BEST PRACTICES IN FUTURE PROOFING EMERGING TECHNOLOGIES

FINAL REPORT

February 2022

ENTERPRISE TRANSPORTATION POOLED FUND STUDY TPF-5(359)

Prepared by:
Athey Creek Consultants

Technical Report Documentation Page

1. Report No. ENT-2022-6	2. Government Accession No.	3. Recipients Catalog No.	
4. Title and Subtitle Best Practices in Future Proofing for Emerging Technologies		5. Report Date February 17, 2022	
		6. Performing Organization Code	
7. Author(s) Dean Deeter, Jeremy Schroeder, Linda Preisen, and Matt Weatherford		8. Performing Organization Report No.	
9. Performing Organization Name and Address Athey Creek Consultants 2097 County Road D, Suite C-100 Maplewood, MN 55109		10. Project/Task/Work Unit No.	
		11. Contract (C) or Grant (G) No. 2019-0045	
12. Sponsoring Organization Name and Address ENTERPRISE Pooled Fund Study TPF-5 (359) Michigan DOT (Administering State) PO Box 30050 Lansing, MI 48909		13. Type of Report and Period Covered Final Report	
		14. Sponsoring Agency Code	

15. Supplementary Notes
Final Report available at: https://enterprise.prog.org/wp-content/uploads/ENT-Future-Proofing-Emerging-Technologies-FR-Feb-2022.pdf

16. Abstract
Transportation agencies continue to deploy and operate emerging technologies and ITS assets in both urban and rural areas. These assets serve key roles in operations of the transportation system. Maintaining the ability of these ITS assets to continue to be of value in the future is referred to as "future proofing the asset." The focus of this project was on researching best practices and overall approaches towards future proofing ITS assets. As part of this research, seven categories of threats have been identified that present possible risks to the future of ITS assets, including: natural, human interactions, functional performance, extended use, financial, license/policy/regulatory, and security threats. The research also identified multiple approaches for mitigating the future proofing risks to ITS assets. A business model suggesting roles for seven existing DOT activities was drafted, and finally an overall four step approach to mitigating risks to ITS assets was developed. State and local DOTs can implement this research by reviewing the recommended actions and considering which are appropriate for their organization to mitigate risks to the future use of ITS assets. Lastly, the project recommends future research activities to further assist agencies with streamlining activities for future proofing ITS assets.

17. Key Words Future proofing, emerging technologies, ENTERPRISE		18. Distribution Statement No restrictions	
19. Security Class (this report) Unclassified	20. Security Class (this page) Unclassified	21. No. of Pages 74	22. Price

Acknowledgments

This *Best Practice in Future Proofing Emerging Technologies* report was prepared for the ENTERPRISE Transportation Pooled Fund TPF-5(359) program (http://enterprise.prog.org/). The primary purpose of ENTERPRISE is to use the pooled resources of its members from North America and the United States federal government to develop, evaluate, and deploy Intelligent Transportation Systems (ITS).

Project Champion

Charles Tapp, Texas Department of Transportation, was the ENTERPRISE Project Champion for this effort. The Project Champion serves as the overall lead for the project.

ENTERPRISE Members

The ENTERPRISE Board consists of a representative from each of the following member entities of the program:

- Illinois Department of Transportation
- Iowa Department of Transportation
- Kansas Department of Transportation
- Michigan Department of Transportation
- Minnesota Department of Transportation
- Ontario Ministry of Transportation
- Pennsylvania Department of Transportation
- Texas Department of Transportation
- Wisconsin Department of Transportation

Table of Contents

Executive Summary

Document Overview

Transportation agencies continue to deploy and operate emerging technologies and intelligent transportation system (ITS) assets in both urban and rural areas. These assets serve key roles in operations of the transportation system. Maintaining the ability of these ITS assets to continue to be of value in the future is referred to as "future proofing the asset." The focus of this ENTERPRISE Pooled Fund Study project, Best Practices in Future Proofing for Emerging Technologies, was on researching best practices and overall approaches towards future proofing ITS assets. A three-step approach (plan, act, assess) is defined in this report that transportation agencies can consider as small changes to seven existing activities that transportation agencies already perform to help to mitigate the risks to the future of ITS assets. These seven existing activities are: system engineering analysis, procurement, information technology (IT) and security, ITS architecture & strategic planning, asset management, professional capacity building, and research and development.

Context of Future Proofing Related to System Benefits

At the onset of this research project, ITS asset future proofing was understood to relate to the ITS asset continuing to be operational, compatible with inter-related systems, and useful through the intended asset's lifecycle. The three-step approach (plan, act, assess) suggests that agencies perform a series of actions to reduce the risks to future proofing of ITS assets. The "assess" step suggests a capability maturity framework (CMF) approach to assess and ultimately increase the maturity of future proofing activities. However, based on insights from the Project Champion, pooled fund members, and the literature review, the "assess" step recognizes that successful future proofing is a factor of three 'aspects of assessments': the maturity of an agencies future proofing activities, the longevity of ITS assets, and ultimately the benefits that the ITS assets help to deliver. These three aspects of assessment are illustrated in Figure 1.

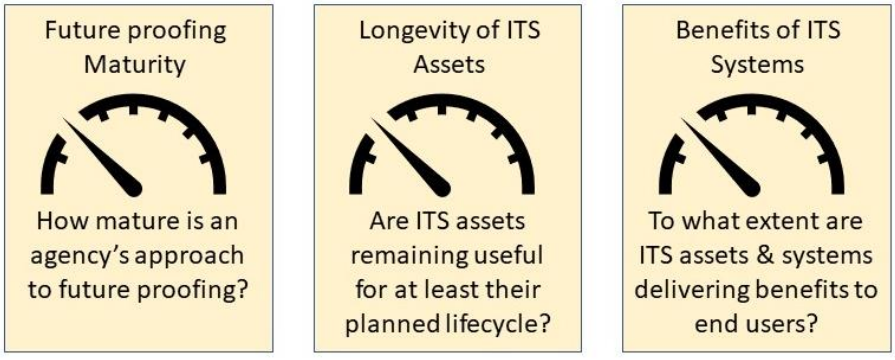


Figure 1: Graphical Representation of Three Assessments of Future Proofing

Overview of Future Proofing and Threats to ITS Assets

Future proofing has many definitions, but one way of defining it is "the ability of an asset to continue to be of value in the future." When state and local Departments of Transportation (DOTs) deploy ITS assets to support transportation operations, there are several threats to the future use and value of these assets. Table 1 identifies seven threat types and specific threats to ITS assets.

Table 1: Threat Types and Associated Potential Threats to ITS Assets

Threat Type	Potential Threats to ITS Assets
Natural	**Wear and Tear** – ITS assets are exposed to elements (e.g., air, water, insect infestations) and may cause faster than expected deterioration. **Weather Events** – Regular and unusual events (e.g., flood, wind, lightning) that cause inoperability of ITS assets.
Human Interactions	**Vandalism –** Physical damage or theft of ITS assets caused by vandalism. **Event Exposure –** ITS assets damaged by vehicles crashing or colliding with the assets or other non-natural events.
Functional Performance	**Incompatibility** – System is not compatible with future devices, communications, security, etc. **Outdated** – System is no longer effective compared to the current state of practice. **Unused** – Even when functioning properly, system is no longer used by primary user group because it does not meet their needs.
Extended Use	**Exceeding Life Expectancy** – Attempting to use ITS assets beyond the intended life expectancy. **Limited Expansion Capacity** – Use of ITS assets may require expansion and without capacity to expand the usefulness of the asset may be jeopardized. **Unavailable Support –** Hardware or software support to the ITS asset is no longer available, including replacement parts.
Financial	**Excessive Cost Increases** – System maintenance or operation costs are no longer practical. **Missed Opportunities** – System does not allow an agency to benefit from lower cost options (e.g., devices, communications, maintenance). **Reduced Funding** – Agency allocation of funds to the ITS solution is reduced.
License, Policy, and Regulatory	**Allowed Use** – Licensing, policy, and/or regulations may prevent future use of system components. **Agency/Department Policy Decisions** – Threats that may result from changes to agency policies and/or procedures.
Security	**Security Threats** – Security vulnerabilities may open devices to hackers and intentional attacks. **Limited Accessibility** – Security precautions (e.g., firewalls) could prevent use of ITS assets.

