The Enormous Future Challenge to Systems Engineering

Artificial Intelligence, 5\textsuperscript{th} Generation Communications, and Aging, Failing Infrastructure

Mark Evans
MSEE, MS-National Resource Strategy, ASEP
President 2020, INCOSE Chesapeake Chapter
January 15, 2019
Outline

- Forecasting – a little Prediction Humor
- The 3 Existential Challenges that could “break” the SE we know & practice.
- Our definition of a Engineered System…. how it creates a boundary problem wrt. the three challenges. The challenges have no easy boundary—THAT is their greatest challenge.
- What do we do?
Forecasts BEWARE!!

A WARNING to all Technologists and wannabe Prognosticators: there is a long list of very smart people who have tried predictions and FAILED.

The people particularly bad at forecasting are CEOs, College Presidents and Presidents of companies and organizations.

“Prediction is very difficult, especially if it is about the future.”
- Niels Bohr, Nobel Prize-Physics 1922
“The Americans have need of the telephone, but we do not. We have plenty of messenger boys.”
– Sir William Preece, 1878.
William Henry Preece wasn’t uppity, nor was he a troglodyte. Preece was an electrical engineer, an inventor, an undersea telegraph cable repairman, a Morse code pioneer, the Chief Engineer of the British Post Office, and one of the earliest backers of Marconi.

“Television won’t be able to hold on to any market it captures after the first six months. People will soon get tired of staring at a plywood box every night.”

“There is no reason anyone would want a computer in their home.”
– Ken Olson, 1977
One of the all-time classic tech prediction flubs, this quote came from the lips of president, chairman and founder of Digital Equipment Corp.,
“I predict the Internet will soon go spectacularly supernova and in 1996 catastrophically collapse.”
– Robert Metcalfe, 1995

In 1995, Robert Metcalfe, co-invented a little thing called Ethernet and opened a little company called 3Com. The same year, in a column for InfoWorld, he famously predicted the 1996 annihilation of the Internet.

“The truth is no online database will replace your daily newspaper, no CD-ROM can take the place of a competent teacher and no computer network will change the way government works.”
– Clifford Stoll, 1995

In a 1995 Newsweek column entitled “The Internet? Bah,” astronomer, author, hacker and computer geek Clifford Stoll bravely dissed the newfangled gizmo known as the WWW. He claimed it overflowed with a “cacophony” of voices and opinions – some intelligent and worthy of our attention, but many not.
He spoke of a “wasteland of unfiltered data” and problematic information searches. And he lamented there was no trustworthy way to send virtual money. Right about his present; wrong about the future.
1943:
"I think there is a world market for maybe five computers."

Thomas J. Watson
IBM CEO (1914-1956)

640K ought to be enough for anybody

-Bill Gates, CEO Microsoft, 1981

Open the pod bay doors, Hal.

I'm sorry, Dave. I'm afraid I can't do that.
Artificial Intelligence

Intelligence = the ability to process information either naturally (carbon based) or otherwise for some reason.

Most psychologist define Intelligence as a person’s ability to learn and remember information, to recognize concepts and their relations, and to apply the information to their own behavior in an adaptive way.

True AI people believe computers will eventually duplicate or surpass human capability.

The AI lament: every time AI scores big with a capability, the Engineers and CompScientists rip it out of the AI area and call it an expert system.
Is Superintelligence a real possibility?
YES, but the better question is:
What do we do before it gets here?

- Once an AI reaches a critical point (a singularity) the superintelligence will develop rapidly and come into existence more like an explosion.

In case you missed it: AI is active and producing algorithms at an accelerating rate. The earlier well-known examples: word recognition, playing chess, solving mazes, voice recognition, automobile assembly took years. Recent Technical progress came faster than expected: neural Turing machines, deep reinforcement learning, Bayesian hyperparameter optimization, grid LSTMs, memory networks, variational encoders, sentence level vector embeddings, and generative adversarial networks.
The BIG Fear: Machines will take over and dominate the human species

- Robopocalypse
- Asimov’s 3 Laws of Robotics are looking less like Science Fiction and more like our future bet for survival as a species
- Motivation: why would a robot race seek power? Robots are logical; not emotional, they don’t have egos they are driven to satisfy.
- Would a robot species try to enslave humans to acquire more energy or more manufacturing of their machine species?
- Control: Will a robot have a survival urge? A reproductive urge? An urge to move, explore, create, design, grow?
- Need to caution against anthropomorphizing the capabilities of a superintelligent AI, as well as the motivations of an AI.
- Carbon and Silicon intelligence are NOT the SAME.
Why humans may still have an edge

7 deadly sins — our expertise in pride, greed, lust, anger, gluttony, envy, and sloth are possibly uniquely human emotions that may not program into an artificial intelligence.

Our ability to reason: to extract ourselves from a strange or endless loop.

Gödel’s Incompleteness Theorem — any axiomatic system using its own rule set can construct a statement that requires going outside the system to prove ....in other words, all systems are incomplete and can be broken.... humans are very comfortable going outside of a broken system, extricating themselves from an endless loop or hopeless logic. This is thought to be the one advantage of humans over AI and the lower forms of natural intelligence.

