THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

VOLUME 14 NUMBER 7

April 2015
Transportation Sector

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

Follow us on Twitter here
Like us on Facebook here

This month, our authors discuss aspects of security and resilience within the Transportation Sector. After the article in the April 14 edition of the Wall Street Journal (http://on.wsj.com/1JEBOIY) that described the possible effects of an oil train accident, the topics of transportation sector resilience and security and the cascading effects of incidents in this lifeline sector take on an added relevance.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

Michel Dinning, Director of Multimodal Programs and Partnerships at the U.S. Department of Transportation's Volpe National Transportation Systems Center, opens this month's issue with an article on the challenges of transportation security and resilience in a connected world. This is followed by an article from David Buczek, Senior Fellow with the Center for Infrastructure Protection and Homeland Security, on the principles of effective resilience and security management that are relevant across all modes of the transportation infrastructure.

Next, colleagues from Argonne National Laboratories - Roland Varriale, Michael Thompson, and Dr. Nathaniel Evans - present a survey of Argonne's current work on vehicle security. Denise Rucker Krepp, professor of Homeland Security with Pennsylvania State University, discuss the growing reliance of the maritime transportation sector on foreign-flagged ships.

The U.S. Department of Homeland Security provides an update on "Project Jack Rabbit," a successful public-private partnership which highlights the interdependencies between the transportation and chemical sectors. In an article written jointly by Argonne National Laboratory, Delft University of Technology (Netherlands), and Radboud University (Netherlands), an overview of transportation planning methods for coping with climate change uncertainty is presented. Finally, Dr. Silvana Croope, of the Delaware Department of Transportation, gives a strategic state perspective on transportation infrastructure security and resilience. We would like to take this opportunity to thank this month's contributors. We truly appreciate your valuable insights and the rich dialogue that accompanies each issue.

Best Regards,

Mark Troutman, PhD
Director, Center for Infrastructure Protection and Homeland Security (CIP/HS)

Transportation Security and Resilience – Challenges in a Connected World

by Michael G. Dinning*

A Culture of Resilience

"It's really nothing short of miraculous; all of the facilities involved in this project have accomplished things they were never designed to do." That's how Jim Larson of the National Air Traffic Controllers Association described the response of FAA controllers, who scrambled to restore flight operations after a fire closed the air route traffic control center near Chicago in September, 2014.[1] As a result of the fire, which was set by a disgruntled contractor, the FAA declared "ATC Zero," shutting down over 91,000 square miles of airspace in one of the busiest areas in the country, and disrupting thousands of flights. The response of controllers was considered heroic by many. Even before they received orders to do so, many jumped in their cars and drove to control centers in neighboring states to help restore air traffic control in the Chicago region.[2]

The air traffic control facility fire incident highlights the importance of information technology, communications and control systems in our national transportation system. It also provides an example of three key characteristics of resilience: robustness, redundancy, and adaptiveness. These features were all present, but were challenged by the extreme event. The air traffic control facility was **robust**, with physical access control systems providing physical security, but the contractor was a trusted employee—an insider threat who had access to secure areas. The communications networks were **redundant**, but both the primary and the back-up network cables were destroyed. Nearby air traffic centers provided overall system redundancy and took over the Chicago-area traffic but at reduced levels. Finally, the staff and systems were **adaptive**, as they reconfigured the functions of other centers to handle operations in Chicago and reverted to manual procedures using paper forms and telephones to replace the automated system. Their efforts were laudable, but it was challenging for the controllers to adapt quickly. Improvements under the Next Generation Air Transportation System (Next Gen) initiative promise to provide additional system resilience, but the preparation and training of personnel to adapt and respond to extremely challenging disruptions will continue to be essential to maintain a culture of resilience.

91,000 square miles of "ATC Zero" following the Chicago air traffic control facility fire (adapted from image posted on Twitter)

The Chicago air traffic control fire highlighted the need for a systems approach to security and resilience. We need to address all aspects of the system, including physical, cyber, and personnel security. To do this effectively, security and resilience must be built into our systems, policies, and procedures from the earliest stages of planning, to system design and operations.

New Challenges in Transportation

Our transportation system is transforming, and much of this transformation is based on information technologies and communications. Our vehicles and fixed infrastruc-

(Continued on Page 3)

[1] Ernie Smith, "Air Traffic Control Center Recovers from Fire, But Broader Challenges Linger," *Associations Now* (October 22, 2014), available at http://associationsnow.com/2014/10/air-traffic-control-center-recovers-fire-broader-challenges-linger/.

[2] David Hirschman, "Inside the Chicago Center Fire: ATC Zero," *AOPA* (November 6, 2014), available at http://www.aopa.org/News-and-Video/All-News/2014/November/06/ATC-Zero-Inside-the-Chicago-Center-fire.

(Continued from Page 2)

ture are becoming connected and automated. Autonomous cars and aircraft are being developed, generating strong interest. Travelers have access to real time information on an ever-expanding range of mobility choices. Transportation is vital to our global economy, with just-in-time supply chains now the norm. Most importantly, we are connected as never before: to information, devices, and to each other. Indeed, the Internet of Things is alive and well in transportation. At the same time, we face a variety of new threats, including cyber attacks, on our critical information systems and networks. These transformational changes will demand and enable new approaches to transportation security and resilience.[3]

In this brief paper, I will give several examples of the challenges facing transportation today and suggest that we must take a collaborative, multi-modal, systems approach to keep our transportation systems secure and resilient. I will focus on two themes:

- Our cyber infrastructure (information technologies and communications) is critical and must be secure and resilient; and

- Smart and connected systems can greatly enhance transportation system resilience.

We Are Dependent on Information Technology

Virtually every part of our transportation infrastructure is dependent on information systems and networks. This dependence is growing rapidly, with initiatives like Next Gen and e-enabled aircraft in aviation, positive train control for railroads and transit, and connected and automated technologies for cars, trucks, and busses. Our pipeline networks are controlled by supervisory control and data acquisition systems (SCADA). The maritime industry has e-enabled ships with integrated bridge systems.

We all encounter transportation control systems daily. Highway traffic signals are monitored, and often controlled, from central traffic management centers. Intelligent transportation systems (ITS) such as dynamic message signs, traveler information systems, and video cameras have become essential to managing traffic in congested areas. The importance of traffic control systems was painfully clear to thousands of commuters in Washington, DC, when an aging computer server failed in the traffic management center several years ago, causing disruptions to traffic signals and massive traffic delays.

Highway ITS systems may also be vulnerable to deliberate attacks. Hackers have found it easy to put messages like "Zombies Ahead" on roadside message signs. While this type of attack is not normally a great risk to transportation operations, misleading information could be dangerous in situations like emergency evacuations. Researchers have identified potential vulnerabilities in traffic signals which could put entire networks at risk.[4] Some of these vulnerabilities can be mitigated with relatively easy fixes, such as making sure devices aren't deployed with the factory-installed passwords, but others require comprehensive "Defense in Depth" strategies, coordinated with the organization's information technology security programs.[5]

Ensuring Our Cyber Systems are Robust and Resilient

Clearly, the cyber networks supporting highways, airports, transit systems, and other modes of transportation need to be protected and resilient, but the scope of the challenge is immense. How do transportation agencies which are dependent on thousands of information and control systems ensure that the most critical cyber risks are addressed? It's a challenge faced by all types of infrastructures, and many of them, like energy and communications, are critical to transportation. In 2013, the White

(Continued on Page 4)

[3] "Beyond Traffic: US DOT's 30 Year Framework for the Future," *United States Department of Transportation* (Updated March 20, 2015), http://www.dot.gov/BeyondTraffic.

[4] Brendan Harris, "Hacking Traffic Controllers," Presentation to AASHTO Security Summit, August 2013, available at http://onlinepubs.trb.org/onlinepubs/conferences/2013/SecuritySummit/presentations/21harris.pdf; Branden Ghena, et al, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure," Proceedings of the 8th USENIX Workshop on Offensive Technologies, August 2014; Edward Fok, "You've Been P0wned: Summary of Recent Cybersecurity Incidents and Threats," Presentation at TRB Annual Meeting, January 14, 2015.

[5] Edward Fok, "Cyber Security Challenges: Protecting Your Transportation Management Center," *ITE Journal* (February 2015): 32-36, available at http://library.ite.org/pub/898748dd-0c0c-2cb9-c9db-0cac2bc3bd7d.

(Continued from Page 3)

House issued Executive Order 13636 to address this challenge, making cyber security a national priority. To help guide this national effort and facilitate sharing of experiences and best practices, the National Institute of Standards and Technology (NIST) developed a Cybersecurity Framework. Transportation agencies are now using the NIST Framework and are developing metrics to evaluate and prioritize risk mitigation efforts.[6] In addition, NIST developed a Cyber Resiliency Review to help organizations assess their cyber resilience, and additional guidance and coordination is focused on the resilience of cyber-physical systems and smart cities. DHS summarizes the strategies of the transportation sector in the *Transportation Systems Sector-Specific Plan*, which is being updated to address the latest challenges in cyber security and resilience.

Many transportation operators have assumed that the risks to their systems were minimal because they were "closed" or "air-gapped" systems, but even these may be vulnerable. For example, a 14-year-old boy in Poland used a modified television remote controller to change the signals on his local transit system, derailing four trams. Never envisioning this type of attack, the transit agency failed to build in safety measures to prevent derailments if the signals were deliberately set incorrectly. This is a good example of the need for an "all-hazards" approach, where safety and security hazards are considered together as part of system risk management.[7]

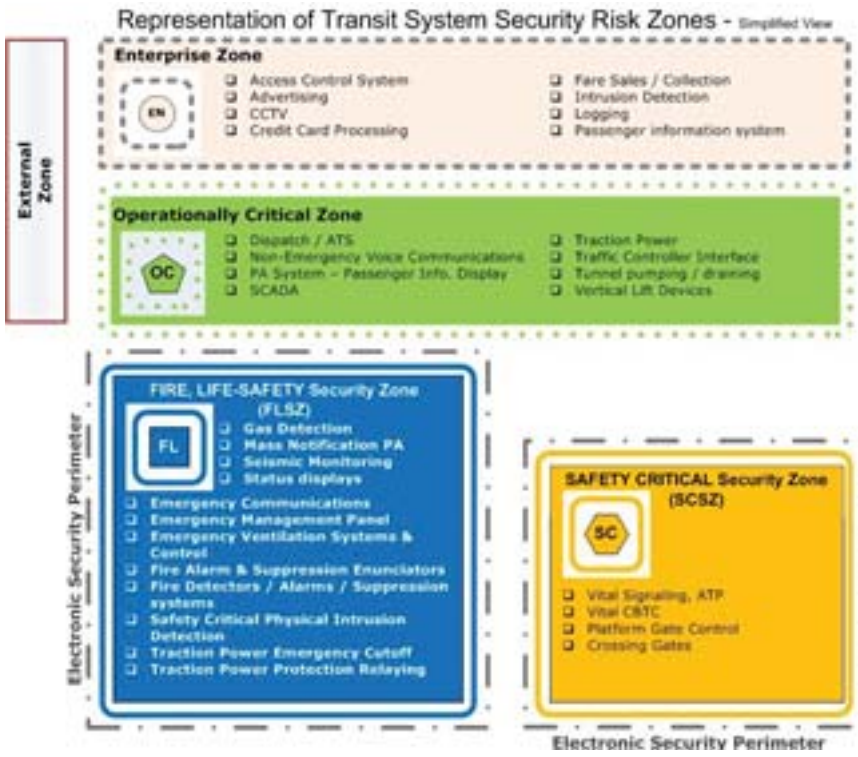

Image from reference 9

Vehicle designers have been working to find ways to minimize the risks from cyber attacks or other types of cyber-physical system failures. Designers of aircraft, transit vehicles, and automobiles are promoting the

(Continued on Page 5)

[6] Craig Schumacher, Idaho Transportation Department's Application of the NIST Cyber Security Framework, TRB Cyber Security Subcommittee Telconference, April 2, 2015, exhibit on TRB Cyber Security Resource Center, http://trbcybersecurity.erau.edu/.
[7] John Leyden, "Polish teen derails tram after hacking rail network," *The Register* (Jan. 11, 2008), available at http://www.theregister.co.uk/2008/01/11/tram_hack/.
[8] Charlie Miller and Chris Valasek, "A Survey of Remote Automotive Attack Surfaces," Paper presented at Black Hat USA 2014 in Las Vegas, NV, August 6 & 7, 2014, available at http://www.scribd.com/doc/236073361/Survey-of-Remote-Attack-Surfaces; "Car Hacked on 60 Minutes," *CBS News* (Feb. 6, 2015), available at http://www.cbsnews.com/news/car-hacked-on-60-minutes/.