Translating Threat into Risks

Understanding the threats to ITS assets is critical, however it is difficult to assess and respond to threats alone. The research revealed that defining the risks that are caused by each threat helps to understand the likely impacts and eventually implement strategies for managing risks created by the threats. Risks are defined as the potential loss, damage, or destruction of assets caused by one or more threats. The AASHTO document Understanding Transportation Resilience: A 2016-2018 Roadmap published in 2017[1] includes a suggestion of defining as many risks as possible, as well as defining opportunities for mitigating these risks. The AASHTO report goes on to note that risks are best described as a series of "if-then" statements to frame them in the context of contributing factors and resulting risks. This report defines a series of likely risks that should be considered for each of the threats identified in Table 1 above, in a similar approach to the AASHTO report.

Concepts for Mitigating and Managing Threats and Risks to ITS Assets

Based on a synthesis of the resources reviewed in this project, three concepts are introduced:

- Future proofing **should not be an after-thought** following deployment of an ITS solution; rather, it should begin in project conception.
- Future proofing **should be managed throughout the entire process** of considering, designing, procuring, installing, and operating the ITS solution.
- Whenever possible, **future proofing should be part of existing business, technical, and financial activities of the DOT** – not implemented as a new stand-alone area or activity.

Fitting ITS Future Proofing into the DOT Business Model

The culmination of the three concepts described above is a suggestion that future proofing should be addressed by the activities of seven existing areas/activities within each DOT. These seven areas/activities are identified in Figure 2.

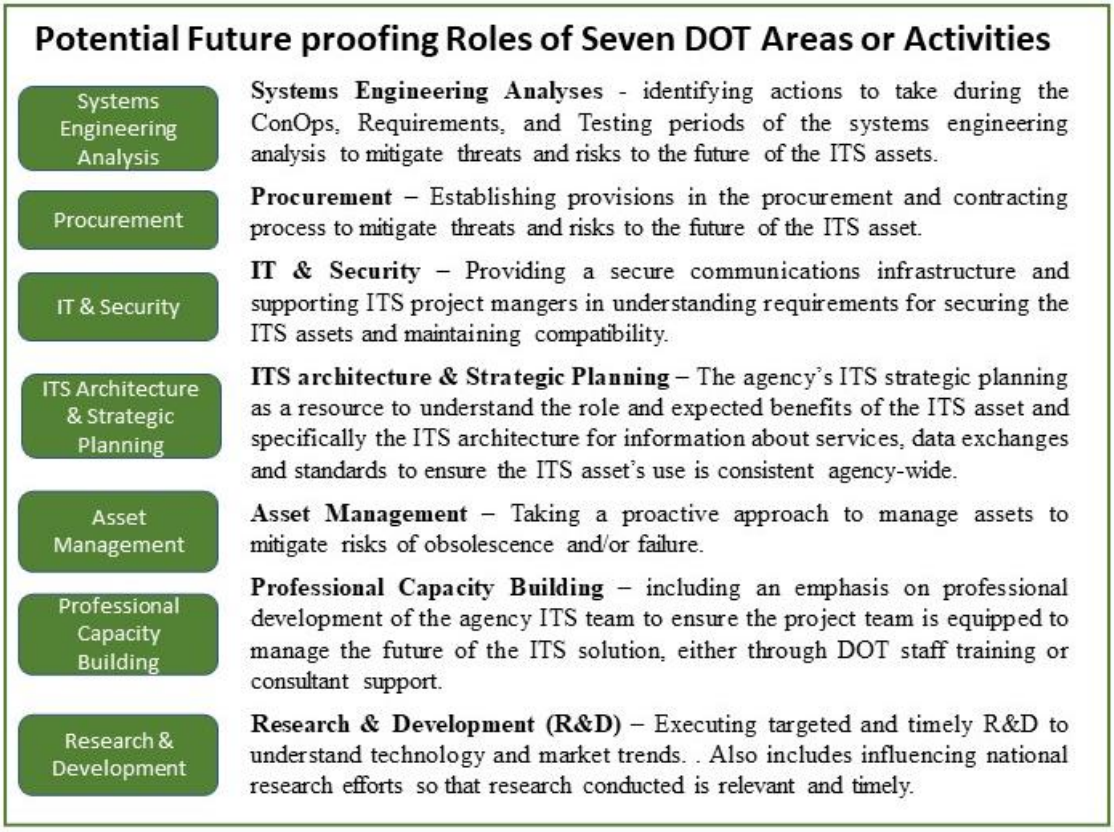


Figure 2: Areas/Activities of State DOTs That May Contribute to Managing Future Proofing

Defining a Model Approach for Future Proofing ITS Assets

A three-step approach is proposed to plan, act, and assess future proofing activities. As illustrated in Figure 3, the three steps are seen as circular and ever-repeating activities to continuously advance to improved future proofing results.

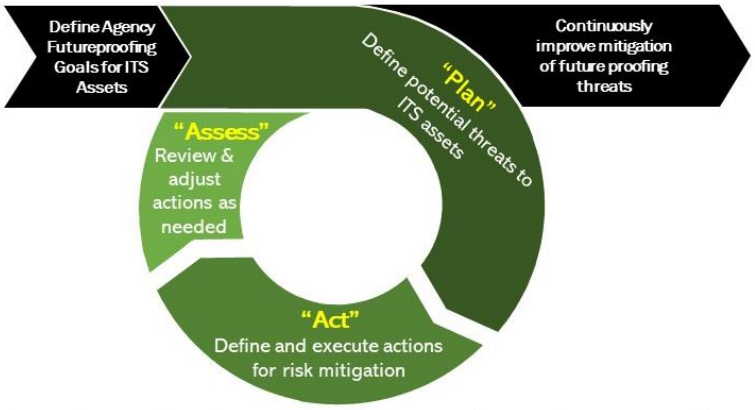


Figure 3: Repeating Approach to Plan, Act, and Assess Future proofing

During the "Plan" step, agencies are encouraged to define potential threats to assets and to perform general actions (i.e., not specific to a project or individual asset) that will help mitigate the risks to future proofing.

During the "Act" step, agencies are encouraged to incorporate future proofing actions into project activities. For each project, agencies are encouraged to consider the potential threats and risks to the ITS asset. It is important to recognize that future proof risk management is not about avoiding all risks, but rather determining which risks to avoid, which risks should be transferred, and which risks should be mitigated. When you ***avoid a risk,*** it means you change your plan to eliminate the probability of the risk

occurring or the effect of the risk if it does occur. This may involve not proceeding with the project or eliminating some aspects of the planned deployment. ***Transferring a risk*** refers to when the negative impact is shifted to a third party, such as through an insurance policy or penalty clause in a contract. The risk may still occur; however, the financial impact will be somewhat displaced from the agency. Risk transference usually involves some type of contractual agreement. ***Risk mitigation*** occurs when you proactively change the plan to minimize the impact or probability of the risk occurring.

Risk mitigation is the emphasis of the recommendations of this project, and Table 3 in section 3.1 represents the likely threats to ITS assets, risks that may result from the threats, and proposed actions that agencies are encouraged to take on a project-by-project basis to mitigate the risks (each action is identified with the suggested DOT group/activity, based on Figure 2 above.

During the Assess step, agencies are encouraged to reflect on their progress towards implementing risk mitigation activities for future proofing ITS assets. A maturity assessment, specifically a capability maturity framework (CMF) approach, is suggested for agencies to assess the extent to which they are progressing towards a mature implementation and institutionalization of activities recommended in this report. However, agencies with mature future proofing approaches may still not accomplish the potential benefits of ITS solutions. Therefore, as illustrated in Figure 4, the "assess" step goes further than exploring maturity of future proofing activities to include a focus on ITS asset lifecycles and the extent to which ITS assets contribute to end-user benefits.