Human intelligence is resilient in the face of failure and disaster— it is this imaginative ability to envision a future not yet possible, coupled with our ability to reason that sets us apart

Machines need a motivation to takeover; a motivation that would have to be seeded and developed. Evil Humans in concert with an AI is a different story.
AI gone seriously wrong

- Robopocalypse most likely won’t occur by itself—someone has to teach machines the concept of evil.
- Evil Humans in the Human-Machine loop are a different story
- Adversaries may build Killer Robot Armies (AI arms race)
- Pinker points out machines don’t have emotions; ability to extract themselves from strange loops or ability to reason?
- Intelligent Agents may not “want” to do mundane, menial human tasks
Coping with Super Intelligence

• When the Intelligence Explosion (singularity) gets here sometime in the 21st Century, humans will not be able to compete on a cognitive level.…
• The best response: Focus Human Design Effort and Engineering on seeding the right CONTROL System.…
• There are 2 broad classes for dealing with the CONTROL problem which is at the heart of AI safety: Capability control and Motivation selection.

Each control method comes with potential vulnerabilities and presents different degrees of difficulty in its implementation.

The VALUE-LOADING problem or “teaching a machine to acquire values” (whatever THAT means) is one of the thorniest and still open problems for AI developments.

Q: Does this mean SEs need to become experts in AI? A: Yes!
# Control Methods for a Superintelligence

## Capability Control methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boxing methods</td>
<td>The system is confined in such a way that it can affect the external world only through some restricted, pre-approved channel. Encompasses physical and informational containment methods.</td>
</tr>
<tr>
<td>Incentive methods</td>
<td>The system is placed within an environment that provides appropriate incentives. This could involve social integration into a world of similarly powerful entities. Another variation is the use of (cryptographic) reward tokens. “Anthropic capture” is also a very important possibility but one that involves esoteric considerations.</td>
</tr>
<tr>
<td>Stunting</td>
<td>Constraints are imposed on the cognitive capabilities of the system or its ability to affect key internal processes.</td>
</tr>
<tr>
<td>Tripwires</td>
<td>Diagnostic tests are performed on the system (possibly without its knowledge) and a mechanism shuts down the system if dangerous activity is detected.</td>
</tr>
</tbody>
</table>

## Motivation selection methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct specification</td>
<td>The system is endowed with some directly specified motivation system, which might be consequentialist or involve following a set of rules.</td>
</tr>
<tr>
<td>Domesticity</td>
<td>A motivation system is designed to severely limit the scope of the agent’s ambitions and activities.</td>
</tr>
<tr>
<td>Indirect normativity</td>
<td>Indirect normativity could involve rule-based or consequentialist principles, but is distinguished by its reliance on an indirect approach to specifying the rules that are to be followed or the values that are to be pursued.</td>
</tr>
<tr>
<td>Augmentation</td>
<td>One starts with a system that already has substantially human or benevolent motivations, and enhances its cognitive capacities to make it superintelligent.</td>
</tr>
</tbody>
</table>
The traditional approach to controlling an AI

*Issac Asimov’s 3 Laws of Robotics*

1. A robot may not injure a human being or, through inaction, allow a human being to come to harm;
2. A robot must obey any orders given to it by human beings, except where such orders would conflict with the First Law;
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

_Embarrassingly for our species_, Asimov’s laws remained state-of-the-art for over half a century despite obvious problems with the approach, some of which are explored in Asimov’s own writings.

- Consider……how one might explain Asimov’s first law to an AI.
- Does it mean that the robot should minimize the probability of any human being coming to harm? In that case the other laws become needless since it is always possible for the AI to take some action that would have at least some microscopic effect on the probability of a human being coming to harm.
- How is the robot to balance a large risk of a few humans coming to harm versus a small risk of many humans being harmed?
- How do we define “harm” anyway?
- How should the harm of physical pain be weighed against the harm of architectural ugliness or social injustice?
# Superintelligence Risks and Rewards

<table>
<thead>
<tr>
<th>Task</th>
<th>Skill set</th>
<th>Strategic relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intelligence amplification</strong></td>
<td>AI programming, cognitive enhancement research, social epistemology development, etc.</td>
<td>• System can bootstrap its intelligence</td>
</tr>
</tbody>
</table>
| **Strategizing**            | Strategic planning, forecasting, prioritizing, and analysis for optimizing chances of achieving distant goal | • Achieve distant goals  
• Overcome intelligent opposition                                                       |
| **Social manipulation**     | Social and psychological modeling, manipulation, rhetoric persuasion     | • Leverage external resources by recruiting human support  
• Enable a “boxed” AI to persuade its gatekeepers to let it out  
• Persuade states and organizations to adopt some course of action |
| **Hacking**                 | Finding and exploiting security flaws in computer systems                | • AI can expropriate computational resources over the Internet  
• A boxed AI may exploit security holes to escape cybernetic confinement  
• Steal financial resources  
• Hijack infrastructure, military robots, etc. |
| **Technology research**     | Design and modeling of advanced technologies (e.g. biotechnology, nanotechnology) and development paths | • Creation of powerful military force  
• Creation of surveillance system  
• Automated space colonization |
| **Economic productivity**   | Various skills enabling economically productive intellectual work       | • Generate wealth which can be used to buy influence, services, resources (including hardware), etc. |
The 5G promise: broadband access everywhere, entertaining higher user mobility, and enabling connectivity of massive number of devices (e.g. Internet of Things (IoT)) in an ultrareliable and affordable way.

