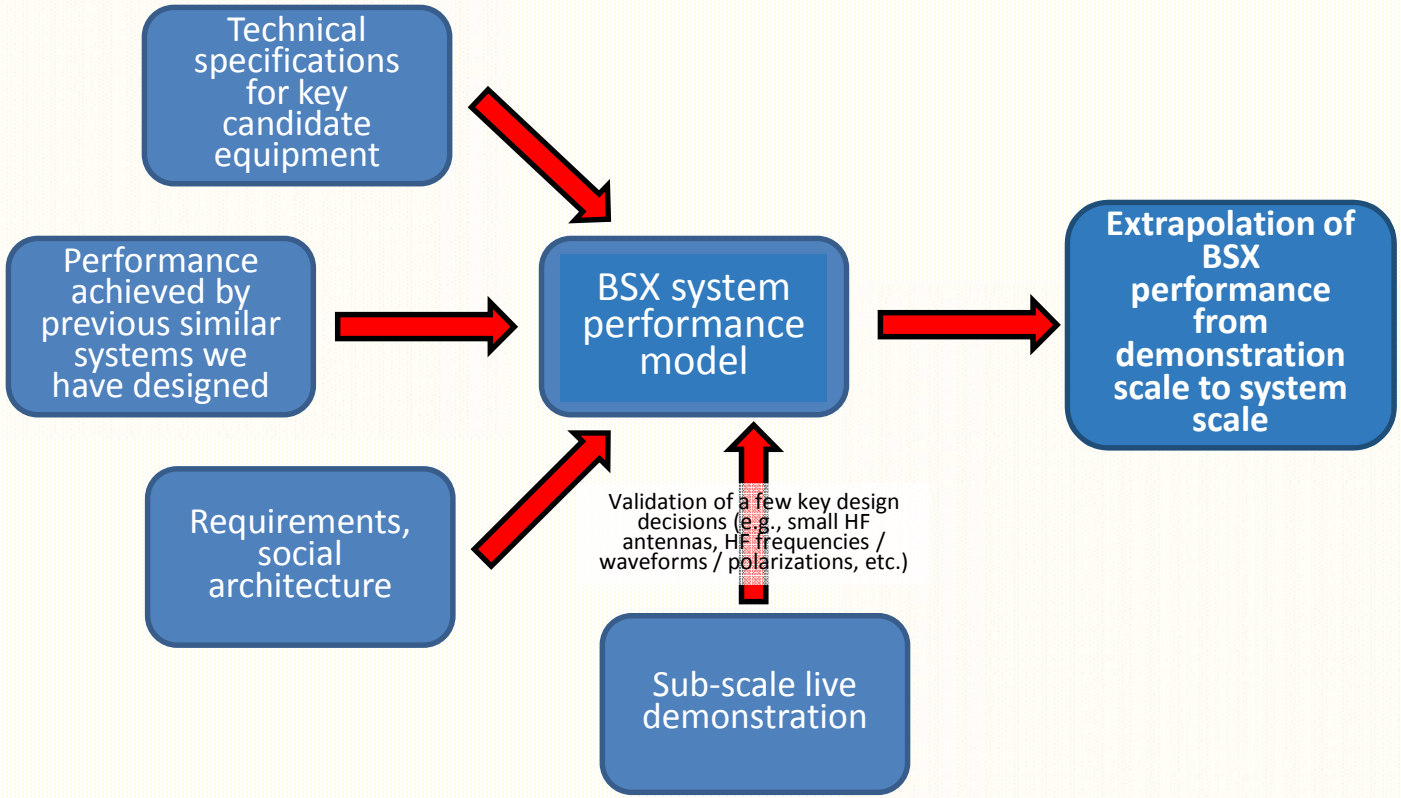
The data are hierarchical

- Many data requirements support each operational mission requirement
- Systems architecture guides implementation



(with thanks to Ellie Graeden, Ph.D. and Joel Thomas, Ph.D.)

Validation


Technical specifications for key candidate equipment
Performance achieved by previous similar systems we have designed
Requirements, social architecture
BSX system performance model
Extrapolation of BSX performance from demonstration scale to system scale
Validation of a few key design decisions (e.g., small HF antennas, HF frequencies / waveforms / polarizations, etc.)
Sub-scale live demonstration

CSER 2017 15 YEARS
conference on systems engineering research

Candidate next steps

- Develop a software specification
- Implement a pilot (e.g., smaller scale than the actual deployed system) implementation of the emergency communications system
- Build and utilize a system-level cost model
- Continue advocacy and educational efforts

CSER 2017 15 YEARS
conference on systems engineering research

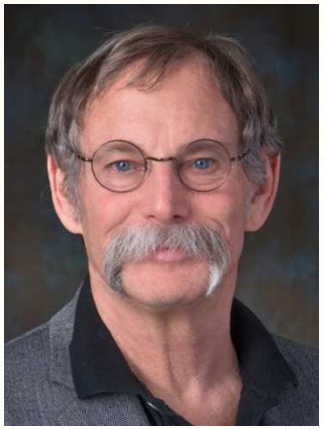
Summary

- Society is highly vulnerable to "Black Sky" events
- Analysis by experts has indicated that a survivable emergency communications system is an essential element of a recovery strategy
- Analysis has also indicated that, due to scale, a stand-alone system is far less expensive than retrofitting existing communications systems to this purpose
- Systems engineering methods – social architecture studies, technical architecture studies, modeling, etc. – have led to the development and validation of a candidate design
- Industry executives want to build a prototype, and use it in actual grid exercises

Questions / discussion

CSER 2017 15 YEARS
conference on systems engineering research

About the author



- **Neil Siegel**, Ph.D., is the IBM professor of Engineering Management in the Daniel Epstein Department of Industrial and Systems Engineering at USC's Viterbi School of Engineering.
- Until the end of 2015, he was the sector vice-president & chief technology officer at Northrop Grumman, where he was responsible for the creation of many first-of-their-kind, large-scale, high-reliability systems.
- 20+ patents. His inventions are used in a billion devices around the world.
- He is a member of the National Academy of Engineering, a Fellow of the IEEE, an INCOSE-certified expert systems engineering practitioner, and the recipient of the IEEE Simon Ramo Medal for systems engineering and systems science, among many other awards and honors.