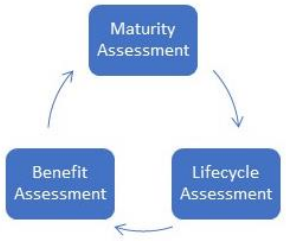


Figure 4: Aspects of "Assess" Step

Figure 5 illustrates theoretical progress along two hypothetical axes as maturity progresses from level one to level three. As illustrated in Figure 5:

- The development and establishment of a mature model for future proofing (denoted as a progression from Maturity Level 1 to Level 3) should move the agency to the "desired state" where:
  - The agency operations recognize high benefits of ITS assets; and
  - ITS assets have a high ability to remain operational and useful for anticipated lifecycles.
- There are risks that the "desired state" will not be reached, and the black boxes illustrate two risk potentials: 1) Limited lifecycles and 2) Limited benefits.
- Finally, the yellow arrows and supporting text describe the business case for two actions:
  - ITS asset lifecycle measurement, recording, and assessments; and
  - Comprehensive evaluation of benefits of ITS systems accompanied by midcourse corrections.

The body of this report describes additional details about the research findings, specifically describing possible risks and proposed actions to mitigate the risks. Finally, example scenarios are presented for mitigating future proofing risks for communications and detection systems.

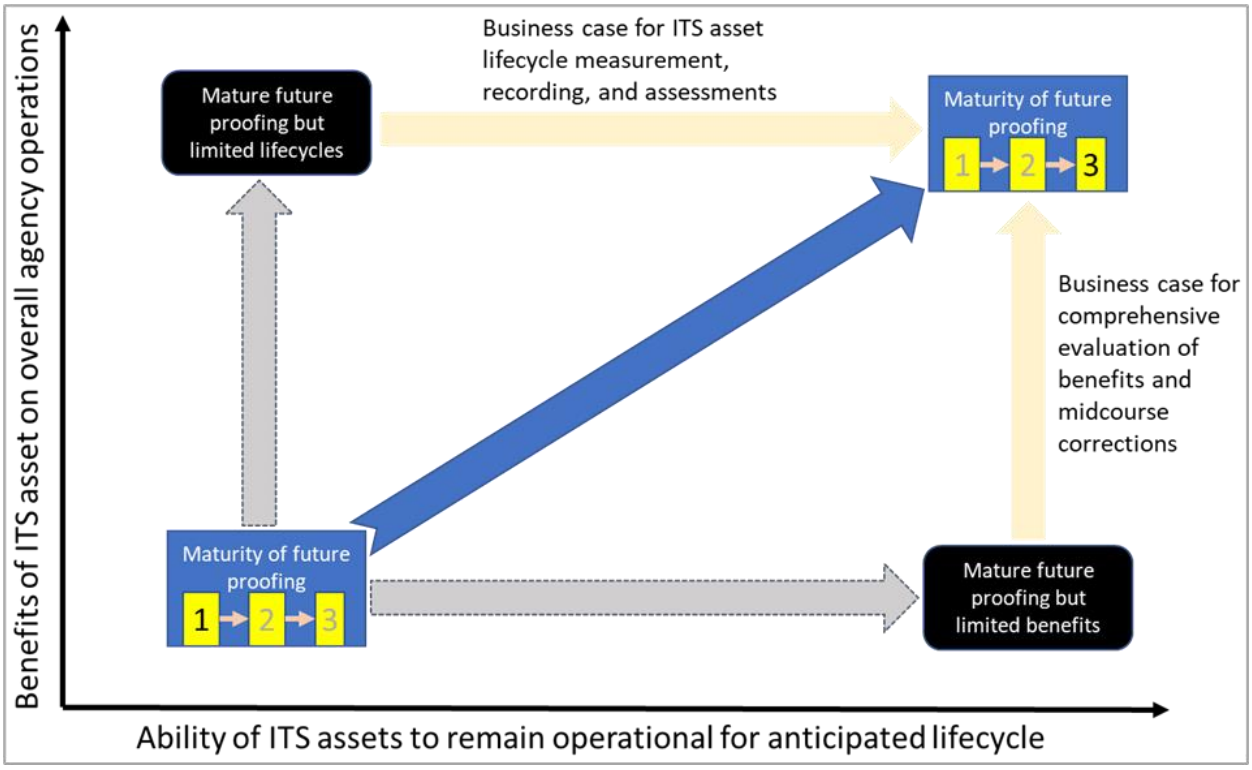


Figure 5: Graphical Representation of Desired Maturity of Future Proofing

Recommended Next Steps

The Conclusion section outlines four candidate next steps for future research to help mainstream ITS asset future proofing into the DOT model. These next steps include:

- **Research and document specific examples of recommended actions.** This additional research would add clarity and additional context to the actions identified to mitigate future proofing risks by researching and identifying case studies or examples of how agencies are taking these actions today. This research would also reaffirm the validity of the actions proposed in this report.
- **Research the potential of mainstreaming recommended actions.** This recommendation suggests that the actions proposed in this report be translated into checklists and a research effort encourages a group of states to test the checklists to assess their impacts on future proofing.
- **Research the logic of an automated software tool to support risk mitigation.** This recommendation would research the logic and processes of an automated software solution to support the actions.
- **Develop a software package to automate the logic of risk mitigation.** If a new software product is required, this research would research options for either expanding existing software solutions or creating a new solution to automate and support the future proofing actions, with research emphasizing the logic required.

Each recommendation is further defined in Chapter 6.

1.0 Introduction

1.1 Transportation Resilience and Future Proofing

Transportation agencies across the country have deployed numerous Intelligent Transportation System (ITS) devices and systems (collectively referred to as ITS assets). Transportation professionals rely on these ITS assets to perform their daily duties, while travelers also rely on the data/images/reports from these assets as they plan and execute travel. As the industry increasingly relies on ITS, there are increased vulnerabilities associated with the systems. For example, as illustrated in 2022 when the FCC reallocated the 5.9 GHz bandwidth originally dedicated to transportation safety, agencies that have deployed and are relying upon Dedicated Short-Range Communication (DSRC) roadside units now face the expensive task of replacing these devices. However, policy or licensing changes are not the only thing that impacts the ability of an asset to continue to be of value in the future (i.e., future proof). Other factors including weather and climate change, compatibility with other technologies, and user preferences are other examples of threats to the future of technology systems.

Future proofing

"The ability of an asset to continue to be of value in the future"

The overall intent of this synthesis is to provide insight to state and local DOTs on the approaches they might consider to future proof ITS deployments. Once an overall approach to ITS future proofing is explained, Chapters 6 and 7 explore an emphasis on detection systems and communications systems.

Nearly every report published on future proofing and/or resilience offers a definition for these terms, and while most definitions are similar, they do vary with each report. A report titled "Future-proofing Our Transportation Infrastructure" by Mark Conway[2] defines three key terms related to future proofing is follows:

- ***Future proofing*** is defined as "the ability of an asset to continue to be of value in the future."
- "***Resilience*** refers to the ability of the infrastructure to maintain/resume normal operations during/after unexpected/uncontrollable events and circumstances. This may include climate change, flooding, terrorism, and pandemics."
- "***Adaptability*** refers to the ability to adapt or respond to changing needs, uses, or capacities of an uncertain future. This includes allowing for changing requirements, building to avoid/reduce the impact of future events, and considering numerous socioeconomic and environmental dimensions."