The main technological enablers: Cloud computing, Software Defined Networking (SDN) and Network Function Virtualization (NFV) are maturing toward 5G. However, there are pressing security challenges in these technologies and growing concerns for user privacy.

https://www.researchgate.net/publication/3182223878_5G_Security_Analysis_of_Threats_and_Solutions
The extreme vulnerability of 5G networks

The network has moved away from centralized, hardware-based switching to distributed, software-defined digital routing. In the 5G software defined network, cyber hygiene functions are pushed outward to a web of digital routers throughout the network, and the inspection and control by hardware chokepoints is lost. 5G further complicates its cyber vulnerability by virtualizing in software higher-level network functions formerly performed by physical appliances. These standardized building block protocols and systems have proven to be valuable tools for those seeking to do ill. The network is also being managed by software—often early generation artificial intelligence—that itself can be vulnerable to an attacker that gains control of the network software.

The dramatic expansion of bandwidth that makes 5G possible creates additional avenues of attack. Physically, low-cost, short range, small-cell antennas deployed throughout urban areas become new hard targets. When software allows the functions of the network to shift dynamically, cyber protection must also be dynamic rather than relying on a uniform lowest common denominator solution. Finally, the vulnerability created by attaching tens of billions of hackable smart devices (actually, little computers) to the network colloquially referred to as IoT. Plans are underway for a diverse and seemingly inexhaustible list of IoT-enabled activities, all of which are both wonderful and uniquely vulnerable.

In July, for instance, Microsoft reported that Russian hackers had penetrated run-of-the-mill IoT devices to gain access to networks. From there, hackers discovered further insecure IoT devices into which they could plant exploitation software.

Q: Does this mean SEs need to become Network & Cyber Security experts? A: Yes!
5G Security Threats and Challenges

**Flash network traffic:** High number of end-user devices and new things (IoT).

**Security of radio interfaces:** Radio interface encryption keys sent over insecure channels.

**User plane integrity:** No cryptographic integrity protection for the user data plane.

**Mandated security in the network:** Service-driven constraints on the security architecture leading to the optional use of security measures.

**Roaming security:** User-security parameters are not updated with roaming from one operator network to another, leading to security compromises with roaming.

**Denial of Service (DoS) attacks on the infrastructure:** Visible nature of network control elements, and unencrypted control channels.

**Signaling storms:** Distributed control systems requiring coordination, e.g. Non-Access Stratum (NAS) layer of Third Generation Partnership Project (3GPP) protocols.

**DoS attacks on end-user devices:** No security measures for operating systems, applications, and configuration data on user devices.

https://www.researchgate.net/publication/318223878_5G_Security_Analysis_of_Threats_and_Solutions
Global Interconnectivity Threats and Costs

• Malicious cyber activity **cost the U.S. economy between $57 billion and $109 billion in 2016.**
• Malicious cyber activity directed at private and public entities manifests as denial of service attacks, data and property destruction, business disruption (sometimes for the purpose of collecting ransoms) and theft of proprietary data, intellectual property, and sensitive financial and strategic information.
• Damages from cyberattacks and cyber theft can spill over magnifying the damage to the economy.
• Firms share common cyber vulnerabilities, causing cyber threats to be correlated across firms.
• Cybersecurity is a common good; **lax cybersecurity imposes negative externalities on other economic entities and on private citizens.** Failure to mitigate negative externalities results in underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment.
• **Cyberattacks against critical infrastructure sectors could be highly damaging to the U.S. economy.**

**Bad Guys can be:** Nation-states, Corporate competitors, Hacktivists, Organized criminal groups, and Company insiders.

Foreign Economic Espionage in Cyberspace

1. In 2018, Foreign economic and industrial espionage against the United States continues to represent a significant threat to America’s prosperity, security, and competitive advantage.

2. Cyberspace remains a preferred operational domain.

3. Next-generation technologies, such as Artificial Intelligence (AI) and the Internet-of-Things (IoT) will introduce new vulnerabilities to U.S. networks for which the cybersecurity community remains largely unprepared.

4. Building an effective response 1st requires understanding economic espionage as a worldwide, multi-vector threat to the integrity of the U.S. economy and global trade.

5. Foreign intelligence services continue to represent the most persistent and pervasive cyber intelligence threat.

6. China, Russia, and Iran stand out as three of the most capable and active cyber actors tied to economic espionage and theft of U.S. information.

7. Despite advances in cybersecurity, cyber espionage continues to offer bad actors a relatively low-cost, high-yield access to a wide range of intellectual property.