(Continued from Page 4)

idea of separating systems or "information domains" on the vehicle according to risk. This concept is also being applied to include fixed infrastructure systems. Risk is reduced by separating or protecting information used in safety-critical systems from the information used to operate non-safety functions or provide passenger entertainment.[9]

Redundancy is another key element of resilience, and we need to ensure that we have back-up technology or procedures for critical capabilities like GPS-based position, navigation, and timing systems. Many operators are heavily reliant on GPS (including most of us without paper maps in our cars), which has been found to be vulnerable to jamming and spoofing. A recent Federal Register notice is asking for comments on this critical issue, and many designers and equipment suppliers are considering building in redundant navigation capabilities in case GPS fails.[10] As we learned from the air traffic control fire, it is essential that we have back-up or down-time policies and procedures, and that we have the staff trained and available to apply them. The availability of staff during emergencies is a major challenge in transportation, as our human capital is stretched thin and there is not a lot of depth in critical expertise. Cyber failures must be included in continuity of operations plans and should be part of exercises, and these should involve multiple transportation modes and related industries.

Moving to a Connected and Automated World

Some of the most revolutionary new technologies are emerging with connected and automated vehicles. In the future, cars and trucks may be connected with high speed digital communications, detecting impending collisions and significantly reducing accident risks. Automated cars, trucks, and aerial and maritime vehicles are emerging, all incorporating dozens of cyber physical systems. In aviation, unmanned aerial vehicles are expected to surpass manned aircraft operations by 2035.[11]

Cyber risks in automated systems are a key concern, whether from deliberate attack or equipment failure. Automated systems must be designed to be adaptive and be able to stop safely or resort to manual operations if automation fails. The reaction of drivers to automation is also a concern. If vehicles are autonomous, will operators be able to respond to system failures? As one human-factors expert suggested, "It's hard enough to have the human understand what the computer's doing, but having the computer understand what the human's doing is an even bigger challenge."[12]

The automated transportation systems of the future not only need to be secure and resilient, they also need to be discrete. Some drivers are concerned about privacy and do not want to be tracked by connected vehicle systems. We need to be able to ensure that the signals being exchanged between vehicles are authentic and at the same time ensure that the privacy of drivers is not compromised. The scalability of this type of vehicle authentication scheme to the entire national transportation system is an unprecedented challenge.[13]

Using Connected Smart Systems to Ensure Resiliency

In addition to e-enabled vehicles, the transportation fixed infrastruc-

(Continued on Page 6)

[9] "Securing Control and Communications Systems in Rail Transit Environments," *APTA Recommended Practice*, APTA-SS-CCS-RP-002-13 (June 28, 2013), available at http://www.apta.com/resources/standards/Documents/APTA-SS-CCS-RP-002-13.pdf.

[10] Karen Van Dyke, "We Need Backup! Potential Vulnerabilities and Risks in the Global Positioning System," Presentation at Transportation Research Board Annual Meeting, January 14, 2015; Complementary Positioning, Navigation, and Timing Capability, 80 Fed. Reg. 15268 (Mar. 23, 2015)(Notice, Request for Public Comments), available at https://www.federalregister.gov/articles/2015/03/23/2015-06538/complementary-positioning-navigation-and-timing-capability-notice-request-for-public-comments.

[11] John A. Volpe National Transportation Systems Center, *Unmanned Aircraft System (UAS) Service Demand 2015 – 2035: Literature Review and Projections of Future Usage* (Cambridge, MA: United States Department of Transportation, 2014), available at http://ntl.bts.gov/lib/51000/51400/51460/UAS_Service_Demand_2015-2035_Version_1_0.pdf.

[12] Dr. Thomas Sheridan, "Automation and the Human: Intended and Unintended Consequences," Roundtable hosted by John A. Volpe National Transportation Systems Center, April 13, 2012, available at http://www.volpe.dot.gov/events/automation-and-human-intended-and-unintended-consequences.

[13] "Connected Vehicle Test Bed," *United States Department of Transportation Intelligent Transport Systems Joint Program Office* web site, http://www.its.dot.gov/connected_vehicle/dot_cvbrochure.htm. (Last visited Apr. 23, 2015).

(Continued from Page 5)

ture is becoming smarter, too. ITS systems already provide real-time information on traffic, signals, and weather conditions. Infrastructure designs are incorporating sensors into bridges, roadways, and other structures, which give us situational awareness of structural conditions.

The I-35 bridge collapse in Minnesota has been cited as an example of lack of resilience because of the weaknesses in the bridge's "fracture-critical" design features. But the response and recovery from the bridge collapse demonstrated many desirable attributes of resilience which leveraged ITS technologies. Within seconds of the collapse, the traffic management center was able to assess the situation with video cameras. Emergency responders from many agencies were able to communicate and coordinate their response using programmable radios with prioritized transmissions. There was a vast network of traffic sensors built into the roads in the region, and they had collected detailed data on road performance. When the disaster occurred, the Minnesota DOT was able to create alternate routes within hours, and then monitored the traffic changes carefully to identify bottlenecks and safety problems. The new bridge was constructed in less than a year, thanks to experts dedicated to the project and a streamlined procurement and approval process. The new bridge was built to be significantly more resilient. The structure has separate spans for each direction and space for light rail transit to be added in the future. The bridge incorporates reinforced designs, and has embedded sensors to monitor strains on the structure. The new I-35 bridge exemplifies what many feel should be the goal of recovery efforts: to "build it back better."[14]

Connected vehicles will provide additional situational awareness in the future. They are part of the internet of things and the smart city, collecting and transmitting large amounts of information in real time. Connected vehicles may act as nodes, generating information on weather, roadway conditions, and congestion.[15] Travelers themselves are becoming sources of real-time information, providing information on congestion, weather, and system problems. Social media and crowdsourcing was used in Hurricane Sandy, and the information enriched the situational awareness provided by more traditional information sources.

Transportation systems and users are producing truly "big data" that is improving situational awareness and our ability to adapt to disruptions. For example, more accurate weather data and modeling allows meteorologists to predict the impacts of tidal surges more precisely. During Hurricane Sandy, the New York MTA took preventative actions based on these forecasts, closing tunnels, protecting low-lying infrastructure and moving their transit vehicles to higher ground. These efforts avoided millions of dollars of potential damage.[16] Remote sensing technologies, like satellites and aerial vehicles, can provide real-time information on the conditions of transportation infrastructure and the progress of recovery efforts.[17]

Collaboration is Essential

Emergency managers know that relationships and collaboration are essential to effective response. To ensure that our transportation systems are resilient, however, we need collaboration throughout the system life cycle, from planning to operations. In the ITS community, experts have been collaborating for years on system-level security architectures and standards, and these must be updated to reflect emerging technologies. New technologies are being introduced in transportation so rapidly that the impact on the security and resilience of the overall system is not always well understood. Reference architectures and standards are needed to ensure that all modes of transportation are robust to cyber threats. The DHS is sponsoring formation of an Automotive Industry Cyber Security Research Consortium to enable manufacturers and suppliers to collaborate on a pre-competitive

(Continued on Page 7)

[14] Thomas Fisher, Designing to Avoid Disaster: The Nature of Fracture-Critical Design, (Abingdon, UK: Routledge, 2012).
[15] Matthew Cuddy, et al, *The Smart/Connected City and Its Implications for Connected Transportation*, FHWA-JPO-14-148 (Cambridge, MA: United States Department of Transporation, 2014), available at http://www.its.dot.gov/itspac/Dec2014/Smart_Connected_City_FINAL_111314.pdf.
[16] Surviving Sandy – the Superstorm That Reshaped Our Lives (Airmont, NY: Ambient Funding Corp., 2013): 32-35.
[17] Greg Winfree, "UAVs hit the mark in disaster assessment," Fast Lane, *The Official Blog of the U.S. Department of Transportation* (March 26, 2015), https://www.dot.gov/fastlane/uavs-help-disaster-assessment.

(Continued from Page 6)

basis to develop more secure and resilient designs. Similar efforts are underway in other modes.

To disseminate threat information and help coordinate effective responses to incidents, information sharing and analysis centers (ISACs) have been formed for most modes of transportation. The Federal Highway Administration has recently established a capability to do this for their stakeholders at the National Operations Center of Excellence run by the American Association of State Highway and Transportation Officials.[18]

A collaborative, multimodal approach to transportation recovery is lacking, however, and this could severely hamper our ability to minimize disruptions and recover quickly from large scale incidents. After Hurricane Sandy, for example, freight movements were disrupted for truck, rail, air, and maritime transportation, and diversions impacted ports hundreds of miles away. Transportation systems cannot adapt to disruption quickly if resiliency is not considered in regional transportation improvement plans. These plans must take into account passenger and freight requirements in the region, and the potential impact of disruptions to the national and global economies. Public- and private-sector organizations must develop relationships and coordinate their plans to be prepared to recover from all types of transportation disruptions. These collaborative efforts need to address cyber risks, which should be a part of exercises and regional recovery planning.

Involvement of the community is an essential part of transportation resilience. One of the lessons from the severe winter storms in Boston in 2015 was that the transportation community needs to coordinate their recovery actions, and communicate accurate and timely information to the public on the status of recovery efforts for all modes of transportation. The importance of this was seen in the San Francisco Bay area when it was faced with "Carmageddon" during the repair of the Bay Bridge. Transportation officials prepared for the potential traffic nightmare by developing multimodal contingency plans, which they publicized widely to local employers and commuters. As a result, traffic problems during construction were minimal.[19]

Final Thoughts

We're demanding more from our transportation system than ever before, and technology is helping us meet these demands. We need to make sure that we build security and resilience into our evolving transportation infrastructure and our myriad connected systems. Our smart systems are giving us situational awareness and connections that will enable us to adapt to potential disruptions with coordinated, collaborative efforts. The users of our transportation system don't think in terms of separate "modes" of transportation, so we need to give them multimodal solutions to ensure overall transportation resilience. Developing these strategies will require a collaborative effort among system planners, researchers, designers, suppliers, operators, supporting infrastructures, emergency managers, and the public. We all must take part in making our transportation system resilient.