1.2 The Need for ITS Future Proofing

While ITS devices and systems are part of a holistic transportation infrastructure that must consider and prepare for resilience in the broader sense, ITS assets have some unique characteristics (e.g., rapidly changing technologies, communications needs, etc.). In the 2018 report titled "Future-proofing 'Next Generation' infrastructure assets"[3] the need for future proofing is described as:

> "*Put simply, infrastructure assets are still being delivered and managed under the auspices of a 20th Century paradigm and an urgent shift is required to operate in the 'digital era' to accommodate the changing nature of work, demographic patterns, markets, sustainability and climate change.*"

Using input from this and other resources, the need for ITS future proofing can be described as a merging of two contributing factors:

- **Expanding Role of ITS.** ITS is becoming more critical to the daily activities of state and local DOTs. Outages cause impacts to the operations staff within the DOTs and to travelers; and
- **External Factors are Ever-Changing.** The global, regional, and local environments around such things as available products and services, consumer demand, reliance on Internet and/or cloud services is ever-changing. The integrated world we live in has increased the percentage of assets that are influenced by these external factors in one way or another.

While this merging of these two factors has led to great advantages to travelers and transportation professionals, it has increased the threats that are associated with temporary or long-term outages of ITS devices and systems.

1.3 Key Resources Related to Resilience and Future Proofing

More than 50 technical reports, papers, and website postings were reviewed during the literature review for this project. The knowledge gained from this literature review has led to the formation of the concepts presented in this report and therefore are identified and cited throughout the text of the document as endnotes (with supporting text describing the use of the resource when appropriate). The resources researched and reviewed within this project focused on the following areas:

- General resilience and future proofing concepts and experiences;
- Transportation related resilience and future proofing concepts and experiences;
- Infrastructure related resilience and future proofing;
- Systems and technology related resilience and future proofing; and
- ITS specific resilience and future proofing.

The intent of this broad review of resilience and future proofing was to glean as much as possible from other industries that could translate to the narrow emphasis of this study (i.e., ITS assets).

Chapter 10 identifies the primary resources referenced in this document, with brief summaries of the key takeaways from each.

2.0 Approach to Research

2.1 Overall Approach

The primary research activity was a literature review of resources both from within the transportation industry and external to the transportation industry, with the intent of learning as much as possible about resilience and future proofing. In addition to the literature review, the Project Champion and support contractor conducted bi-weekly discussions to interpret the content learned in the literature review and formulate an overall approach to future proofing ITS assets. Finally, the ENTERPRISE Pooled Fund Study (PFS) members were engaged through a series of webinars to review and react to the concepts developed, leveraging the combined insight of the member agencies to help finalize the concepts.

2.2 Research Steps

The research can be described as four sequential steps, each one building on the outcome and findings of the earlier steps. These steps are described below and illustrated in Figure 6.

2.2.1 Step One: Understanding of Threats to the Future Proofing of ITS Assets

The initial focus of the literature review was to understand the threats to ITS assets and the risks that result from these threats. Once these were defined, a series of mitigating actions were identified, either through published materials or derived from discussions and interpretations about the material.

2.2.2 Step Two: Researching Where ITS Future Proofing Fits in the DOT Business Model

Using the candidate actions to mitigate risks to future proofing ITS assets defined in Step One, Step Two benefitted from key insights in the literature review that suggested future proofing should not be a stand-alone activity, but rather integrated into the existing structure of an agency. Building upon this, Step Two explored the areas and activities (areas/activities) common to most DOTs to identify suggestions for how a typical DOT business model might perform the mitigating actions identified in Step One. The outcome was a set of assigned actions for each DOT area to consider.

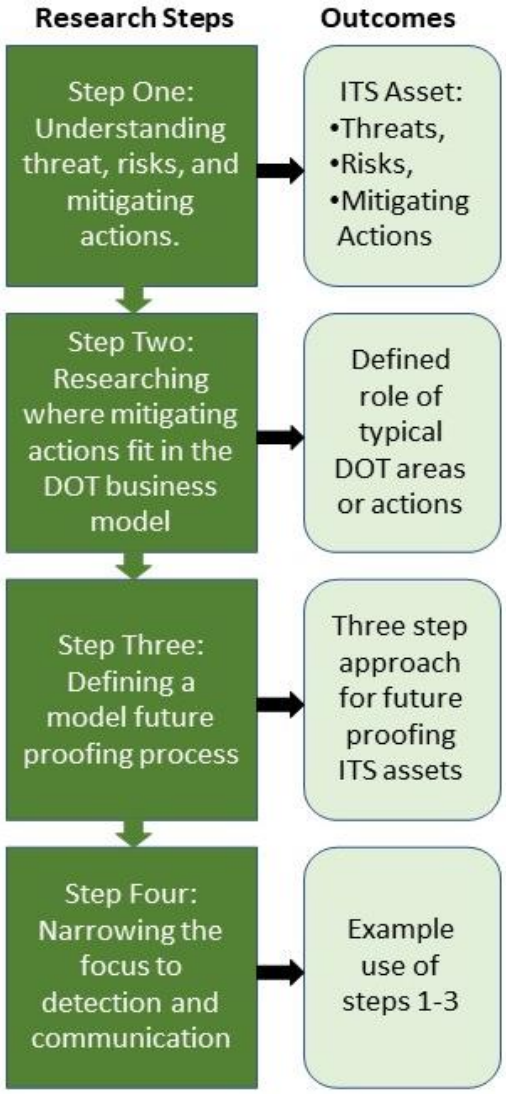


Figure 6: Research Steps and Outcomes

2.2.3 Step Three: Defining a Model Future Proofing Process for ITS Assets

The intent of Step Three was to define a model future proofing process that DOTs can consider and adapt as needed to fit their overall needs.

2.2.4 Step Four: Narrowing the Focus to Detection and Communication

Step four was intended to demonstrate how the research findings could be used when applied to a specific ITS asset type, as an illustrative scenario example. Two groups of ITS assets, detection and communications, were the focus of a brief illustration of specific examples of the steps agency groups might take to implement the recommended actions.

3.0 Defining Threats and Risks to ITS Assets

3.1 Summary of Resilience and Future Proofing Threats

The first step in understanding and managing an asset's ability to continue to be of value is to understand what threatens the future use of these assets. The website Threatanalysis.com offers clear definitions and interpretations of some often-misused terms[4] as follows:

- ***Asset*** – People, property, and information. An asset is what we're trying to protect.
- ***Threat*** – Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. A threat is what we're trying to protect against.
- ***Vulnerability*** – Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. A vulnerability is a weakness or gap in our protection efforts.
- ***Risk*** – The potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability. Risk is the intersection of assets, threats, and vulnerabilities.

Based on these definitions and the research in this project, seven types of threats (i.e., Threat Types) have been identified that might impact the future value of ITS assets, summarized as follows:

- ***Natural Threats*** – Including climate change, specific weather events, exposure to daily weather elements, insects, and other creatures and overall wear and tear through continuous exposure to the elements.
- ***Human Interactions*** – Including human inflicted vandalism or events such as vehicular collisions with the ITS asset.
- ***Functional Performance Threats*** – Where assets no longer perform functionally, either because they are incompatible, outdated, or no longer used by the primary user group.
- ***Extended Use Threats*** – In situations where the ITS asset is used longer than the planned life expectancy or when hardware and software support and replacements are no longer available.
- ***Financial Threats*** – Including the risk of excessive cost increases for maintenance or operations of the assets, as well as threats of reduced funding to maintain or operate the asset.
- ***Policy/Regulatory Threats*** – Including threats to the future "allowed use" of assets (e.g., if licensing changes no longer allow use of a device) as well as threats related to agency specific policies that may change (e.g., selecting the use of a specific vendor product).
- ***Security Threats*** – Including threats from unwanted intentional attacks.

For each threat type, one or more specific threats have been defined, based on the research in this project and experiences of the project team. Table 2 defines the threats specific to each threat type that will be the basis for the remainder of this report. Note that this list is not intended to represent an all-inclusive list of threats or threat types. Section 5 will include suggestions for considering additional (agency specific) threats.