8. A range of potentially disruptive threat trends warrant attention. Software supply chain infiltration already threatens the critical infrastructure sector and is poised to threaten other sectors.

https://publicintelligence.net/ncsc-cyber-economic-espionage/
Is there a health issue with radiation at the higher frequencies used for 5G?

One more risk?

• It's easy to find claims online that the higher frequency of 5G constitutes a health risk.
• 1G, 2G, 3G and 4G use between 1 to 5 gigahertz. 5G uses between 24 to 90 gigahertz. There are several assertions about the RF Radiation portion of the electromagnetic spectrum, the higher the frequency, the more dangerous it is to living organisms."
• But asserting that the higher frequency is more dangerous is just that—an assertion, and there’s little real science to stand behind it.
• 5G remains non-ionizing in nature.

https://www.howtogeek.com/423720/how-worried-should-you-be-about-the-health-risks-of-5g/
Addressing Cyber Security

- INCOSE 2025: Systems engineering routinely incorporates requirements to enhance systems and information security and resiliency to cyber threats early and is able to verify the cyber defense capabilities over the full system life cycle, based on an increasing body of strategies, tools and methods.
- Cyber security is a fundamental system attribute that systems engineers understand and incorporate into designs using the following strategies:
  - Continuous threat and system behavior monitoring
  - Management of access rights and privileges
  - Use of testbeds for assessing new threats in fielded systems
  - Supply-chain diligence
  - Certification and accreditation standards
  - Formal methods for identification of vulnerabilities

*The INCOSE Vision recognizes that Cyber Security has become another key skill the SE must have a working knowledge of.*
The Aging Infrastructure

- Every 4 years, the ASCE Foundation grades the US Infrastructure.
- The 2017 Infrastructure Report Card reveals that we have made some incremental progress toward restoring our nation’s infrastructure.
- But it has not been enough. As in 2013, America’s cumulative GPA is once again a D+.

Critical Risks to US Infrastructure
The FUTURE System Environment... is here NOW!
The FUTURE System Environment… is here NOW!
WHAT do we DO?

• Read, Research, Reflect, Revisit, Relearn, Redesign, Revise, Retrofit, Retest, Adapt, Repeat; ..... 
• Try to incorporate methods from other disciplines
What do we do?

INCOSE 2025 has a vision for the future with a particular emphasis upon MBSE

SE Vision 2025 addresses the AI threat generally, the 5G threat specifically, and infrastructures generally

Several of our colleagues are already out-front leading with solutions described in important papers

Simulation and Visualization

Modeling, simulation, and visualization enable complex system understanding that helps anticipate and verify solutions and prevent failures before building them. As systems become more complex, understanding their designer behavior due to complexity cascading down to physical environments, soft- and hardwarized behaviors and human interactions becomes essential for successful systems development.

Integrated Model-based Approaches

Model-based Systems Engineering will become the “norm” for systems engineering execution with specific emphasis on integrated modeling environments. These systems models spill beyond the boxes, incorporating geometric, production and operational views. Integrated models reduce inconsistencies, enable automation and support early and continual verification by analytics.

Transforming Virtual Model to Reality

A shift towards an integrated, digital engineering environment enables rapid transformation of concepts and design into physical prototypes through the application of additive manufacturing technologies, such as 3D-printers. This capability enables teams to rapidly and continuously assess and update their designs prior to committing costs to production hardware. The Boeing 777X virtual design process establishes a point of departure for the future of highly integrated, virtual design and production. Systems engineers and designers will leverage this capability to rapidly assess alternative designs in terms of their form, fit and function.
**Systems Engineering will be....**

- **Relevant to a broad range of application domains**, well beyond its traditional roots in aerospace and defense, to meet society’s growing quest for sustainable system solutions to providing fundamental needs, in the globally competitive environment.

- **Applied more widely to assessments** of socio-physical systems in support of policy decisions and other forms of remediation.

- Comprehensively **integrating multiple market, social and environmental stakeholder demands against “end to end” life cycle considerations and long term risks.**

- A key integrating role to support collaboration **that spans diverse organizations and regional boundaries, and a broad range of disciplines.**

- Supported by a more encompassing foundation of theory and **sophisticated model based methods and tools** allowing a better understanding of increasingly **complex systems** and decisions in the face of uncertainty.

- Enhanced by an educational infrastructure that **stresses systems thinking and systems analysis** at all learning phases.