**Michael Dinning is Director of Multimodal Programs and Partnerships at the U.S. Department of Transportation's Volpe National Transportation Systems Center, where he leads cross-cutting initiatives such as cyber security and transportation resilience. Dinning is chair of the Transportation Research Board subcommittee on cyber security, and teaches a graduate course in Transportation Security Management for the Massachusetts Maritime Academy. The thoughts in this paper are those of the author, and do not represent the policies or positions of the U.S. DOT.* ❖

[18] Robert Arnold, "Transportation Systems Cyber-Security Framework," Presentation at the TRB Cyber Security Subcommittee Meeting, January 13, 2015.

[19] Randell H. Iwasaki, "Beyond Bouncing Back," Roundtable on Critical Transportation Infrastructure Resilience at the Volpe Center, April 30, 2013.

Principles for Effective Security and Resilience Management

by David A. Buczek*

Introduction

The nation's transportation sector is truly vast, with air, water, rail, and roadway modes each having their own unique vehicles, infrastructure, and management systems. Identifying and integrating a common approach to security and resiliency into each unique mode is challenging, and coordinating efforts across modal touch points is even more daunting. Perhaps by examining the past we can define principles that can be used today irrespective of the intricacies within and across transportation modes. Admiral Hyman G. Rickover, the "Father of the Nuclear Navy," devised and implemented many of the management principles that resulted in an operational record for the nuclear navy that is second to none. By looking across his writings, and anecdotes written by those who worked directly with him, we can identify five guiding principles that are applicable to developing and integrating an effective security and resilience mindset into the day-to-day management of modern transportation systems.

Source: PBS

Five Guiding Principles

1. Develop tactical plans within a strategic context.

When Rickover began his efforts to create the nuclear navy he understood that he was at the forefront of an entirely new industry. Nuclear power held the promise of allowing submarines to operate for months without coming to the surface and ships to ply the seas for thousands of miles without refueling. But at that time, nothing existed to support turning that promise into reality. Everything required to design, supply, build, field, and support his nuclear submarines and ships was yet to be created. Rickover knew that new and highly complex reactor systems needed to be designed and created; new materials developed; submarine and shipbuilding techniques enhanced; unseen radiation and its effects better understood and controlled; and many other equally complex issues had to be dealt with. With a detailed vision of the future, he took the methodical, tactical steps needed to systematically work his way towards that desired future state.

Source: PBS

On multiple and parallel tactical development tracks and timelines he helped to build the entire industry that was needed to achieve his strategic goal.

2. Understand and mitigate the greatest risks to your ultimate success.

Radiation is a byproduct from nuclear reactors. Rickover tasked his senior engineering staff with determining how much shielding would be required around the reactor of the first nuclear submarine, the Nautilus, to adequately protect the crew. His staff met with numerous experts in the field and decided the Navy could use less shielding, and therefore expose the crew to more radiation than was allowed per civilian standards for the time, and still be somewhat safe. Rickover would hear none of it. He told his staff that they would meet or exceed any civilian or international stan-

(Continued on Page 9)

(Continued from Page 8)

dard.[1] His rationale was simple. He knew that the public feared radiation, and that the politicians that represented the people were some of his chief sponsors. If the crews of his submarines became ill or were adversely affected by radiation, not only would his submarines not be able to complete their missions for the Navy, but also the public would not stand for it.[2] His vision of a fleet of nuclear submarines would never materialize if political support waned. Astute enough to recognize one of the greatest risks to his program he took decisive action early to reduce the risk to the largest extent that he could.

3. Acquire and leverage real world examples of success.

Rickover was a man of action committed to getting things done. To accomplish his goals he needed the ability to cut through bureaucracy and demonstrate that he was producing results that required continued support and funding. He did this by showing his sponsors the small successes that would lead to major successes. In his excellent book *The Rockover Effect*, Theodore Rockwell, who worked directly with the Admiral as his Technical Director, recounts that Rickover said, "You gotta show 'em examples." And that is exactly what they did. They provided samples of new materials for the reactors, mockups, and test rigs. According to Rockwell, Rickover's sponsors "…never doubted they were dealing with a person who was actually creating important, working hardware in the real world."[4] By demonstrating what was producing tangible results, Rickover was able to secure funding, cut through red tape and accomplish his more important, larger goals.

4. Take a systems approach to problem resolution.

When the *Nautilus* was being built and its reactor not yet started, a test was conducted of its steam plant using steam produced on the pier to which the submarine was secured. During the test a small steam line burst. After a rigorous investigation it was found that the burst pipe was not the quality and type of pipe that was supposed to have been installed in the steam plant. Compounding the problem, there was no way of telling which portions of the thousands of feet of pipe now installed were correct and which were not because it all had been covered with insulation. Rickover made an immediate decision to remove all of the suspect pipe and replace it. Equally important, he initiated an inquiry to determine first, how the inspection system at the shipyard had failed and allowed the wrong pipe to be installed, and second, what was required to remedy the quality control processes so that such a mistake could not happen again.[5] Rickover knew that no incident was the result of a single cause, and that the entire chain of events needed to be analyzed and then the overall quality control system adjusted so that such an error would not happen again.

5. Research failures to find the keys to success.

In a speech at the Naval Postgraduate School in 1954, Rickover listed 12 ideas that he tried to convey to people who worked for him. The fifth idea was that "Success teaches us nothing, only failure teaches."[6] Rickover was obsessed with encouraging his people to "Do what is right." He hired incredibly able individuals and coached them to challenge their internal blind spots and base decisions on data and facts no matter which direction they took them. Enabling his people to do what was right meant ensuring that if they did so, and negative consequences ensued, then the whole system had better learn from it so mistakes were never repeated. He knew that failures, large and small, were learning points for the program he was trying to build and the lessons from these failures had to be studied and dealt with. As a result of this and other activities, the nuclear navy's complex system of systems has experienced an ever-increasing level of safety over the decades since its inception.

Application to Transportation Infrastructure Security and Resilience

(Continued on Page 10)

[1] Theodore Rockwell, *The Rickover Effect* (Lincoln, iUniverse, 2002): 121-123.
[2] Dave Oliver, *Against the Tide* (Annapolis, Naval Institute Press, 2014): 50.
[3] Rockwell, *The Rickover Effect* 168.
[4] ibid.
[5] Rockwell, *The Rickover Effect* 183-185.
[6] Oliver, *Against the Tide* 159-160.

(Continued from Page 9)

There are many more management lessons that can be gleaned from researching the efforts of Admiral Rickover, but these five seem particularly appropriate for leaders and managers who seek to enhance the security and resilience of our complex transportation system of systems. Using each principle, a set of questions can be developed and methodically examined to help identify areas of risk, and lay out solution paths that enhance transportation security

Principle	Starter Questions
1 - *Develop tactical plans within a strategic context.*	1. What strategic level security and/or resilience goal needs to be achieved in your transportation mode, in other modes that touch your mode, or across modes? 2. What sub-goals (components) need to be in place to achieve the higher-level goal? 3. What are the resource (government, industry, academia) requirements, integration touch points, and stakeholder support required for the strategic and all component goals? 4. What parallel building block pathways are required to establish the foundation necessary to build-out each component of the overall system? 5. What tactical plans can be established, managed, implemented and tracked that, when placed end-to-end and side-to-side, result in the ultimate goal of increased security and/or resilience?
2 - *Understand and mitigate the greatest risks to your ultimate success.*	1. What are the greatest risk(s) that if they came to fruition would result in the cancelation of your efforts to improve security and/or resilience of your mode? 2. What stakeholder and/or sponsor support for your efforts would be lost if these risks came to fruition? 3. What are the hazard(s) from which these risks emanate? 4. How can these hazards be controlled out of your system and/or be mitigated? 5. After your control and mitigation efforts, what will the effect of the residual risk be on your efforts to improve security and/or resilience?
3 - *Acquire and leverage real world examples of success.*	1. What real world examples of security and/or resilience approaches, or components of approaches, have already been developed in your mode, or other transportation modes, and are proving successful in use? 2. What real world examples have already been developed in other infrastructure components and are proving successful in use? 3. How might leveraging these components garner support for your efforts to build the components you need on your roadmap towards your ultimate strategic goal? 4. What types of examples, mock-ups, showcase projects, etc., do your key stakeholders or sponsors expect and will likely result in tangible support? 5. What resources are required to develop these examples to demonstrate your forward progress and secure ongoing resource allocation to your efforts?

(Continued on Page 11)

(Continued from Page 10)

4 - *Take a systems approach to problem resolution.*	1. Stepping back, what different perspectives can you gain when examining the goal you are trying to achieve? 2. How do these additional perspectives and an understanding of the overall environment inform the goal you are trying to achieve? 3. What are the dynamics and the interrelations between the components of the system or systems you are trying to change and how do they change over time? 4. What are the root causes of the issues we are trying to address and what needs to change across the system to address each contributory element? 5. After developing change plans that are informed by the above analysis, how do we best ensure that feedback about the new system state is received and evaluated to ensure we have achieved the changes we desired without creating unintended negative outcomes?
5 - *Research failures to find the keys to success.*	1. What failures in security or resilience have occurred in your transportation mode, in other modes, or across modes that could severely affect your mode? 2. What were the contributing and causal factors that led to the failure? 3. What inspection, quality control, and/or system control points were present but unsuccessful in preventing the failure? 4. What controls exist, or need to exist in your mode to prevent similar failures? 5. What mitigations exist or need to exist in your mode to prevent similar failures?

All systems are different, and no best practice is universally applicable. However, by using these questions as a starting point, perhaps transportation infrastructure leaders and managers will make better and more effective security and resilience decisions today by leveraging Rickover's principles from our past that have proven so successful.

**David A. Buczek, MA, is the President of DB&A and is a Fellow at the George Mason University, School of Law, Center for Infrastructure Protection and Homeland Security in Fairfax, Virginia. He can be reached at (703) 861-5332 or dave.buczek@dbainnovation.com.* ❖

A Survey of Current Work on Vehicle Security and Vehicle Security Considerations

by Roland Varriale, Michael Thompson, and Dr. Nathaniel Evans*

Intoduction

Modern automobiles each contain upwards of 50 electronic control units (ECUs) that control and monitor system activities as well as interact with the running automobile in real time.[1] These ECUs provide signals that assist the vehicle in performing myriad actions -- from controlling the brakes and steering to interfacing with diagnostic tools for mechanics. The overall safety of the vehicle relies on real-time communication between these ECUs. Safety functionality makes heavy use of these ECUs in predicting crashes, detecting skids, performing anti-lock braking, and other functions.[2]

ECUs present a viable attack surface for performing various malicious acts. Although gaining control of a vehicle is the paramount concern of automotive security researchers, an attacker does not need control of the vehicle to trigger fatal system errors, thereby stopping the car or performing other damaging actions. Previous research has focused on both the car's physical attack surfaces (through an onboard diagnostic port) and the viability of remote attack surfaces. Our work assumes that a physical access breach can exist; we analyze the potential risks, consequences, and failure modes of uninformed, average knowledge, and sophisticated attacks on the control area network (CAN) bus.