Table 2: Seven Threat Types, and Potential Threats to ITS Assets

Threat Type	Potential Threats to ITS Assets
Natural	**Wear and Tear** – ITS assets are exposed to elements (e.g., air, water, insect infestations) and may cause faster than expected deterioration. **Weather Events** – Regular and unusual events (e.g., flood, wind, lightning) that cause inoperability of ITS assets.
Human Interactions	**Vandalism –** Physical damage or theft of ITS assets caused by vandalism. **Event Exposure –** ITS assets damaged by vehicles crashing or colliding with the assets or other non-natural events.
Functional Performance	**Incompatibility** – System is not compatible with future devices, communications, security, etc. **Outdated** – System is no longer effective compared to current state of practice. **Unused** – Even when functioning properly, system is no longer used by primary user group because it does not meet their needs.
Extended Use	**Exceeding Life Expectancy** – Attempting to use ITS assets beyond the intended life expectancy, coupled with the challenge of estimating life expectancy of technology devices and systems. **Limited Expansion Capacity** – Use of ITS assets may require expansion and without capacity to expand the usefulness of the asset may be jeopardized. **Unavailable Support –** Hardware or software support to the ITS asset is no longer available, including replacement parts.
Financial	**Excessive Cost Increases** – System maintenance or operation costs are no longer practical. **Missed Opportunities** – System does not allow an agency to benefit from lower cost options (e.g., devices, communications, maintenance). **Reduced Funding** – Agency allocation of funds to the ITS solution is reduced.
License, Policy, and Regulatory	**Allowed Use** – Licensing, policy, and/or regulations may prevent future use of system components. **Agency/Department Policy Decisions** – Threats that may result from changes to agency policies and/or procedures.
Security	**Security Threats** – Security vulnerabilities may open devices to hackers and intentional attacks. **Limited Accessibility** – Security precautions (e.g., firewalls) could prevent use of ITS assets.

3.2 Understanding the Risks Related to ITS Future Proofing

In Section 3.1, seven types of threats were introduced. However, it is difficult to assess and respond to threats alone. The research revealed that defining the risks that are caused by each threat helps to understand the likely impacts and eventually implement strategies for managing risks created by the threats. As noted above, risks are defined as the potential loss, damage, or destruction of assets caused by one or more threats. The AASHTO document Understanding Transportation Resilience: A 2016-2018 Roadmap published in 2017[1] describes a suggestion of defining as many risks as possible, as well as

defining opportunities for mitigating these risks. The AASHTO report goes on to note that risks are best described as a series of "if-then" statements to frame them in the context of contributing factors and resulting risks.

Risks Impacting Individual Assets vs. Groups of Assets

As was noted in a project workshop, the risks to ITS assets that result from the threats may be risks to individual devices (e.g., one DMS may be at risk due to vandalism if not protected) or may be risks to groups of devices (e.g., if an agency purchases 20 DMS from a vendor that is no longer available to support the devices, all 20 are at risk). Agencies should consider whether the risks to ITS assets would impact individual assets or groups of assets when assessing and mitigating the risks.

Table 3 summarizes the key outcomes of Step One by revisiting the threats introduced in Section 3.1, but also identifies a series of risks for each potential threat. This list is not intended to be an all-inclusive set of risks, but rather to represent the most likely risks, as defined by the research team and the literature reviewed. Each risk is also identified by "Individual," "Group," or both to indicate the most likely impacts.

Table 3: Outcomes of Research Step One: Threats, Risks, and Actions to Mitigate Risks

Potential Threats	Risks (written as "if/then" statements)
Threat Type: Natural ***Threat: Wear and tear*** – ITS assets are exposed to elements (e.g., air, water, insect infestations) and may cause faster than expected deterioration.	• IF the system is continuously exposed to elements without proper protection, THEN service disruption may occur. (Individual) • If the system design is excessive in protecting against extreme weather conditions, then system costs could be inflated. (Individual)
Threat Type: Natural ***Threat: Weather Event*** – Regular and unusual events (e.g., flood, wind, lightning) that cause inoperability of ITS assets.	• IF weather events occur, THEN service disruptions may interrupt access to data and information when it is most needed. (Individual & Group)
Threat Type: Human Interactions ***Threat: Vandalism*** – Physical damage or theft of ITS assets caused by vandalism.	• IF ITS assets are vandalized, THEN the functionality of that device and others depending upon it will be jeopardized. (Individual) • IF ITS assets are stolen, THEN complete replacement and integration of a new device will be required. (Individual)
Threat Type: Human Interactions ***Threat:* Event Exposure –** ITS assets damaged by vehicles crashing or colliding with the assets or other non-natural events.	• IF crashes or collisions with ITS assets could cause them to need to be replaced, THEN costs for replacement would not be covered by warranty and would require investment to replace. (Individual)
Threat Type: Functional Performance	• IF the solution deployed is not compatible with future state of practice devices or communications, THEN early replacement may be needed, and an agency will either incur unplanned costs

Potential Threats	Risks (written as "if/then" statements)
Threat: Incompatibility – System is not compatible with future devices, communications, security, etc.	or experience service disruption. (Individual & Group) • IF the solution deployed is only partially compatible with future state of practice devices or communications, THEN partial interoperability issues may cause degraded performance. (Group)
Threat Type: Functional Performance ***Threat: Outdated***– System is no longer effective compared to current state of practice.	• IF future products/services are better performing or preferred by users, THEN users will discontinue using the deployed system (e.g., switch to Internet-based sources of data vs. DOT provided). (Group) • IF future products/services are better performing or preferred by users, THEN system outputs may have accuracy and/or reliability issues when compared to industry standards. (Group)
Threat Type: Functional Performance ***Threat: Unused*** – Even when functioning properly, system is no longer used by primary user group because it does not meet their needs.	• IF a majority of the general public users of the solution stop using the ITS solution and seek alternatives (e.g., switch from a DOT solution to private offered application), THEN the cost per user will be substantial and could create difficult decisions for the agency (e.g., do they continue something used by a small user group). (Group) • IF DOT staff do not need the full functionality of the ITS solution, THEN portions of it may go unused. (Group)
Threat Type: Extended Use ***Threat:* Exceeding Life Expectancy** – Attempting to use ITS assets beyond the intended life expectancy.	• IF ITS assets are used longer than the design life (life expectancy) THEN there is an increased risk of system failures without cause. (Individual & Group) • IF ITS assets are used longer than the design life, THEN there is risks of degraded service. (Individual & Group)
Threat Type: Extended Use ***Threat:* Limited Expansion Capacity** – Use of ITS assets may require expansion and without capacity to expand the usefulness of the asset may be jeopardized.	• IF the use of a specific ITS asset requires increasing space (e.g., cabinet space, structure space, right-of-way), power, or connections, and expansion is limited, THEN the full benefits of the ITS asset may not be recognized.
Threat Type: Extended Use ***Threat:* Unavailable Support –** Hardware or software support to the ITS asset is no longer available, including replacement parts.	• IF the asset supplier no longer makes hardware or software available, THEN maintaining and repairing the ITS asset may become impossible, time consuming, or expensive. (Group)
Threat Type: Financial ***Threat: Excessive Cost Increases*** – System maintenance or operation costs are no longer practical.	• IF the costs to maintain or operate the solution become high, THEN operations of the system may be discontinued (while still demanded by users). (Individual & Group) • IF the costs to maintain or operate the solution become high, THEN the agency may incur higher than expected costs to maintain operations and, if continued, may eliminate other services. (Individual & Group)
Threat Type: Financial	• IF the design of the system favors proprietary maintenance or operations and prevents agency from benefiting from lower