- Practiced by a growing cadre of professionals who possess not only technical acumen in their domain of application, but who also **have mastery of the next generation of tools and methods necessary** for the systems and integration challenges of the times.
Addressing the AI Challenge
Technical Conferences set the tone and direction

**Conclusions** from the JHU/APL May 25, 2017 Conference on AI:

- While sentient machines are likely a long way off, the opportunities and risks posed by complex autonomous systems are here today.
- Intelligent machines are changing the nature of war.
- Machines don’t know what they don’t know (and neither do we).
- For the foreseeable future, teams of humans and machines will be more effective than either working alone.
- Emerging brain interfaces may enable thought-based communication and control between humans and machines in the near future (without brain surgery)
- In Artificial Intelligence, humanity has created our most sophisticated set of tools yet, with potential that may even reach what we’ve imagined in science fiction.
**Linear Systems Theory**

*Most of our Systems Developments use Linear Mathematics*

- **Quick Review: Linear Systems**
  - Homogeneity (Scaling)
  - Additivity
  - Together:
    - Homogeneity AND Additivity = Principle of SUPERPOSITION
  - Shift-Invariance

- Why we use Linear Math to describe Systems:
  - **Simpler**
  - Characterizing the complete input-output properties of a system by exhaustive measurement is usually impossible.
  - When a system qualifies as a *linear system*, it is possible to use the responses to a small set of inputs to predict the response to any possible input.
  - This can save the scientist/engineer enormous amounts of work, and **makes it possible to characterize the system completely**.

[https://www.cns.nyu.edu/~david/handouts/linear-systems/linear-systems.html](https://www.cns.nyu.edu/~david/handouts/linear-systems/linear-systems.html)
Non-linear Systems are:

- Messy Mathematics.
- Hard to model.....
- Produce outputs that are frequently non-repeatable.
- Everything linear systems are not....
- Real world....
Mitchell Feigenbaum

- Born in New York City, to Polish and Ukrainian Jewish immigrants.
- Attended Samuel J. Tilden High School, in Brooklyn, and City College of New York.
- Graduate studies at the Massachusetts Institute of Technology (MIT) in electrical engineering and then changed to physics. (1964)
- Virginia Polytechnic Institute and State University (1972–1974)
- Long term post at the Los Alamos National Laboratory in New Mexico to study turbulence in fluids. His research led to a study of chaotic maps.[2]
- 1986, awarded the Wolf Prize in Physics "for his pioneering theoretical studies demonstrating the universal character of non-linear systems, which has made possible the systematic study of chaos".
- Discovered the Universality Principle buried deep within Dynamical Systems and Chaos
The number $\delta = 4.6692 \ldots$ is a constant of chaos comparable only to the fundamental importance of numbers like $\pi$. Feigenbaum’s discovery was the first of many footprints by which the tracks of chaos are now recognized. It has been documented in systems as diverse as dripping faucets, oscillations of liquid helium, and gypsy moth population variances.”

Feigenbaum Diagram of the iterated function

$$f(x) = 1 - \mu|x|^r$$

Chaos and Fractals, 1992, p.590

The Feigenbaum Constant
A Monumental Achievement that launched a new science
The Feigenbaum Constant

Discovery of *Universality* within Chaos

\[ \lim_{{n \to \infty}} \frac{r^n - r^{n-1}}{r^{n+1} - r^n} = 4.669... \]
We need to use **Different Mathematics**

- The real world is non-linear
- SE and MBSE use linear, Gaussian mathematics for engineering systems because it simplifies the problem, and the mathematics are more manageable (doable)
- A Complexity Primer for Systems Engineers INCOSE (2015 Whitepaper) advocates some non-linear analytic techniques

<table>
<thead>
<tr>
<th>Table 3. Selected modeling methods for complex systems from the Cook Matrix.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ANALYZE</strong></td>
</tr>
<tr>
<td>Data Mining</td>
</tr>
<tr>
<td>Spikes</td>
</tr>
<tr>
<td>Fuzzy Logic</td>
</tr>
<tr>
<td>Neural Networks</td>
</tr>
<tr>
<td>Classification &amp; Regression Trees</td>
</tr>
<tr>
<td>Kernel Machines</td>
</tr>
<tr>
<td>Nonlinear Time Series Analysis</td>
</tr>
<tr>
<td>Markov Chains</td>
</tr>
<tr>
<td>Power Law Statistics</td>
</tr>
<tr>
<td>Social Network Analysis</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
SE Vision 2025

- Technological advances in basic components, sub-systems and infrastructure will produce innovations at an increasing pace, leading to sophisticated new services and products.

- The internet, for example, has progressed from an emerging technology to having a profound impact on commerce and our personal lives in just 20 years.

- These new services and products will both depend upon and result in new, evermore complex systems.

- With technology infusion rates increasing, the pressure of time to market will also increase, yet customers will be expecting improved product functionality, aesthetics, operability, and overall value.
SE Vision 2025

• Addresses the 3 threats Generally
• The Path Forward is very specific about: Model-based SE becoming the primary method
• Cross-discipline knowledge and techniques being used by all SEs
The Hierarchy of Complexity

- Where an engineering problem set resides on this complexity tier structure has everything to do with the method used to approach the problem.
- Systems Engineers must learn new methods to address top 2 problem classes: “Wicked” and Complex Adaptive.
Assessment of Complex Systems

- Difficult to Do
- Still in its infancy
- Non-Linear Methods using AI is necessary to engineer the complex system.
- The time and effort to fully model a complex system typically exceeds the schedule and budgetary resources of the project. Behavior is nonlinear which means extrapolation of current conditions leads to errors in understanding.
The potentially infinite diversity of complex system examples precludes a 'one-size-fits-all' mentality when it comes to responsible and responsive Systems Engineering approaches to working with complexity.