Initial research into controlling automobiles occurred with direct physical access to the vehicle's CAN bus via the onboard diagnostic port (OBD/II). This CAN bus access was beneficial because it offered entry to unencrypted and unauthenticated messages, which can be viewed by any device present on that bus. This physical access offers the attackers a desirable medium both for analyzing the bus traffic and for transmitting messages to interact with the vehicle's sensors and motors. Technologies present in this attack surface include Bluetooth, Global System For Mobile Communications (GSM), and other cellular wireless protocols. Moreover, additional feature sets such as parking assist, keep lane assist, and assisted cruise control add additional communication pathways that may circumvent the logical flow of messages through their intended gateways.

Research performed at University of California—San Diego and the University of Washington has provided a comprehensive analysis of wireless attack surfaces ranging from Bluetooth to tire pressure-monitoring systems.[3] Their findings provide a high-level overview of various attack vectors and how these vectors contribute to the overall attack surface of modern automobiles. In particular, Bluetooth stacks offer desirable attack surfaces due to the pervasive nature of Bluetooth within automobiles. In addition, due to the weak segmentation of some CAN buses, it may be possible to transmit messages over a CAN bus once a device pairs with the Bluetooth module in the car. Normally, this process occurs through passcode authentication, where the device displays a code the user needs to input in order for the pairing to occur. However, in some cases, researchers have joined a Bluetooth device to a car by brute force or even bypassing the pairing

(Continued on Page 13)

[1] Charlie Miller and Chris Valasek, *Adventures in Automotive Networks and Control Units*, Technical Report, available at http://illmatics.com/car_hacking.pdf.

[2] Pierluigi Paganini, "Car Hacking: You Cannot Have Safety without Security," *INFOSEC Institute*, available at http://resources.infosecinstitute.com/car-hacking-safety-without-security.

[3] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, *Comprehensive Experimental Analyses of Automotive Attack Surfaces* (San Diego: Center for Automotive Embedded Systems Security, 2011), available at http://static.usenix.org/events/sec11/tech/full_papers/Checkoway.pdf.

(Continued from Page 12)

sequence. In the bypass case, car occupants were not able to detect or manually un-pair the device. This override of the pairing authentication could create a substantial risk and offer a foothold into the CAN bus thereby allowing the attacker to perform more nefarious actions.

Contol Area Network (CAN) Bus

The CAN bus is a standard industrial communication network designed to allow microcontrollers, referred to as ECUs, and sensors to communicate with each other within a vehicle.[4] The CAN bus is the main communication channel that carries messages to various physical components of the automobile, including actuators (which control brakes, steering, transmission), from sensors (which monitor electrical levels, fluids). The CAN is a broadcast-only bus, meaning there is no explicit address in the messages exchanged (sometimes called "content-oriented addressing"). All nodes in a network are able to receive all transmissions. There is no way to send a message to just a specific node. Instead, the bus uses an identifier that is unique throughout the network to label the content of the message. Each message carries a hexadecimal value, normally referred to as an arbitrary ID, which controls its priority on the bus, and serves as an identification of the contents of the message. Figure 1 shows an example of the layout of a CAN bus, logically grouped by functionality.[5] In a typical automobile CAN bus, a logical gateway would act as a buffer to prevent errant messages from being transmitted from one segment of the bus to another. However, if the proper packet were transmitted it could invoke a message to be transmitted across the gateway. Although these gateways perform a rudimentary form of message checking, by message ID, they were not created with external access protection in mind, and cannot be trusted to prevent malicious activity. One of the major security concerns with CAN messages is that they offer no authentication mechanism to identify both sender and receiver; therefore, the sender and the receiver are assumed to be who they are claiming to be. In a CAN bus network, authenticity is assumed based on presence on the bus. However, new devices and wireless protocols make this assumption problematic.

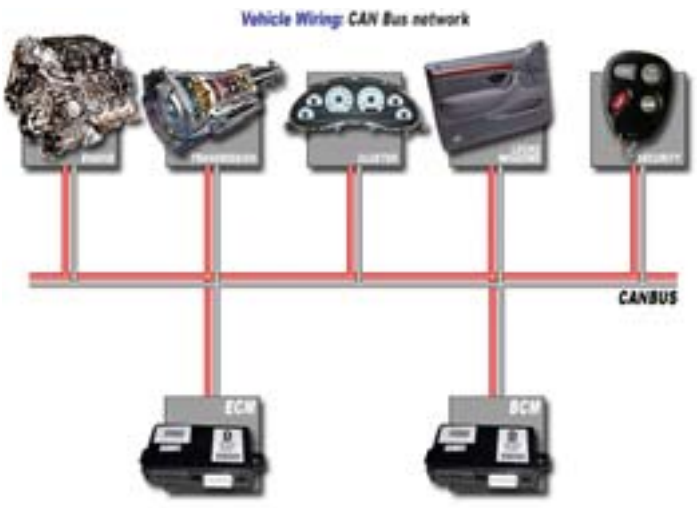

Figure 1. Example of a CAN Bus Layout[6]

The focus of the CAN bus design is on safety and system interoperability. If an ECU in a vehicle receives a message that it understands, it acts upon it; there is no way for an ECU to distinguish a legitimate message from a forged or spurious message. Although some methods have been proposed to fix this[7], none of the proposed methods have yet been implemented in vehicles.

Traditional Network Attacks on the CAN BUS

Access to a CAN bus exposes all of the ECUs connected to that bus.

(Continued on Page 14)

[4] Steve Corrigan, *Introduction to the Controller Area Network* (CAN), SLOA101A (Dallas: Texas Instruments, 2002, rev. 2008), available at http://www.ti.com/lit/an/sloa101a/sloa101a.pdf.

[5] EE Herald, "Module 9: Controller Area Network (CAN) Interface in Embedded Systems," in *Online Course in Embedded Systems*, available at http://www.eeherald.com/section/design-guide/esmod9.html.

[6] "What Is CAN Bus?," *CANBus,* http://canbuskit.com/what.php.

[7] Anthony Van Herrewege, Dave Singelee, and Ingrid Verbauwhede, *CANAuth - A Simple, Backward Compatible Broadcast*, presented at ECRYPT Workshop on Lightweight Cryptography (2011), available at https://www.cosic.esat.kuleuven.be/publications/article-2086.pdf; Chung-Wei Lin and Alberto Sangiovanni-Vincentelli, *Cyber-Security for the Controller Area Network (CAN) Communication Protocol*, in 2012 International Conference on Cyber Security (New York: IEEE 2012), available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6542519.

(Continued from Page 13)

This access can be obtained through many methods, both physical and wireless. As with many cyber-physical systems, network segmentation, such as isolating each ECU, would eliminate these exposures; however, it would also limit the convenience and responsiveness of the automobile. We have concerns about additional risks to vehicles that would occur after gaining access to the CAN bus, whether through legitimate means or by a security exploit. Such risks include denial-of-service (DoS) attacks or replay attacks.

DoS attacks are problematic in most network environments, and although there are no foolproof defenses against denial of service attacks, techniques such as whitelisting known entities and blacklisting bad actors are widely used as a mitigating technique. Unfortunately, many of these techniques require that a protocol have some recognition of addressing or authentication, neither of which are present in the CAN protocol. Networking authorities (e.g., Cisco) have offered insights into how to reduce DoS risk by using router-level procedures such as access lists.[8] The current implementation of the message inspection process offers a viable vector to an attacker using a flooding attack.

A message replay attack is relatively simple to perform once access to the CAN bus has been gained. As attacker sophistication increases, these attacks may have consequences with escalating severity. This form of attack may potentially be performed without specific knowledge of the car, such as make or model; however, the success of these uninformed attacks has not been explored. Researchers have created toolkits (e.g., the CHT) that are useful in executing specific actions, such as transmitting messages or sequences of messages on the CAN bus. If an attacker understands the message contents and sequence dependencies, he or she could issue commands that could disable the vehicle; it is possible to gain such an understanding by analyzing the messages broadcast over the CAN bus and replaying them. Since, as we previously noted, the messages are transmitted in an unencrypted format, any messages that are seen over the CAN bus can be replayed without any modification.

Using knowledge of the underlying network combined with the tools provided, an attacker could modify the CHT to utilize a different set of identification codes specific to the attacked car.

Premilinary Results

The potential consequences of the previously mentioned attacks ranged from simple electronics malfunction (such as the stereo ceasing to function) to complete physical disabling of the vehicle. Moreover, the lack of CAN segmentation may provide additional attack vectors and allow the compromise of one ECU to have potentially cascading consequences across the vehicle, possibly even endangering human life. Vehicles can be composed of one or more CAN buses (high-speed, medium-speed, low-speed), where level of security often correlates well to the number of buses and the gateways contained on those buses.[10] The vehicle chosen for our testing, a 2010 Toyota Prius serendipitously lacks major segmentation of the CAN and contains only a high-speed bus.

We evaluated the three stages of sophistication using the natural progression of an inexperienced attacker: we started by copying CAN bus messages from open-source documents and moved on to identifying ECU message IDs and forging messages and checksums. We did not fully achieve a completely "sophisticated" attack, which we believe would consist of advanced maneuvers such as bypassing or bridging gateways. We observed that the CAN is resilient to an inexperienced attacker, unless that attacker were to employ exact replay attacks of a specific car's make, model, and year. However, once the

(Continued on Page 15)

[8] "Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks," *Cisco* (2008), available at http://www.cisco.com/c/en/us/support/docs/security-vpn/kerberos/13634-newsflash.html#prevention.

[9] Lucian Constantin, "Hacker Coalition Sets out to Improve Critical Device Security, Challenges Car Makers," *PC World* (Aug. 10, 2014), available at http://www.pcworld.com/article/2463420/hacker-coalition-sets-out-to-improve-critical-device-security-challenges-car-makers.html.

[10] Andy Greenburg, "How Hackable Is Your Car? Consult This Handy Chart," *Wired* (Aug. 6, 2014), available at http://www.wired.com/2014/08/car-hacking-chart.

(Continued from Page 14)

message IDs are identified it can be simple to start sending messages to interact with those components—and some of these specific message codes are available on the Internet.

Our experimentation on the 2010 Toyota Prius paralleled the work performed by Miller and Valasek; however, our vehicle did not have the lane keep assist or parking assist options present in their vehicle. Throughout our testing, we were able to exactly replicate the results they obtained using the same message IDs and packet data contents. Although the message IDs and contents were replicated across the same make, model, and year, it is very unlikely that this would be the case if any of those criteria were to change. During the course of our testing, we realized that several codes that were marked as a diagnostic 7-series message could be transmitted even when diagnostic mode was not enabled. This should not be possible, according to the specifications of the car's service manual.

Conclusion and Future Work

Since the majority of current completed research has taken place in stationary vehicles or at low speeds, no exploration of the consequences and failure modes of attacks on most modern vehicles has been published. Without additional information, it is natural to assume extreme consequences: that a naïve attacker could disable a vehicle or accidently trigger a steering or brake event, and that a sophisticated attacker could exercise full, unimpeded control of the vehicle. Our work aims to frame future discussions of consequences and failure modes to pave the way for security improvements to the CAN bus that will mitigate current vulnerabilities. We aim to create and test a histogram-based approach to message transmission frequency, originally proposed by Miller and Valasek. Moreover, we previously mentioned that some ECUs restrict messages to using certain message IDs over the CAN bus. For example, if to change the speed displayed on the car's dashboard we have several options: (1) transmit a message saying that the wheels are rotating at rate x, (2) transmit a message containing the ID that the dashboard recognizes (thus triggering a display change), or (3) transmit a message that is recognized by rear wheels in order to synchronize wheel speeds. In fact, many powertrain and battery activities can be cross-referenced in order to offer another layer of protection against forged messages and replay attacks. We propose that automobiles be built with these internal checks in place, in order to increase the skill level needed to compromise many car functions that are currently easy to transmit messages to.