Potential Threats	Risks (written as "if/then" statements)
Threat: Missed opportunities – System does not allow an agency to benefit from lower cost options (e.g., devices, communications, maintenance).	costs to maintain or operate the solution, THEN agency will incur higher than expected costs to maintain operations and, if continued, may eliminate other services. (Group) • IF the design of the system favors proprietary maintenance or operations and prevents agency from benefiting from lower costs to maintain or operate the solution, THEN agency may have to forego feature upgrades or coverage expansion that would be possible if costs were lower. (Group)
Threat Type: Financial ***Threat: Reduced Funding –*** Agency allocation of funds to the ITS solution is reduced.	• IF the agency funds available to system operation and upgrades is reduced, THEN the system may no longer be feasible to operate. (Individual & Group)
Threat Type: License, Policy and Regulatory ***Threat: Allowed Use*** – Licensing, policy, and/or regulations may prevent future use of system components.	• IF licensing, policy, or regulatory rules change, THEN agency may need to replace equipment, incurring significant costs. (Individual & Group) • IF licensing or regulatory rules change, THEN agency may discontinue service if replacement is not possible/affordable. (Individual & Group)
Threat Type: Policy & Regulatory ***Threat: Agency/Department Policy Decisions*** – Threats that may result from changes to agency policies and/or procedures.	• IF an agency or department policy decisions change, THEN the future technical and financial support of the ITS solution may be jeopardized. (Individual & Group)
Threat Type: Security ***Threat: Security Threats*** –Security vulnerabilities may open devices to hackers and intentional attacks.	• IF the solution deployed does not maintain adequate security, THEN agency may be vulnerable to attacks, impacting not only the devices but other agency systems. (Individual & Group) • IF the solution deployed does not maintain adequate security, THEN agency may risk the contact details of users being jeopardized. (Individual & Group)
Threat Type: Security ***Threat: Limited Accessibility*** – Security precautions (e.g., firewalls) could prevent use of ITS assets.	• IF the functionality and/or use of the ITS asset relies on accessibility that is not allowed by a firewall or other security aspect, THEN the intended use and benefits of the ITS asset may not be recognized. (Individual & Group)

4.0 Challenges to Future Proofing ITS Assets

This chapter summarizes research findings that describe the challenges that state and local DOTs may be facing, and will continue to face, as they future proof ITS assets.

4.1 Synthesis of Challenges Related to Resilience and Future Proofing in General

Findings from the synthesis have identified three primary challenges to future proofing, summarized as:

- Uncertainty is a primary (if not the primary) challenge facing resilience and future proofing.
- Current approaches to future proofing may not be appropriate or effective.
- The challenge of trying to solve future proofing when it should be managed.

The following subsections explore details of each of these challenges.

4.1.1 Challenge #1: Uncertainty as a Challenge Facing Resilience and Future Proofing

Whether the topic of resilience and/or future proofing is regarding climate change, major weather events, or the release of new products that makes existing products redundant, one common theme exists in all examples of resilience and future proofing and that is uncertainty. No one can predict the future with 100% certainty. In 2020, state DOTs learned that even if they have deployed connected vehicle field equipment based on licenses issued by the FCC, those licenses can be taken away from them. Similarly, while there are predictions of timelines when climate change may impact sea levels, there is still uncertainty over the timelines for these. A Nossaman online document[5] discusses Uncertainty as a primary challenge facing resilience, with insightful observations, quoted as follows:

> *"Behind these news strategies lies one key truth – resilience reflects uncertainty. Indeed, it is our inability to know what combination of stressors will occur in the future that must guide our planning."*
>
> *"If the future was predictable, resilience would lose its importance. But since the future is unpredictable, it is necessary to plan for a wide range of possible conditions. Executing these strategies requires a multidisciplinary approach, which draws on the principles of redundancy, responsiveness, and coordination."*

4.1.2 Challenge #2: Current Approaches to Future Proofing May Not Be Appropriate or Effective for ITS Assets

Traditional engineering practices include provisions for designing for expansion, whether it be designing for additional floors that may be added to a building, designing for heavier loads of vehicles or pedestrians than exist when the design happens, or any number of other examples. The future proofing challenges facing industry today represent different types of considerations. In 2021, technology turnover can be months, not decades as it was in the past. New products, companies, and services are introduced regularly, supported by the Internet of Things (IoT) and use of applications. While the

approaches used to future proof physical infrastructure may be applicable, the digital infrastructure that is increasing in importance will likely not be future proofed using the similar approaches.

In a report titled "Future-proofing 'Next Generation' Infrastructure Assets"[3], the authors, after researching this topic summarized that *"the research that has been undertaken has tended to develop new policies and frameworks that have been simply superimposed on top of existing processes that are unable to cope with the complexities and nuances needed to provide resilient and adaptive assets."* The authors go on to make the point that infrastructure assets are increasingly likely to be delivered unsuccessfully as costs and schedules increase.

4.1.3 Challenge #3: The Challenge of Trying to Solve Future Proofing When it Should be Managed

Given the concept of uncertainty being a major challenge to future proofing and the concepts that the increasing complexities and changing industry around transportation system deployments, the third challenge area is that agencies are possibly trying to avoid or solve future proofing risks, when they should be managed.

Illustrative Example: US Air Force Expectations of a Robust System

An INCOSE report in 2017[6] describes the expectations of the US Air Force for a robust system, with the following bullets:

- Capable of adapting to changes in mission and requirements;
- Expandable/scalable and designed to accommodate growth in capability;
- Able to reliably function given changes in threats and environment;
- Effectively/affordably sustainable over their lifecycle;
- Developed using products designed for use in various platforms/systems; and
- Easily modified to leverage new technologies.

The report goes on to indicate that in order to accomplish these, a system needs to be flexible, maintainable, agile, upgradable, modular, resilient, adaptable, and robust. These findings reinforce the concepts introduced in Chapter 3 that the goal should be managing future proofing through all aspects of the system procured.

New Zealand research[7] ***Defines challenges*** that need to be overcome in order to design for resilience:

- Engineering challenges need to be seen as conditions to be managed, rather than problems to be solved.
- Current approaches focus on known, identified hazards and ignore the significance of unidentified hazards either via assumption or because of cost constraints. This issue is fundamental when exploring resilience and risk.
- Current design practices are based on existing codes and are sanctioned by agencies. These codes ignore the possibility of unidentified or emergent hazards.

5.0 Fitting ITS Future Proofing into the DOT Business Model

This chapter defines a concept for how ITS future proofing can fit within a typical DOT business model, with the goal of managing the risks and threats to ITS assets, while recognizing and overcoming the three challenges introduced in Chapter 3.

5.1 Proposed Concept for How ITS Future Proofing Fits in the DOT Model

Based on a synthesis of the resources reviewed in this project, three concepts are introduced regarding where ITS future proofing should fit in the DOT business model:

- *Future proofing* ***should not be an after-thought*** *following deployment of an ITS solution, rather it should begin in project conception.*
- *Future proofing* ***should be managed throughout the entire process*** *of considering, designing, procuring, installing, and operating the ITS solution.*
- *Whenever possible,* **future proofing should be part of existing business, technical, and financial activities of the DOT** *– not implemented as a new stand-alone area or activity.*

The culmination of these three concepts is a suggestion that future proofing should be addressed by the activities of seven existing areas/activities within each DOT. These seven areas are identified in Figure 7.