Much has been written on the nature of complexity in engineered systems though there is little consensus on what precisely generates complexity let alone what to do about it - and that can be seen as the general nature of it.
SE Knowledge of Cross Discipline Languages and SE Learning across another Discipline’s Methods is crucial to future solutions

- Embraces 3 of the 6 INCOSE 2025 tenets

1. Expanding the APPLICATION of systems engineering across industry domains.
2. Embracing and learning from the diversity of systems engineering APPROACHES.
3. Applying systems engineering to help shape policy related to Social And Natural Systems. (INCOSE 2014)
Addressing the 5th Generation Challenge
SE Vision 2025

New Techniques for Engineering a System of Systems

• The Internet of Things extends the SoS challenge beyond interconnected computers and users, to include increasingly interconnected systems and devices that monitor and control everything from household appliances to automobiles.
• A diverse set of stakeholders will increasingly demand SoS to provide information and services, leveraging value from the pieces.
• Techniques for analyzing interactions among independent systems and understanding emergent behaviors in SoS must mature.
• New measures will be developed to characterize the SoS.
• SoSE will employ new continuous verification methods as changes occur without central control.
• Design of experiments is one such methodology for optimizing a verification program with many parameters and uncertainty.
• Requirements management will evolve to address even more diverse stakeholders, in the face of uncertain organizational authority.
• Methods for making evolutionary interoperability agreements among SoS constituents will become more robust.
In 2025 and beyond, systems engineering will be a key integrator role for collaborative enterprise engineering that span regions, cultures, organizations, disciplines, and life cycle phases. This will result in multi-disciplinary engineering workflows and data being integrated to support agile program planning, execution, and monitoring. The collaboration will extend across the supply chain so that customers, primes, subcontractors, and suppliers are integrated throughout all phases of development. Automated workflow, data integration, and networked communications are critical to agile program execution, such as when implementing a change process.
5G Security: Analysis of Threats and Solutions

Ijaz Ahmad1, Teerchal Kumar1, Madhumita Lyangani1, Joki Olkkonen1, Mikko Vainikka1, Andrei Gurtov1
1 Department of Computer and Information Science, Linköping University, 581 83 Linköping, Sweden
E-mail: [ija@liu.se, teerk@liu.se, mly@liu.se, joki@liu.se, miko@liu.se, andreigurtov@liu.se]

Abstract—5G will provide broadband access everywhere, support higher user mobility, and enable comprehensive coverage of a large number of devices e.g., Internet of Things (IoT) objects in an efficient and affordable way. The main challenges of the new 5G system will be in the areas of network security and privacy. This paper presents an analysis of the main threats to 5G, and proposes potential solutions to overcome them.

I. Introduction

The vision of 5G wireless networks lies in providing very high data rates and higher coverage through flexible base station deployment with increased capacity, significantly better Quality of Service (QoS), and extremely low latency. It provides for access service to be required operations changing the clouds, or even services in the cloud.

II. Security Technologies

<table>
<thead>
<tr>
<th>Security Technology</th>
<th>Primary Focus</th>
<th>SDN</th>
<th>NFV</th>
<th>Channels</th>
<th>Cloud</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS, DDoS detection</td>
<td>Security of centralized control points</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration verification</td>
<td>Flow of information in SDN switches</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access control</td>
<td>Control access to SDN and core network elements</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic isolation</td>
<td>Ensures isolation for VNFs and virtual slices</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link security</td>
<td>Provide security to control channels</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity verification</td>
<td>User identity verification for roaming and clouds services</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity security</td>
<td>Ensure identity security of users</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location security</td>
<td>Ensure security of user location</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMSI security</td>
<td>Secure the subscriber identity through encryption</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile terminal security</td>
<td>Anti-malware technologies to secure mobile terminals</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity verification</td>
<td>Security of data and storage systems in clouds</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IX-IXDOS mitigation</td>
<td>Security for cloud web services</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service access Control</td>
<td>Service-based access control security for clouds</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table II: Security Technologies and Solutions

Important 2017 IEEE Paper from Universities in Finland & Sweden proposes potential solutions for 5G Security Threats

https://www.researchgate.net/publication/318223878_5G_Security_Analysis_of_Threats_and_Solutions
Addressing the Infrastructure Challenge
SE Vision 2025 identifies infrastructure and interdependence of technology-global trends as key drivers of future systems. Global trends include changes to both socio-economic conditions and changes in our physical environment. These global changes impose new demands on the types of systems that are needed, yet are often impacted by the very technology and system developments meant to satisfy the human needs.

For example, increased population growth and urbanization impose new challenges on transportation, health, and other modern infrastructures, while at the same time, systems solutions and technology itself can adversely impact air and water quality.