Acknowledgement

The work presented in this paper was partially supported by Argonne National Laboratory under DOE contract number DE-AC02-06CH11357. The submitted manuscript has been created by UChicago Argonne, LLC, operator of Argonne National Laboratory. Argonne, a DOE Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

**Roland Varriale, Michael Thompson, and Dr. Nathaniel Evans are with the Risk and Infrastructure Science Center (RISC), Global Security Sciences Division at Argonne National Laboratory. Roland Varriale and Michael Thompson are cyber security analysts; Dr. Evans is the Section Lead of the Cyber Operation and Analysis team.*

❖

Bye, Bye Blue Water Fleet

by K. Denise Rucker Krepp*

A troubling threat is developing in the maritime sector. It's not cyber-related, nor is it environmental. Rather, the threat stems from the lack of ownership. The majority of the vessels transporting goods around the world are foreign-flagged. There are only 84 U.S.-flagged vessels involved in international trade and we are quickly reaching the point where the U.S. military will have to rely on international flag carriers to transport goods and munitions in times of war.[1]

Maritime History

The next time you walk by your state seal, stop and take a look at it. You'll likely see a maritime motif. Fifteen out of fifty state flags contain a ship or an anchor.[2] Why you may ask? Well, because the maritime industry was important to the economy of these states when the seals were developed. As the country grew, vessels were used to import and export U.S.-made goods. They were also used to bring Americans to new parts of the country like California and Oregon.

The vessels and anchors depicted in the seals were built in America. Shipyards in Louisiana, Mississippi, Maine, Massachusetts, and Pennsylvania built thousands of boats over the past three hundred years. U.S. companies didn't use foreign-built ships to export cargo. Instead, they used U.S.-built ships and if you go on the National Park Service's website, you'll find information about the shipyards and the men and women who worked there.[3]

By 1955, there were 1072 U.S.-flagged vessels in the international trade.[4] These vessels were in addition to those operating domestically and they provided significant support during the Korean and Vietnam wars. The military couldn't transport all of its guns and tanks. Instead, it relied on private U.S. shipowners to haul these goods.

Unfortunately, the number of U.S.-flagged vessels in international trade has shrunk dramatically. Today, there are only 84 remaining. This shocking number was shared by Maritime Administration Administrator Paul Jaenichen last year at a House of Representatives Armed Services Committee hearing.[5] His message was not reassuring. Unless something happens to stop the hemorrhaging, more vessels will leave the fleet.

Ramifications for Homeland Security

The precipitous decline of the U.S.-flagged international fleet has significant ramifications for our country's homeland security. U.S. ships and U.S. mariners transport Department of Defense (DOD) guns and tanks. If they disappear, DOD will be forced to use foreign mariners and foreign owned vessels to transport them.

The Canadian government uses foreign-flagged vessels and they've had some interesting results. In 2000, the Canadian government put $150 million worth of tanks

(Continued on Page 17)

[1] *Logistics and Sealift Force Requirements and Force Structure Assessment Hearing, Before the House Comm. on Armed Services, Subcomm. on Seapower and Projection Forces*, 113th Cong. 125 (2014) (statement of Paul Jaenichen, Maritime Administrator, U.S. Department of Transportation) available at http://docs.house.gov/meetings/AS/AS28/20140730/102432/HHRG-113-AS28-Wstate-JaenichenP-20140730.pdf. (Jaenichen Statement)

[2] The fifteen states include - Alaska, California, Delaware, Florida, Georgia, Iowa, Kansas, New Hampshire, North Carolina, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, and Wisconsin. Photos of these flags can be found at: http://en.wikipedia.org/wiki/Seals_of_the_U.S._states.

[3] "Ships & Shipbuilding," *National Park Service, Maritime History of Massachusetts*, http://www.nps.gov/nr/travel/maritime/ships.htm.

[4] Scott C. Truver, Lifeline of the Nation: *The U.S. Merchant Marine in the 21st Century* (Greenbelt, MD: Gryphon Technologies, 2007), available at http://www.virginia.edu/colp/pdf/US-Merchant-Marine-in-21st-Century.pdf.

[5] See Jaenichen Statement.

(Continued from Page 16)

on a foreign-flag vessel.[6] The ship owner then refused to offload the cargo because of a contractual dispute and the Canadian government was forced to land Marines on the vessels. Does the United States government want to end up in the same situation?

When the Department of Defense uses U.S.-flag vessels, it knows that the owners, vessels, and crews have been highly scrutinized. U.S. owners are subject to rules and policies developed by the U.S. Coast Guard and the Transportation Security Administration (TSA).

TSA requires all U.S. maritime workers on land or at sea to acquire a transportation worker identification credential (TWIC).[7] Applicants must undergo a background check and provide TSA with biometric information (fingerprints). Foreign mariners are not allowed to receive a TWIC card, therefore the U.S. government has no knowledge of any crimes they may have committed.

The Coast Guard requires U.S. vessel owners to write security plans and is responsible for approving them.[8] The plans must include information on access control, training, exercises, and communication. Foreign vessel owners are not required to submit security plans, and as a result, the Coast Guard has no knowledge of their security protocols.

Seapower Strategy

On March 13, 2015, the Navy, Marine Corps, and Coast Guard released their new maritime strategy entitled "A Cooperative Strategy for 21st Century Seapower."[9] The document states that the three services "uniquely provide presence around the globe." They also claim that they "bring everything we need with us and we don't have to ask anyone's permission."

The provision statement is flawed. The three services don't bring everything with them. They have to contract out for oil and food while underway. On April 8, 2015, I did a simple search on FedBizOpps.gov and found a Military Sealift Command (MSC) solicitation for a U.S.- or foreign-flag, double-hull tanker that is capable of carrying 310,000 BBLS for at least two clean petroleum products.[10] The product will be loaded in Bahrain and discharged in the United Arab Emirates. MSC vessels couldn't transport the product so the agency contracted out for domestic or possibly international assistance.

Essentially, U.S. shipowners carry DOD's bags. They make sure that that department has the provisions it needs to go to wars. The problem, however, is that the bags have gotten heavier and the number of people available to carry these bags has shrunk so much that the existing fleet is on life support. Expecting the U.S.-flagged international fleet to meet all of DOD's mission requirements is like expecting a heart attack patient to run a marathon. It's not going to happen.

Recommendations

If the Navy, Marines, and Coast Guard are going to stop the hemorrhaging of the U.S.-flagged international fleet then they must reasonably assess how many vessels are needed in times of war. The United States is not going to make the same mistake Canada did and put tanks on a foreign flag vessel it can't control. The optics and politics of having to land U.S. marines aboard a non-U.S. flagged vessel to regain control of U.S. guns makes that possibility a non-starter, so the services have to figure out how to avoid the situation.

The first step is to identify the needs of the services. What type of goods do they need the U.S. vessel owners to carry? Food? Oil? Munitions?

(Continued on Page 18)

---

[6] James Brooke, "Canada Goes Aboard Ship to Retrieve Its Weapons," *The New York Times* (August 4, 2000), available at http://www.nytimes.com/2000/08/04/world/canada-goes-aboard-ship-to-retrieve-its-weapons.html.

[7] "Frequently Asked Questions: Transportation Worker Identification Credential," *Transportation Security Administration*, http://www.tsa.gov/stakeholders/frequently-asked-questions-0.

[8] The security plans were mandated by the Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, available at http://www.gpo.gov/fdsys/pkg/PLAW-107publ295/html/PLAW-107publ295.htm.

[9] *A Cooperative Strategy for 21st Century Seapower* (Washington, DC: Department of the Navy, 2015), available at http://www.navy.mil/local/maritime/150227-CS21R-Final.pdf.

[10] "Solicitation Number N62387-15-R-5116, TANK VOY from Sitra to Jebel Ali/Fujairah, UAE," *FedBizOpps* (accessed Apr. 8, 2015), https://www.fbo.gov/index?s=opportunity&mode=form&id=fbd618b38d7e25ef5e7dbdee2a407fd1&tab=core&_cview=0.

(Continued from Page 17)

From there, they need to identify the market rate for building and crewing the ships, in addition to the other costs associated with transporting the DOD items. These costs will determine whether or not a U.S. flagged vessel can afford to bid on a DOD shipping contract.

Keep in mind, the vessels that left the U.S. fleet didn't simply disappear. They flagged out and operated under another country's flag to do so. It's cheaper to do so. They don't have to comply with expensive U.S. laws nor employ U.S. mariners; and sadly, this fate is likely to befall the remaining 84.

So after you've looked at your state seal and examined what type of ship is on it, go visit your nearest port. The majority of the ships offloading cargo in Norfolk, New York, and New Orleans aren't American and neither are their crews. Unless something happens soon, all of them will be foreign-flagged. Not a single one will fly the U.S. flag.

**K. Denise Rucker Krepp is a professor at Pennsylvania State University and former Chief Counsel, U.S. Maritime Administration. Ms. Krepp began her career as an active duty Coast Guard officer. After September 11, 2001, Ms. Krepp helped create the Transportation Security Administration and the Department of Homeland Security. She also served as Senior Counsel on the House of Representatives Homeland Security Committee.* ❖

Project "Jack Rabbit:" A Successful Story of Public and Private Partnership and the National Benefits of Technology Transfer

by Department of Homeland Security*

The motivation for *Project Jack Rabbit* was congressional concern over 90-ton railcars filled with chlorine and other toxic inhalation chemicals traveling through metropolitan areas, the potential for an accident, or our own infrastructure used as a weapon for mass destruction. To better understand the behavior and consequences of large-scale hazardous chemical releases and develop critical data necessary to enable risk reduction, mitigation, and physical/industrial cost avoidance, a series of large-scale chemical-release field trials known as *Project Jack Rabbit* was conducted between 2010 - 2012 by DHS and four related trade associations at Dugway Proving Ground, UT. Lessons-learned and resulting improved best practices supported program expansion and a four-year continuation of *Project Jack Rabbit*.

Why are Ammonia and Chlorine Safety and Security Important to You and Your Sector?

Ammonia and chlorine products have become essential commodities to modern day life in the United States and around the globe. Americans and many critical infrastructure sectors benefit by chlorine products making it an essential asset to America's economy.

Both chemicals support U.S. agricultural abundance in the manufacturing of fertilizer and crop protection products. Ammonia is also commonly used for refrigeration, explosives, chemical manufacturing, and consumer cleaning and disinfectant products.

Through 200 years of chlorine chemistry, Americans have learned to expect clean, safe drinking water, sanitary homes and business environments, and safe food processing. However, most Americans do not realize that chlorine is also a key component of industrial and consumer products that we use every day for health, safety, nutrition, security, transportation, lifestyle, and high-tech innovation. For example, it is used in over half of all industrial chemical processes to include 90 percent of pharmaceuticals, and the manufacturing of plastics (such as PVC), paper, medical devices, automobiles, computers, aircraft parts, and textiles – the list is virtually endless! There are often no alternatives to chlorine use in these products, and when alternatives have been identified, chlorine-based processes are often considered safer and more effective.