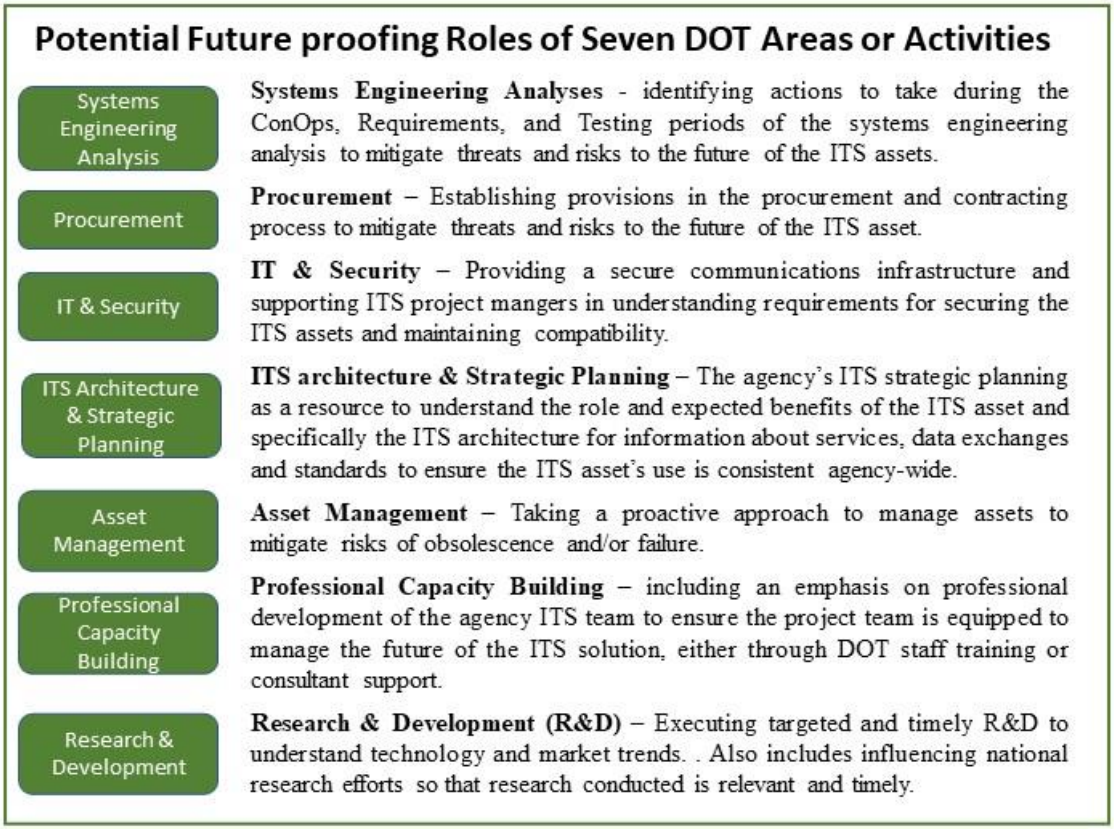


Figure 7: Areas/Activities of State DOTs That May Contribute to Managing Future Proofing

5.1.1 Role of Systems Engineering in ITS Future Proofing

A systems engineering analysis is a common first step in designing and deploying ITS assets. Whether this is conducted by an office dedicated to systems engineering, or by the project team assigned to a project, there are several activities that can be done as part of the systems engineering process to mitigate the risks to the future of the device or system. Table 4 describes the potential role of systems engineering in future proofing.

Table 4: Systems Engineering Role and Timing in ITS Future Proofing

What threats/risks can the Systems Engineering process help mitigate?	• Natural threats, including wear and tear and weather event threats (defining the system environment).
	• Human Interaction threats, including vandalism and event exposure.
	• Functional Performance threats including:
	  ○ Incompatibility with future devices/communications;
	  ○ Outdated or ineffective compared to future systems;
	  ○ Systems or components that are unused even if functioning properly; and
	  ○ Risks that internal and external systems are not integrated (i.e., cross-system integration).
	• Extended use threats, including limited expansion capacity, and exceeding life expectancy.
	• Financial threats, including missed opportunities (if the design is not open to non-proprietary solutions).
	• Security threats if the security vulnerabilities are not documented.

What role is needed from the Systems Engineering process?	• Ensure that the system environment and external conditions (including weather extremes) are defined and translated into requirements. • Ensure that protection against vandalism and vehicular crashes is appropriately included in requirements. • Ensure that current and forecasted end user needs are defined and translated into requirements. • Ensure that performance and compatibility objectives are defined and translated into requirements. • Ensure interoperability with other existing and planned systems. • Ensure that projected expansion needs are identified and included in requirements. • Ensure that life expectancy of ITS assets is considered when developing operational concepts and plans for future replacements. • Ensure that ongoing maintenance and operations needs are defined and translated into requirements. • Define acceptance test procedures based on requirements. • Ensure that cross agency data integrates.
When should the Systems Engineering process perform this role?	• The systems engineering process is recommended for all ITS projects. • The most applicable portion of the systems engineering process to this role is during the Concept of Operations (ConOps), Requirements, and Testing portions of the systems engineering process (i.e., the downward slant of the "Vee" diagram).

5.1.2 Role of Procurement in ITS Future Proofing

The procurement process is an opportunity to consider what will mitigate future proofing risks when selecting a contractor, vendor, or device provider. Similarly, by including provisions in the procurement and contract signing phase of the project, safeguards can help to minimize future risks.

Table 5: Agency Procurement Role and Timing in ITS Future Proofing

What threats/issues can procurement help mitigate?	• Functional Performance threats including incompatibility
	• Extended use threats, including unavailable support for ITS assets in the future.
	• Financial threats, including:
	  ○ Excessive cost increases; and
	  ○ Missed opportunities

What role is needed by procurement?	• Support project managers (PMs) in considering procurement language to support compatibility with current and future systems? • Include procurement language or proposal/bid requirements that minimize risks of excessive cost increases in the future (e.g., require clear declarations of warranty coverage, require costs and labor rates for periods beyond warranty periods)? • Include procurement considerations to minimize the risks that hardware or software replacements will not be available in the future. • Require bidders to describe the process (and hours) for agency performed maintenance beyond the warranty period?
When should Procurement be involved?	• Prior to the final definition of requirements. • During procurement and evaluation of bids.

5.1.3 Role of IT and Security in ITS Future Proofing

Information Technology (IT) and security activities of an agency typically maintain the communications, power, and other utilities needed by ITS equipment and ensure the technology systems are secured.

Table 6: ITS/Security Role and Timing in ITS Future Proofing

What threats/issues can IT/security help mitigate?	• Security threats, including:
	  ○ Threats to the security of the agency and travelers, and
	  ○ Threats of limited accessibility to ITS assets.
	• Functional Performance Threats, incompatibility with future devices, communications, and security.

What role is needed by IT/security?	• Providing overall guidance and resources to support ITS Project Managers (PMs) in understanding how to mitigate security and cybersecurity threats. • Providing input to requirements and specifications during the project procurement/contracting period for cyber prevention, IT compatibility, and accessibility to the ITS asset and data generated by it. • Participating in procurement processes to review proposals for security or compatibility concerns. • Participating in acceptance testing prior to final approval of deliverables to ensure security and compatibility concerns are addressed.

When should IT/security be involved?	• Continuously by providing overall guidance. • During the systems engineering and procurement phases. • During the installation/acceptance phase.

5.1.4 Role of the ITS Architecture and Strategic Planning Efforts in ITS Future Proofing

Strategic planning allows a programmatic approach towards the deployment and operations of ITS devices and systems. The ENTERPRISE Pooled Fund Study Report titled "Evolving and Phasing Out Legacy ITS Devices and Systems"[8] cites several examples of strategic technology obsolescence planning, including the following:

- ITS Device Obsolescence and Modernization Planning (Michigan DOT)
- Antiquated ITS Devices Effort (PennDOT)
- ITS Device Replacement Planning (ODOT)
- Device Consistency (ODOT)
- Continual Evaluation of ITS Technology Needs (MassDOT)

The ITS Architecture provides a common framework for planning, defining, and integrating ITS. Project architectures create descriptions of services to be provided, relationships required, and items to be deployed. The Functional View of the architecture describes the processes and data flows to satisfy system requirements. The Communications View describes the communications protocols and standards needed to support communications among the physical objects.

Through strategic ITS planning and the use of the ITS Architecture to understand and deploy the ITS asset using the appropriate data flows and standards, risks of incompatibility with other devices (current or future) can be minimized.

Table 7: ITS Architecture & Strategic Planning Efforts Role and Timing in ITS Future Proofing

What threats/issues can the ITS Architecture & Strategic Planning help mitigate?	• Functional performance threats, including incompatibility with future devices and communications. • ITS device replacement planning. • ITS device obsolescence and modernization planning.
What role is needed from ITS Architecture & Strategic Planning activities?	• Provide an overall programmatic plan for the use of ITS assets, including evaluation criteria to understand benefits of ITS solutions. • Help to understand the overall goals of ITS solutions in order to accurately assess the benefits received. • Assist PMs in identifying the range of services related to the ITS asset deployment (Project architecture). • Assist PMs in identifying the data flows. • Assist PMs in identifying the communications protocols and standards needed to support the data flows.
When should the ITS Architecture &	• Strategic planning has potential to mitigate future proofing risks on a continuous basis.