The global community is calling for more attention to how systems can positively contribute to our social condition and natural environment to help advance our quality of life.
Leadership & Planning

**ASCE’s Grand Challenge**

- **Smart investment will only be possible with leadership, planning, and a clear vision for our nation’s infrastructure.** Leaders from all levels of government, business, labor, and nonprofit organizations must come together to ensure all investments are spent wisely, prioritizing projects with critical benefits to the economy, public safety, and quality of life.

- **To do so, we must:**
  1. Require all projects greater than $5 million that receive federal funding use life cycle cost analysis and develop a plan for funding the project, including its maintenance and operation, until the end of its service life.
  2. Create incentives for state and local governments and the private sector to invest in maintenance, and to improve the efficiency and performance of existing infrastructure.
  3. **Develop tools** to ensure that projects most in need of investment and maintenance are prioritized.
  4. **Streamline the project permitting process** across infrastructure sectors, with safeguards to protect the natural environment, to provide greater clarity to regulatory requirements, bring priority projects to reality more quickly, and secure cost savings.
  5. **Identify a pipeline of infrastructure projects attractive to private sector investment** and public-private partnership.
  6. ASCE recognizes civil engineers’ unique leadership role in addressing our infrastructure challenges. ASCE issued its “**Grand Challenge**,” a call to action for the entire civil engineering profession to increase the value and capacity of infrastructure and increase and optimize infrastructure investments.
  7. Central to the Grand Challenge is a commitment to rethinking what’s possible through life cycle cost assessments, innovation, performance-based standards, and enhanced resiliency, with **the goal of reducing the life cycle cost of infrastructure by 50 percent by 2025.**

[https://www.infrastructurereportcard.org/solutions/leadership-planning/](https://www.infrastructurereportcard.org/solutions/leadership-planning/)
CISA Established November 16, 2018

- Cybersecurity and Infrastructure Security Agency
- Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The nation's critical infrastructure provides the essential services that underpin American society.
- On November 16, 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018. This landmark legislation elevates the mission of the former National Protection and Programs Directorate (NPPD) within DHS and establishes the Cybersecurity and Infrastructure Security Agency (CISA).

https://publicintelligence.net/dhs-collapsing-bridges/
Wicked Problems

- Definition:

  "one of the most intractable problems is that of defining problems (of knowing what distinguishes an observed condition from a desired condition) and of locating problems (finding where in the complex causal networks the trouble really lies)"

- Planning Problems are Wicked Problems

Dilemmas in a General Theory of Planning*

HORST W. J. RITTEL
Professor of the Science of Design, University of California, Berkeley

MELVIN M. WEBBER
Professor of City Planning, University of California, Berkeley

ABSTRACT

The search for scientific bases for constraining problems of social policy is bound to fail, because of the nature of these problems. They are "wicked" problems, wherein science has developed to deal with "tame" problems. Policy problems cannot be definitively described. Moreover, in a pluralistic society there is nothing like the well-defined public good; there is no objective definition of equity; policies that respond to social problems cannot be objectively assessed or falsified; and it means no sense to talk about "optimal solutions" to social problems where some qualifications are imposed first. Even worse, there are no "solutions" in the sense of definitive and objective answers.

George Bernard Shaw diagnosed the case several years ago; in more recent times popular protest may have already become a social movement. Shaw asserted that "every profession is a conspiracy against the laity." The contemporary pullers are responding as though they have made the same discovery.

Few of the modern professional's seem to be immune from the popular attack—whether they be social workers, educators, lawyers, public health officials, policemen, city planners, highway engineers or physicians. Our restless clients have been selling us that they don't like the educational programs that schoolmen have been offering, the re-development projects urban renewal agencies have been proposing, the law-enforcement styles of the police, the administrative behavior of the welfare agencies, the locations of the highways, and so on. In the city, the streets, and the political campaigns, we've been hearing ever-louder public protests against the professionals' diagnoses of the clients' problems, against professionally designed governmental programs, against professionally certified standards for the public services.

It does seem odd that this attack should be coming just when professionals in

* This is a modification of a paper presented to the Panel on Policy Sciences, American Association for the Advancement of Science, Boston, December 1969.
‘Wicked’ Problems have characteristics very different from complex problems

1. There is no definitive formulation of a wicked problem
2. Wicked problems have no stopping rule
3. Solutions to wicked problems are not true-or-false, but good-or-bad
4. There is no immediate and no ultimate test of a solution to a wicked problem
5. Every solution to a wicked problem is a "one-shot operation"; because there is no opportunity to learn by trial-and-error, every attempt counts significantly
6. Wicked problems do not have an enumerable (or an exhaustively describable) set of potential solutions, nor is there a well-described set of permissible operations that may be incorporated into the plan
7. Every wicked problem is essentially unique
8. Every wicked problem can be a symptom of another problem.
9. The existence of a discrepancy representing a wicked problem can be explained in numerous ways. The choice of explanation determines the nature of the problem's resolution
10. Because of the social consequences, the planner has no margin for being wrong unlike the situation when a scientist makes a scientific hypothesis.