Chlorine is used everywhere, but only produced in a few locations. It is the second largest quantity of chemical transported by rail. Shipment by railroad is considered the safest mode of transportation. Wide-scale application of chlorine, high demand for large-scale production, the highly toxic and hazardous nature of chlorine, and the ability

Chlorine Facts

- Each specially-designed rail tank car carries 90-tons of compressed/pressurized chlorine.
- Almost all "bulk" chlorine (shipped from the manufacturers to the end user or repackage facility) is shipped by rail.
- There are approximately 30,000 tank car rail shipments per year.2 (Truck and barge shipments are repackaged chlorine in 150lb. cylinders or one to 10-ton containers for small-scale use. Chlorine also moves by pipeline within facilities or over very short distances.)
- Given the total number of chlorine rail shipments in 2011, incidents represented only 0.028% of total chlorine shipments. Most were minor releases from improperly secured tank car valves or fittings (Data from DOT's 5800 Incident Reports Database).
- Chlorine products of all kinds, and their derivatives, contribute more than $46 billion to the U.S. economy each year.

(Continued on Page 20)

(Continued from Page 19)

to transport chemicals millions of miles across the country annually in a safe and secure manner further supports stakeholders' commitment to making the nation's hazardous chemical transportation system as safe as possible.

Jack Rabbit I Findings

Jack Rabbit I was a series of ten chlorine and ammonia field release trials intended to gain critical knowledge and address data gaps for large-scale hazardous chemical release disasters. From the data and analysis, new insights and updated/validated chemical release/reaction modeling was developed to support novel risk mitigation strategies and enhancements in emergency response training for potential accidents or terrorist attacks on chemical storage tanks or railcars.

The team of public and private sector chemical scientists, chemical engineers, and transportation/manufacturing experts determined that emergency response protocols needed to be updated with new guidance to address the low, fog-like dispersion of chlorine, its chemical reactivity with the environment, and spontaneous explosive plumes of chlorine observed from the ground after the releases. Chemical suits would likely not provide adequate protection from these violent eruptions, which were documented in the Jack Rabbit trials for the first time. Additional future applications of this work include updating guidelines for surrounding community shelter-in-place or evacuation protocols based on new modeling, and improving current tank rail cars' puncture resistant/crash worthiness design without exceeding railroad track or highway weight limitations.

Jack Rabbit II

Jack Rabbit II is a four-year program that expands and continues studies of *Jack Rabbit I* with planned chlorine field releases from 5 to 20 tons, which is consistent with the actual operational scales involved in a potential release from chlorine tank railcars and tank trucks in transport. The purpose and goal will be to further collect data on the release source, cloud concentration, movement, and chemical reactions based on surrounding terrain and meteorological conditions (humidity, wind direction and speed, quantity of sunlight, and temperature). Consideration will also be given to the exposure effects on equipment and infrastructure, assessing urban impact using a mock urban testbed, and environmental chemical absorption (ground, trees, wind, and managing water reactivity).

Data and findings generated are expected to drive improved hazard prediction modeling, more effective emergency response and training, national preparedness, and mitigation strategies.

Excellence in Technology Transfer and Public/Private Partnership

Immediately following the field release trials, DHS and the private sector held a workshop with more than 100 representatives from the emergency services and response sector at the U.S. Army's Edgewood Chemical Biological Center in Edgewood, MD to show the field test video and discuss existing protocols within the emergency services industry to respond to a chlorine release. The participants were in concurrence that a novel approach was needed to transition the critical findings to stakeholders in the private sector. Working groups were established to tackle the issue of communicating this information to others around the Nation. As a result of this effort, the Jack Rabbit technology and knowledge products were transferred through four major trade associations representing hundreds of industrial members to include: The Chlorine Institute, the Ammonia Safety and Training Institute, The Fertilizer Institute, and the Association of American Railroads through presentations at industry meetings; and through national-level training sessions for emergency responders, and the distribution of field test data and findings.

The Mid-Atlantic Regional and National Federal Laboratory Consortium Awards for Excellence in Technology Transfer was awarded to five DHS chemical engineers, scientists, and program managers from the Office of Infrastructure Protection's Chemical Sector-Specific Agency, Science and Technology's (S&T)Chemical Security Analysis Center (CSAC), the Transportation Security Administration, and the U.S. Army's Dugway Proving Groundfor their efforts to establish a web-based data repository, modeling data and methodologies, and training products from Project Jack Rabbit to the private sector, and novel risk mitigation strategies for the chemical, railroad, and emergency response industries.

(Continued on Page 21)

(Continued from Page 20)

The *Jack Rabbit* program successfully demonstrates a "One DHS" approach where members from different DHS directorates and other Federal agencies continue to work in unison with the private sector to further our national goals for the protection, safety, and security of America's way of life.

Additional Information

DHS Chemical Security Analysis Center products are published on HSIN

Homeland Security Information Network (HSIN): http://www.dhs.gov/homeland-security-information-network

Jack Rabbit Database (Request access through form at: https://jr-dpg.dpg.army.mil/

Office of Infrastructure Protection Chemical Sector-Specific Agency: *http://www.dhs.gov/chemical-sector* ❖

Transportation Planning Methods for Coping with Climate Change Uncertainty: An Overview

by Thomas A. Wall, Warren E. Walker, and Vincent A.W.J. Marchau*

Introduction

Uncertainty is a common challenge for transportation planners and infrastructure managers, which can affect transportation operations, planning, and policymaking. Over the years, methods have emerged that attempt to quantify and manage these uncertainties in order to enable progress in transportation planning. However, the influence of climate change and the potential for different environmental impacts to infrastructure in the future present new and complex sources of uncertainty. To effectively plan for and adapt to these new uncertainties, transportation planners and infrastructure managers must be aware of the range of planning tools available and select those that can best address the unique situations they will encounter. We present a brief characterization of uncertainty, followed by an overview of several of the leading planning methods available to transportation professionals to cope with uncertainty, which may enable more effective climate change adaptation planning for transportation systems and the communities that they serve.

Uncertainty and Climate Change

One of the most general definitions of uncertainty is "any departure from the unachievable ideal of complete determinism."[1] This state can be characterized either as one in which limited or inadequate (i.e., inexact or unreliable) information exists for past, present, or future events,[2] or where there is a lack of information (i.e., the "border with ignorance"[3]). In addition, uncertainty can also arise from *natural variability* within a system[4]; in engineering, this dichotomy is frequently distinguished as epistemic uncertainty (i.e., lack of knowledge) and aleatory variability.[5]

The sources of climate change uncertainty are complex and, at times, different in nature from those that are familiar to transportation professionals. For one, our understanding of future climate change relies heavily on scenarios of future greenhouse gas emission, for which probabilistic likelihoods of occurrence do not exist.[6] These emission scenarios inform physical models of global atmospheric and oceanic climate, which are then downscaled to regionally-relevant projections of climate impacts. At each step in the climate modeling process, some uncertainty exists that then propagates or "cascades" across the process.[7] Therefore, it is uncertain how and when changes in climate will manifest, and how various social, economic, and ecological factors will influence those changes. Relevant to infrastructure, four key climate uncertainties include: how

(Continued on Page 23)

[1] Warren Walker, P. Harremoes, J. Rotmans, J.P. Van Der Sluijs, M.B.A. Van Asselt, P. Janssen, and M.P. Krayer Von Krauss, "Defining Uncertainty: A Conceptual Basis for Uncertainty Management in Model-Based Decision Support," *Integrated Assessment 4,* no. 1 (2003): 5-17.

[2] W.E. Walker, R. Lempert, and J.H. Kwakkel, "Deep Uncertainty," in *Encyclopaedia of Operations Research and Management Science*, ed. Saul Gass and Michael Fu (New York: Springer, 2013).

[3] Funtowicz, S.O., and J.R. Ravetz, *Uncertainty and Quality in Science for Policy* (Dordrecht, NL: Kluwer Academic Publishers, 1990).

[4] Walker, "Defining Uncertainty."

[5] Armen Der Kiureghian and Ove Ditlevsen, "Aleatory or Epistemic? Does It Matter?" *Structural Safety 31* (2009): 105-12., 31(2), 105-112.

[6] N. Nakicenovic, et al., "Special Report on Emissions Scenarios," in *Special Report of Working Group III of the Intergovernmental Panel on Climate Change* (Cambridge, UK: Cambridge University Press, 2000); Detlaf P. van Vuuren, et al., "The Representative Concentration Pathways: An Overview," Climatic Change 109, no. 1-2 (2011): 5-31.

[7] L.O. Mearns, and M. Hulme, "Climate Scenario Development. Chapter 13," in *Climate Change 2001: The Scientific Basis, Contributions of Working Group I to the Third Assessment Report of the Intergovernmental Panel on Climate Change* (Cambridge, UK: Cambridge University Press, 2001).

(Continued from Page 22)

global climatic trends will translate into local effects, the magnitude and spatial extent of impacts, the rate at which climate change is occurring and will continue to occur, and how best to respond (i.e., adapt) when no obvious or consensus response exists.[8] The following section introduces several uncertainty planning methods—some of which are already in use, and others that may be useful—to address these four elements of climate change uncertainty for infrastructure planning.

Traditional Approaches for Handling Uncertainty

Risk Management: Many of the current frameworks developed for climate change adaptation planning are heavily influenced by the concept of risk (Wall and Meyer[9] provide an overview of many of these frameworks). Transportation professionals are familiar with risk,[10] and many state Departments of Transportation use risk in asset management activities. By looking at the elements of risk (likelihood and consequence; or threat/hazard, vulnerability, and consequence), risk management identifies, assesses, and responds to risks by attempting to predict a likely future (or small number of likely futures). A key challenge in a risk-based adaptation approach is determining the likelihood of system impacts under deep uncertainty. As noted above, climate projections are not assigned a degree of likelihood, and thus subjective probability distributions (often informed by expert opinion) are frequently used to describe the likelihood of impacts and vulnerabilities.[11] However, these subjective distributions often amount to "statements of 'degree of belief,'"[12] which can be inexact, and thus problematic.

Scenario Planning: Developed by the RAND Corporation in the 1950s,[13] scenario planning is widely used to examine plausible futures and to aid in selecting a plan or policy that performs satisfactorily across these futures; such a solution is called a *robust* solution.[14] Scenario analysis and planning has been applied to the transportation field and to climate change uncertainties in transportation,[15] and is frequently used in conjunction with risk-based planning methods to explore multiple potential climate futures (e.g., developing projections for low- and high-emission scenarios, or for multiple time horizons, to better identify the range of impact magnitudes and timing). Computer-based exploratory analysis can also be used to enable decisions that are robust across very large ensembles of *plausible* futures, not just a small number of *probable* or expected futures.[16] However, climate change uncertainty pushes the limits of scenario analysis as emission reduction efforts and future socio-economic conditions, which directly affect the scenarios used in adaptation planning, remain largely uncertain.[17]

(Continued on Page 24)

[8] S. Adnan Rahman, Warren Walker, and Vincent Marchau, *Coping with Uncertainties About Climate Change in Infrastructure Planning - an Adaptive Policymaking Approach* (Rotterdam: RAAD voor Verkeer en Waterstaat, 2008).

[9] Thomas A. Wall, and Michael D. Meyer, "Risk-Based Adaptation Frameworks for Climate Change Planning in the Transportation Sector: A Synthesis of Practice," in *Transportation Research Circular E-C181*, 32 (Washington, DC: Transportation Research Board of the National Academies, 2013).

[10] Shomik Raj Mehndiratta, Daniel Brand, and Thomas E. Parody, "How Transportation Planners and Decision Makers Address Risk and Uncertainty," *Transportation Research Record* 1076 (2000).