Dealing in earnest with a ‘Wicked’ Problem

• The “Science Of Muddling Through”—not an elegant sounding engineering method, but it’s scientific, adaptive, legitimate and just may be our best option
• The paper identifies the best way to address Wicked Problems—dive into the middle, work locally, solve what you can, keep working to the edges..... this is a radical shift in systems engineering
• Some solutions were out there in other disciplines and only need to be revisited
• The Science of Muddling Through is an elixir for some wicked problems.

The Science of “Muddling Through”

By CHARLES E. LINDBLOM
Associate Professor of Economics
Yale University

S
uppose an administrator is given responsibility for formulating policy with re
gard to inflation. He might start by trying to list all related values in order of impor-
tance, e.g., full employment, reasonable business profits, protection of small savings, pre
vention of a stock market crash. Then all possible policy outcomes could be rated as more or less efficient in attaining a maximum of these values. This would of course require a more or less linear process set of calculations on how much of each value is equal to how much of each other value. He could then proceed to examine all possible policy alternates. In a third step, he would undertake systematic comparison of his multiple of alternates to determine which attains the greatest amount of values.

In comparing policies, he would take advantage of any theory available that gene-
ralized about classes of policies. In considering inflation, for example, he would compare policies in the light of theory of prices. Since no alternatives are beyond his investiga-
tion, he would consider entire economic control and the abolition of all prices and mar-
enets on the one hand and elimination of all public controls with reliance completely on the free market on the other, both in the light of whatever theoretical generalizations he could find on such hypotheses economics.

In the second step, he would try to make the chart that would in fact maximize his values.

An alternative line of attack would be to set as his principal objective, either explicitly or without conscious thought, the relatively simple goal of keeping prices stable. This objective might be compartmentalized or complicated by only a few other goals, such as full em-
ployment. He would in fact disregard most other social values as beyond his present in-
terest, and he would be the moment not even attempt to rank the few values that he re
garded as immediately relevant. Were he as great as he were, he would quickly admit that he was ignoring many related values and many possibly important consequences of his policies.

As a second step, he would confine those relatively few policy alternatives that occurred to him. He would then compare them. In comparing his limited number of alternatives, most of them familiar from past controversies, he would not disorderly find a body of theory precise enough to carry him through a com-
parison of their respective consequences. In
tead he would rely primarily on the record of past experience with small policy steps to pre-
dict the consequences of smaller steps exten-
sed into the future.

Moreover, he would find that the policy alter-
natives combined objectives or values in different ways. For example, one policy might offer price level stability at the cost of some
SE Thought Provokers

• Does the INCOSE Boundary Definition of a System need to be amended?
• Does recognition of underlying order in apparently random, chaotic activities allow the possibility of limited prediction and/or control?
• Do we have a chance of designing and building an effective Control System for a Superintelligence?
• Will the ubiquity of 5th Generation comms from all kinds of devices and systems overwhelm our ability to effectively respond to anything within a digital world blanketed by unceasing queries, requests, and communications?
• WHO really thinks it is their job to solve the Aging Infrastructure problem?
**Artificial Intelligence**
- AI has the real potential to result in a National crisis.
- SE Vision 2025 only generally addresses AI, but smart people are out there working it.
- Members’ papers on new adaptive methods are specific and focused about the engineering way ahead.
- AI is still a specialized discipline that more Systems Engineers need to be knowledgeable or expert about.
- INCOSE should be addressing the future AI training needs for all SEs.

**5th Generation Communications Ubiquity**
- INCOSE is addressing this threat through its focus on Cyber Security, Virtual Engineering, and SoS.
- INCOSE should be addressing the future 5G training needs for all SEs.

**Aging Infrastructure**
- This problem haunts us all because of funding and needed government leadership. Could INCOSE be better engaged?
- Aging Infrastructure, Porous 5G networks, and AI will interact with crisis results.

**Takeaways**
- Not all engineering problems will be linear, self-contained, or well-bounded. i.e. we are solidly in the era of the non-linear, unbounded engineering problem and it is challenging our ability to solve problems using older methods.
- Current Adaptive, Model-Based SE is the correct approach for addressing complexity, and delivering quality, SE solutions.
- SEs will always need to learn new methods and keep learning new methods to tackle today's problems.
Books

These books are cited throughout the presentation
Notes, Books and References

- Wikipedia and Intellipedia are cited throughout the presentation
- Any uncited images are coordinated through Google’s Image Search and have either Public Domain or Fair Use usage rights associated with the image.

- [https://www.cns.nyu.edu/~david/handouts/linear-systems/linear-systems.html](https://www.cns.nyu.edu/~david/handouts/linear-systems/linear-systems.html)
- [https://www.infrastructurereportcard.org/solutions/leadership-planning/](https://www.infrastructurereportcard.org/solutions/leadership-planning/)
Papers

These papers are cited throughout the presentation

• Ahmad, Ijaz & Kumar, Tanesh & Liyanage, Madhusanka & Okwuibe, Jude & Ylianttila, Mika & Gurto, Andrei. (2017). 5G Security: Analysis of Threats and Solutions. 10.1109/CSCN.2017.8088621.

• https://www.howtogeek.com/423720/how-worried-should-you-be-about-the-health-risks-of-5g/