[11] Robert Willows, and Richenda Connell, "Climate Adaptation: Risk, Uncertainty and Decision-Making," in *UKCIP Technical Report (Oxford: UKCIP, 2003).*

[12] M. Granger Morgan, "Characterizing and Dealing with Uncertainty: Insights from the Integrated Assessment of Climate Change," *Integrated Assessment 4*, no. 1 (2003): 46-55.

[13] Ron Bradfield, George Wright, George Burt, George Cairns, and Kees Van Der Heijden, "The Origins and Evolution of Scenario Techniques in Long Range Business Planning," *Futures 37* (2005): 795-812.

[14] W.E. Walker, "*Uncertainty: The Challenge for Policy Analysis in the 21st Century*," Paper presented at the Inaugural Lecture, Delft University of Technology (2000).

[15] James A. Dewar and Martin Wachs, *Transportation Planning, Climate Change, and Decisionmaking under Uncertainty*, (Washington, DC: Transportation Research Board of the National Academies, 2008).

Uncertainty, (Washington, DC: Transportation Research Board of the National Academies, 2008).

[16] Steve Bankes, "Exploratory Modeling for Policy Analysis," *Operations Research 41*, no. 3 (1993): 435-49.

[17] T.R. Carter, R.N. Jones, X. Lu, S. Bhadwal, C. Conde, L.O. Mearns, B.C. O'Neill, M.D.A. Rounsevell, and M.B. Zurek, "New Assessment Methods of the Characterization of Future Conditions," *In Climate Change 2007: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change*, ed. M.L. Parry, O.F. Canziani, J.P. Palutikof, P.J. van der Linden and C.E. Hanson (Cambridge, UK: Cambridge University Press, 2007): 133-71.

(Continued from Page 23)

Iterative Risk Analysis: Current risk-based climate adaptation frameworks often employ an iterative or cyclic approach to assessment and planning (for example, the Federal Highway Administration[18]) to periodically identify, assess, and respond to risks. The inherent assumption with this approach is that over time, future outcomes will be better understood, or that uncertainty will be reduced. This condition may or may not be true, and new information can also either diminish or increase uncertainty,[19] which is problematic for an iterative approach.

Dynamic Approaches for Handling Climate Uncertainty

In recent years, new planning approaches have emerged in response to the inability of the approaches discussed above to handle the 'deep uncertainty'[20] associated with climate change. Whereas the previous approaches attempt to predict characteristics of the future (or a small number of possible futures), and respond by increasing "static robustness" (robustness with respect to the few scenarios, none of which is likely to actually occur exactly as predicted), these new approaches pursue "dynamic robustness" by building flexibility and learning mechanisms into the basic structure of plans and policies that enable them to adapt over time.[21]

Dynamic Strategic Planning is a systems analysis method that incorporates elements of decision analysis and real options.[22] Decision analysis assists in decision making under uncertainty by using decision trees and/or influence diagrams to predict the likelihood and consequences of decision outcomes. Real options then respond to these risks by building flexibility into the design of systems to dynamically adapt to future conditions.[23] For example, a 10-foot-tall storm surge barrier may be built with an over-designed foundation to allow the flexibility to increase the height of the barrier at some point in the future, if warranted by changing conditions.

Adaptive Planning is a term used here to describe a family of approaches based on adaptive management, which originated in the environmental management field,[24] but has become an important concept in managing climate change risks.[25] These approaches build learning mechanisms into plans that respond to inputs over the course of their implementation. Although other adaptive approaches exist (e.g., adaptive foresight,[26] anticipatory governance,[27] adaptation pathways,[28] dynamic adaptive policy pathways[29]), two are described here.

Assumption-Based Planning (ABP) was developed by the RAND Corporation to improve the robustness of an existing plan by identifying its underlying assumptions that are vulnerable to plausible events, and taking actions to increase the plan's

(Continued on Page 25)

---

[18] Federal Highway Administration, *Climate Change & Extreme Weather Vulnerability Assessment Framework*, (Washington, DC: United States Department of Transportation, 2012).
[19] Walker, "Defining Uncertainty."
[20] Walker, "Deep Uncertainty."
[21] Warren E. Walker, Marjolijn Haasnoot, and Jan H. Kwakkel, "Adapt or Perish: A Review of Planning Approaches for Adaptation Under Deep Uncertainty," *Sustainability 5*, no. 3(2013): 955-979.
[22] Richard de Neufville, "Dynamic Strategic Planning for Technology Policy," I*nternational Journal of Technology Management 19*, no. 3/4/5 (2000): 225-45.
[23] Richard de Neufville, "Real Options: Dealing with Uncertainty in Systems Planning and Design," *Integrated Assessment 4*, no. 1 (2003): 26-34.
[24] C.S. Holling, *Adaptive Environmental Assessment and Management*, (New York: Wiley, 1978).
[25] National Research Council, "Adapting to the Impacts of Climate Change," in America's Climate Choices (Washington, D.C.: National Academies, 2010).
[26] E. Anders Eriksson and K. Matthias Weber, "Adaptive Foresight: Navigating the Complex Landscape of Policy Strategies," *Technological Forecasting and Social Change 75* (2008): 462-82.
[27] Ray Quay, "Anticipatory Governance: A Tool for Climate Change Adaptation," *Journal of the American Planning Association 76*, no. 4 (2010): 496-511.
[28] Nicola Ranger, Tim Reeder, and Jason Lowe, "Addressing 'Deep' Uncertainty over Long-Term Climate in Major Infrastructure Projects: Four Innovations of the Thames Estuary 2100 Project," E*URO Journal on Decision Processes 1*, no. 3-4 (2013): 233-62.
[29] Marjolijn Haasnoot, Jan H. Kwakkel, and Warren E. Walker, "Dynamic Adaptive Policy Pathways: A New Method for Crafting Robust Decisions for a Deeply Uncertain World," *Global Environmental Change 23*, Issue 2: 485–498.

(Continued from Page 24)

robustness to these events.[30] ABP identifies all assumptions that form the basis for the plan, those assumptions that are both critical to the success of the plan and are vulnerable to plausible future events, and produces "signposts" to monitor vulnerable assumptions and serve as warning signs of impending surprises. It then designs and implements (1) shaping actions to influence favorably the outcomes of uncertain events, and (2) hedging actions to mitigate impacts should an assumption fail to occur as expected.[31]

Dynamic Adaptive Planning (DAP) expands upon some of ABP's core concepts for use in ground-up planning.[32] DAP involves developing a basic plan, identifying the vulnerabilities of the plan, developing a series of actions to guard against these vulnerabilities, and establishing a series of signposts to monitor the uncertain vulnerabilities. Then, during implementation, if monitoring indicates that signposts reach predetermined critical levels, a series of predetermined adaptive actions are taken to ensure that the basic plan stays on track to meet its goals and objectives. The basic plan, monitoring program, and planned adaptations remain in place unless monitoring indicates that the intended outcomes can no longer be achieved, or if the goals and objectives of the basic plan change. In these instances, the adaptive plan is then reassessed. These elements of adaptability and learning enable DAP to adjust to new information as it becomes available. Wall, et al. show how DAP can be applied to deal with climate change uncertainties in transportation infrastructure adaptation planning.[33]

Conclusion

The uncertainties associated with climate change impacts introduce new challenges to transportation professionals tasked with infrastructure planning and management. Many of the approaches that have been used historically to address uncertainty in these activities are being applied to climate change adaptation planning. These traditional approaches assume that the future is 'known' to a certain extent (either through probabilities or through scenarios). However, it is increasingly being accepted that this future is 'unknown', and approaches have been developed to cope with this situation of 'deep uncertainty'. For example, adaptive planning approaches offer processes that guide adaptation planning and policy throughout the implementation process and use monitoring activities (which may be able to leverage or mainstream with current asset management activities) to make adjustments to these plans in the future. What is most important is that transportation professionals are aware of the broad range of uncertainty planning methods at their disposal for climate change adaptation, and that they let the context of the planning effort help to guide their selection of the most appropriate method.

Aknowledgement

The work presented in this paper was partially supported by Argonne National Laboratory under DOE contract number DE-AC02-06CH11357. The submitted manuscript has been created by UChicago Argonne, LLC, operator of Argonne National Laboratory. Argonne, a DOE Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

**Thomas A. Wall, Ph.D., is Infrastructure & Preparedness Analyst for the Risk and Infrastructure Science Center (RISC), Global Security Sciences Division, Argonne National Laboratory. Warren E. Walker, Ph.D., is Professor for the Faculty of Technology, Policy and Management, and Faculty of Aerospace Engineering, Delft University of Technology, the Netherlands. Vincent A.W.J. Marchau, Ph.D., is the Managing Director of the Dutch Research School on TRAnsport, Infrastructure and Logistics (TRAIL) & Professor, Nijmegen School of Management, Radboud University, the Netherlands.*

❖

[30] James Dewar, *Assumption-Based Planning: A Tool for Reducing Avoidable Surprises*, (Cambridge, UK: Cambridge University Press, 2002).
[31] Dewar, Transportation Planning, Climate Change, and Decisionmaking under Uncertainty.
[32] W.E. Walker, A. Rahman, and J. Cave, "Adaptive Policies, Policy Analysis, and Policy-Making," *European Journal of Operations Research 128* (2001): 282-89.
[33] Thomas A. Wall, Warren E. Walker, Vincent A.W.J. Marchau, and Luca Bertolini, "Climate Change Adaptation: Dynamic Adaptive Planning for Transportation Infrastructure," *ASCE Journal of Infrastructure Systems*, forthcoming.

Transportation Infrastructure Security and Resilience – State DOT Strategic Perspectives

by Dr. Silvana Croope*

Introduction

Separate and complementary concepts such as security and resilience can help to address specific needs in transportation yet focus on "ends," and a critical perspective on the "means" to reach or produce those "ends" are the driving force necessary to building and operationalizing resilience. A strategic approach to defining work at the State DOT level to set the stage for an organized, progressive, and evolving approach to security and resilience is necessary to identify critical areas of work and define an implementation agenda recognizing the interconnected relationship of internal and external elements of such transportation infrastructure systems.

An overview of some concepts and contexts allows exploration of the need for review of understanding and differentiation of strategic planning from other types of planning to improve the path to building a resilient transportation infrastructure and supporting the construction of a resilient Nation.

Concepts and Context

Some approaches to security include the idea of physical protection, plans and actions towards minimizing threat and risk, and ensure minimum needs for continuity of activities are met. An example of this approach in the real world is the Transportation Security Administration (TSA). The agency focuses on counter-terrorism, ensuring freedom of movement for people and commerce, and uses a risk-based strategy including intelligence communities, law enforcement, and transportation. A broader perspective of security is the use of the concept of homeland security, which has also taken the shape of an agency, the U. S. Department of Homeland Security (DHS). Homeland security, in the United States, as distinguished from homeland defense, includes safety, security, and resilience against terrorism and hazards challenging American interests, aspirations, and way of life, including reduction of vulnerability and damage.[1]

Security and resilience are distinct but, at the minimum, interdependent and include hardening of infrastructure, standards, and interoperability. On the one hand, security focuses on blocking and defeating threats to national security such as terrorists or anarchists with objectives to destabilize government and its people, whereas resilience focuses on reducing the impact of events, facilitating recovery through ongoing processes of risk and threat assessments, and preparing to face threats that can eventually be responsible for disruption.

Critical infrastructure protection is part of the business of homeland security carried on by civilian work together with DHS in collaboration with sector-specific governmental agencies, the private sector, academia, and non-governmental organizations. As part of these efforts, members of the transportation, one of the critical infrastructure sectors, have pursued work targeting decreases of vulnerability and damages, and increased resilience.[2]

The work around resilience evolved from the early 17th century in different disciplines before it started in transportation with initial ideas related to rebound.[3] Resilience may be organized in many ways, one of them considering resilience factors that vary according to different contexts of risk, therefore being not only a characteristic of a system, but also a process[4] or a means to reaching a bigger goal such as sustainability.[5]

(Continued on Page 27)

[1] "Origins of the Term," *Torrens Resilience Institute* (2009), http://www.torrensresilience.org/origins-of-the-term (Last accessed Apr. 15, 2015).
[2] "Critical Infrastructure Sectors," *United States Department of Homeland Security* website, http://www.dhs.gov/critical-infrastructure-sectors (Accessed Apr. 15, 2015).
[3] "Origins of the Term," *Torrens Resilience Institute*.

(Continued from Page 26)

Governing principles for transportation system resilience are specifications incorporated by governmental agencies setting the standard for programs and actions that tie up program funding and policies. These principles serve to establish the common base of work, which many times, State DOTs interpret, advance, and customize. Examples of this resilience approach include:

•

DHS "spread-out enterprise";[6]

- National Academies "disaster resilience";[7]
- National Academies "community disaster resilience through private-public collaboration";[8]
- U.S. Department of Transportation Climate Adaptation Plan describing system resilience is "more than just the sum of their individual parts";[9] and
- Transportation Research Board of the National Academies publication of TRB and Resilience including security, resilience, and different STIP/TIP (State Transportation Improvement Program, Transportation Improvement Program) and long-range plans.[10]

Identifying plans[11] that helps reach the ends State DOTs want is part of organizing strategic, tactical, operational, and project level activities. Strategic planning and long-range

(Continued from Page 28)

Strategic Plan/ Planning	Long–Range Plan/ Planning
• systemic process built upon vision, goals, objectives and the "how to get there" • looks at the *end* desired position or outcome and works backwards to existing status; looks at things in a bigger picture and uses a flexible approach to choices of *means* to get to the *ends* • *question:* what needs to happen earlier to get to current position? • space for creativity, innovation and change that requires strategic management and strategic thinking • deals with resource allocation decision making, comprehensive approach to problem solving, research and analysis of the organization and its environment • uses either intended or emergent (for adaptation) strategies, or combination of styles at different moments or interacting elements, variables, institutions and people • includes development and implementation processes, therefore is analytic and synthetic (find dots and connect dots) possible through strategic thinking	• includes review of existing status and defines how to answer to future needs •capacity building, decision-making development and implementation support guidance, identification of gaps in policy, assessment and definition of system's performance, management of fiscal constraints, identification of needs of financial and economic resilience, creation and expansion of spatial livability and sustainability, addressing challenges posed by climate change and other global risks • question: what accomplishments are needed here to go to the next stage?

[4] John Fleming and Robert J. Ledogar, "Resilience, an Evolving Concept: A Review of Literature Relevant to Aboriginal Research," *Pimatisiwin 6*, no. 2 (Summer 2008): 7-23.

[5] Cameron Gordon, "Can Transport System Resilience and Sustainability be Economically Efficient?," Presented at *Transportation Research Board 94th Annual Meeting,* Jan. 11-15, 2015, Washington, D.C.

[6] "Resilience," United States Department of Homeland Security website, http://www.dhs.gov/topic/resilience (Accessed Apr. 14, 2015).

[7] The National Academies, *Disaster Resilience: A National Imperative* (Washington, D.C.: The National Academies Press, *2012).*

[8] The National Academies, *Building Community Disaster Resilience through Private-Public Collaboration* (Washington, D.C.: The National Academies Press, 2011).

[9]United States Department of Transportation, "2014 DOT Climate Adaptation Plan," *U.S. Department of Transportation Climate Adaptation Plan 2014: Ensuring Transportation Infrastructure and System Resilience* (Washington, D.C.: United States Department of Transportation, 2014).

[10] "TRB and Resilience," *Transportation Research Board of the National Academies* (April 2015), http://onlinepubs.trb.org/onlinepubs/dva/securityactivities.pdf (Accessed Apr. 12, 2015).

[11] John A. Volpe National Transportation Systems Center, *Trends in Statewide Long-Range Transportation Plans: Core and Emerging Topics* (Cambridge, MA: United States Department of Transportation, 2012), available at http://www.planning.dot.gov/documents/State_plans_report_508_A.PDF.

[12] "Strategic Planning," *BusinessDictionary.com*, http://www.businessdictionary.com/definition/strategic-planning.html (Accessed Apr. 16, 2015); "Strategic Planning," *Wikipedia The Free Encyclopedia*, *http://en.wikipedia.org/wiki/Strategic_planning* (Accessed Apr. 15, 2015); Stephen Haines, *Strategic and Systems Thinking: The Winning Formula* (Chula Vista, CA: Systems Thinking Press, 2007).

(Continued from Page 27)

planning can be characterized as shown below.[12]

Work by the World Economic Forum (WEF) on long-term global risks[13] evolved from risk identification to risk interconnections and consequent cascading effects. The National Academies used WEF global risks reports to help discuss resilience and underscore the importance of public-private partnership.[14] Global risks reports should be used by State DOTs for strategic planning and implementation and for long-term planning.

Examples of strategic plans for transportation that include direct or indirect approach to resilience include:

- U.S. Department of Transportation for 2014 to 2018;[15]
- National Academies "resilient nation" set for 2030 and addresses topics on many science disciplines; a holistic approach;[16] and
- Federal Highway Administration (FHWA) with varied parts updates.[17]

Identification of type of plan, strategic or long-range plan, can help leaders understand time constraints for implementation of plans, include feasibility perspectives, and fit political perspective impacts—an integral part of the issue of building resilience at all levels of government and transportation sector. The question remains: how good is the current understanding and use of strategies for security and resilience of transportation? The task for State DOTs is determining how and when to build the different types of plans and finding or developing policies to support desired results and ends. The means, in this perspective, are contributions to implementation of strategies. Next is how State DOTs can review strategic planning to address security and resilience.

Strategic Resilient State DOT

Transportation is important to all economic sectors, a cross-sector under the classification of critical infrastructure sectors as described in the National Infrastructure Protection Plan.[18] Compartmentalized transportation allows for building detailed knowledge and efficiencies. Work in progress to review, update, and improve governing documents struggles with bureaucracy and makes the overall process to evolve to a more resilient transportation system difficult—"trying to catch up on things for ten years," a reactive action instead of proactive. To change this situation a good illustration is a puzzle. A picture defined needs the pieces to come together to make it whole. The different plans are the pieces that need to be developed and "placed" to build the picture, the picture being the strategic *end*. The plans do not have to come all at once, but a desired time for the outcome is important to define. One example was the rush between the U.S.A. and Russia to see who would be the first to put men on the moon (end), and the PERT-CPM process developed answering the need for management (means) of the work.[19]

Examples on how to develop strategic plans and to use strategic management process include phases such as

- determining position, develop-

(Continued on Page 29)

---

[13] "Global Risks 2015: 10th Edition," *World Economic Forum*, http://reports.weforum.org/global-risks-2015/ (Accessed Apr. 24, 2015).
[14] "Building Resilience to Catastrophic Risks through Public-Private Partnerships," *National Academy of Sciences* (Sep. 5, 2013), http://nas-sites.org/resilience/resilience-events/ (Accessed Jan. 15, 2015).
[15] United States Department of Transportation, *Transportation for a New Generation: Strategic Plan, Fiscal Years 2014-18* (Washington, D.C.: United States Department of Transportation, 2014), available at http://www.dot.gov/sites/dot.gov/files/docs/2014-2018-strategic-plan_0.pdf (Accessed April 16, 2015).
[16] The National Academies, *Disaster Resilience: A National Imperative*.
[17] Federal Highway Administration, *FHWA Strategic Plan* (Washington, D.C.: United States Department of Transportation, 2008), available at http://www.fhwa.dot.gov/policy/fhplan.htm (Accessed Apr. 16, 2015).
[18] United States Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: United States Department of Homeland Security, 2013), available at http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.
[19] V.P.B. Chakravarthi Kajana and Abhijeet Kumar, "Project Management CPM/PERT," *Slideshare.net* (2015), http://pt.slideshare.net/ninoto/pert-cpm-intro (Accessed Apr. 17, 2015).
[20] "Essentials Guide to Strategic Planning," *OnStrategy* (2015), http://onstrategyhq.com/resources/strategic-planning-process-basics/ (Accessed Apr. 13, 2015).

(Continued from Page 28)

ing strategies, developing the plan, and managing performance,[20] which includes verifying readiness of organization and marketing; and

- use of vision, mission, objectives, strategies, and action plans towards making ideals attainable, translating each of those terms respectably into the dream, what and why, how much and when, how, who does what.[21]

Barriers to successful implementation of strategies include:

- establishing and getting strategic perspective buy-in from staff and management (not a one-time action);
- determining staff/team role to implement strategy throughout the organization (individual or team, team role or team support empowerment towards leadership and staff);
- proper leadership team formation to cover type and size of the organization;
- not identifying existing practice that can be startups for resilience and security;
- change and adaptation challenged by the compartmentalized structure and people; and
- gaps on policy and funding.

Specifically for security and resilience, a business, environmental, political, economic, financial, social and even psychological perspective must be considered beyond the transportation infrastructure system (pure engineering focus). Custom-

(Continued on Page 30)

[21] Work Group for Community Health and Development, "Chapter 8: An Overview of Strategic Planning or VMOSA," *Community Tool Box* (Lawrence: University of Kansas, 2014), available at http://ctb.ku.edu/en/table-of-contents/structure/strategic-planning/vmosa/main (Accessed Apr. 17, 2015).

(Continued from Page 29)

ers of transportation need working bridges, accessible and reliable transit, smooth pavement, and the best certainty possible of normal life activities including jobs, food, health and other basic needs provided. Insights into strategic thinking topics for State DOTs towards a holistic perspective of security, resilience and the end sustainability are shown above.

Final Remarks

While this work did not present frameworks or equations to guide State DOTs, this paper is disclosing the current challenges needing re-evaluation in current practices. Lack of coordination, noise in communication, internal competition for budget, and external influences are part of the day-to-day challenges DOTs face. Considering transportation as a closed system and dedicated funding without flexibility to identify and enable expansion of taxpaying dollars to be employed on cross-topic areas or areas for innovation builds vulnerability and sustains gaps. For example, technology for combating human trafficking should take advantage of technologies for freight (the means used for such pervasive activity), but current policies do not include permission or prohibition. Strategic planning must become a strong component of State DOTs lined up with Federal government and State and local needs.

**Dr. Silvana V Croope ENV SP, has a multicultural background with experience including elementary, undergraduate and graduate education; training; transportation system planning, development and implementation; ITS systems; transportation risk and resilience assessment and State strategic planning. She does international voluntary and consulting activities on disasters and transportation; participates on applied research panels and research groups on risk, resilience, climate change, sea-level-rise, freight, flooding, economic and financial resilience, decision support system and sustainability. She leads the FEMA Transportation Specific Hazus User Group.* ❖

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for The CIP Report, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1