Strategic Planning perform this role?	• The use of the ITS Architecture should begin as early in the deployment as possible and continue through operations.

5.1.5 Role of Asset Management in ITS Future Proofing

The Asset Management activities in an agency may provide a mechanism to take a proactive role to managing assets. Asset Management can assist in activities such as:

- Early identification of complementary or competing technology solutions.
- Understanding impacts of emerging technologies on ITS assets
- Cost considerations of implementing emerging technologies against risks to future use of existing systems.

Table 8: Asset Management Role and Timing in ITS Future Proofing

What threats/issues can Asset Management help mitigate?	• Functional Performance threats, including:
	  ○ Risk of the asset becoming outdated (by annual assessments of emerging technologies)
	• Extended Use threats, including:
	  ○ Limited expansion capacity and
	  ○ Unavailable hardware and software support.
	• Financial threats, including:
	  ○ Risk of excessive cost increases
	  ○ Risk of reduced funding availability (by understanding the lifecycle costs to allow for budgeting)
	  ○ Risk of missed opportunities for lower cost options in the future.

What role is needed from the Asset Management?	• Conduct periodic assessments of emerging technologies to identify complementary and/or competing technology solutions to the system. • If identified, assess whether emerging technologies will impact the system and if/how they could be incorporated. • Include assessments of space for asset expansion. • Include assessments to predict future unavailability of hardware or software related to ITS assets. • Include assessments to identify new and evolving risks. • Manage replacement part supply to support continuous operations. • Consider costs of implementing emerging technologies against risks to future use of existing systems. • Support lifecycle analyses of various funding scenarios. • Describe the role of field visits for inspecting and assessing ITS asset conditions.

What threats/issues can Asset Management help mitigate?	• Functional Performance Threats, including:
	  ○ Risk of the asset becoming outdated (by annual assessments of emerging technologies)
	• Financial threats, including:
	  ○ Risk of excessive cost increases
	  ○ Risk of reduced funding availability (by understanding the lifecycle costs to allow for budgeting)
	  ○ Risk of missed opportunities for lower cost options in the future.

5.1.6 Role of Professional Capacity Building in ITS Future Proofing

Professional capacity building (PCB) represents those activities in the DOT dedicated to helping keep ITS project managers and subject matter experts (SMEs) informed about research and development (R&D) findings, real-world field deployments, and overall advances in technologies. PCB will mostly support non-project specific activities, such as annual training, access to research, and generally enabling ITS professionals to better understand technology trends.

Table 9: Professional Capacity Building (PCB) Role and Timing in ITS Future Proofing

What threats/issues can PCB help mitigate?	• Natural threats including:
	  ○ Threats due to weather events and climate change
	• Functional Performance threats including:
	  ○ Threat of incompatibility with future devices/communications
	  ○ Threat of being outdated or ineffective compared to future systems
	  ○ Threat of being unused by the primary user group, even if still functional.
	• Policy and regulatory threats including:
	  ○ Threats of allowed use (e.g., licensing or regulatory actions that may prevent use)
	  ○ Threat of agency policy decisions that impact future use.

What role is needed from PCB?	• Include an emphasis on PCB of the agency ITS team to ensure they are equipped to manage the future of the ITS assets, either through DOT staff training or consultant support. • Address the challenge of knowledge retention within the DOT to avoid losing critical knowledge during staff turnover or position changes. • Incorporate business decision processes into PCB to encourage consideration of costs of implementing emerging technologies against risks to future use of existing systems. • Support PMs and SMEs to understand technology trends. • Support PMs and SMEs to understand current and possible changes to policies/regulations (internal and external). • Support PMs and SMEs in understanding environmental impacts on ITS assets.
When should PCB perform this role?	• Allow time for PCB on a regular basis. • During project periods, allow additional (project related) PCB.

5.1.7 Role of Research and Development in ITS Future Proofing

Research and Development (R&D) can help agency project managers understand a variety of concepts that will provide background into decisions to mitigate future proofing risks to ITS assets. Examples of these include:

- Trends that will impact ITS assets (e.g., technology, private products, trending threats, actual usage, or user preferences);
- Positive experiences of other state DOTs preparing for future proofing;
- Negative experiences of other state DOTs regarding future proofing.

Understanding these will help project managers make decisions about project approach, ITS asset procurement, selection, deployment and integration, minimizing the risks of future proofing.

Table 10: Research and Development Role and Timing in ITS Future Proofing

What threats/ issues can R&D help mitigate?	• Functional Performance threats including:
	  ○ Threat of incompatibility with future devices/communications
	  ○ Threat of being outdated or ineffective compared to future systems
	  ○ Threat of being unused by the primary user group, even if still functional.
	• Financial threats, including:
	  ○ Risk of excessive cost increases.

What role is needed from R&D?	• Help PMs and SMEs better understand technology and market trends through local R&D project selection and by influencing national research efforts. • Help PMs understand usage trends, user preferences, costs, and cost-benefit of individual devices or an entire ITS system, to assist with selecting and prioritizing ITS investments. • Help agency PMs and SMEs consider the most recent trends in ITS asset future proofing by shortening the timeline of agency R&D project selection and performance.
When should R&D perform this role?	• Ongoing through annual R&D activities • In anticipation of upcoming projects (tailored research) • When new technologies are introduced (tailored research)

6.0 Defining a Model Future Proofing Process

6.1 Proposed Overall Approach to Future Proofing ITS Solutions

The 2017 AASHTO Report[1] describes the importance of understanding risks, incorporating resilience into operational practice, developing tools, models, and standards to mitigate risks, and reviewing progress on mitigating risks. Based on this, as well as the overall synthesis of research, a three-step approach is proposed to Plan, Act, and Reflect/Repeat future proofing for ITS solutions as illustrated in Figure 8 below.

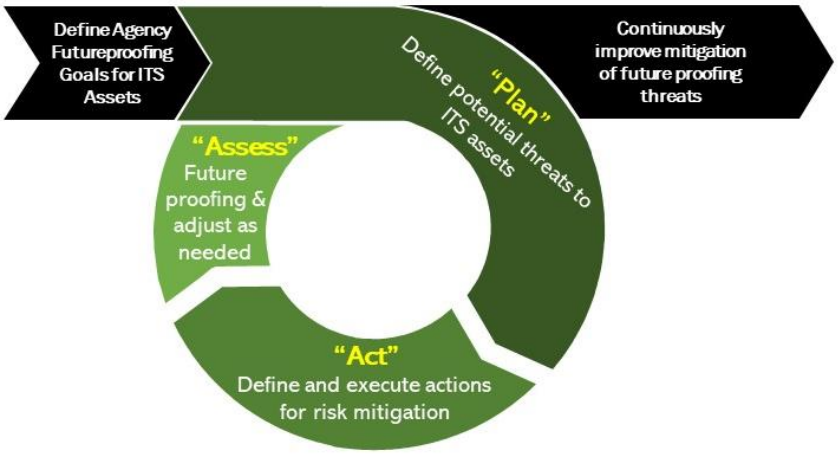


Figure 8: Repeating Approach to Plan, Act, and Assess Future Proofing

6.2 Step 1: Plan for ITS Future Proofing

During the "Plan" step, agencies are encouraged to define potential threats to assets and to perform general actions (i.e., not specific to a project or individual asset) that will help mitigate the risks to future proofing.

Defining Potential Threats to ITS Assets. Once high-level goals for future proofing ITS assets are defined, agencies are encouraged to review the seven threat types defined in Section 3.1. Agencies may determine some of these threats are not applicable to their ITS assets and/or may identify additional threat types not described in this report.

Step 1 – "Plan" Recommended Action #1:

Agencies should review the potential threat types and individual threats, identifying those that they wish to prioritize and manage when planning, deploying, operating ITS assets.

Define and execute actions (not project specific) to prepare for future proofing. Based on the research and collaboration of the project team, a series of potential activities have been defined that agencies can perform to prepare for future proofing ITS assets. These activities are not specific to individual projects, but rather should be done on a regular basis to help mitigate risks to ITS assets. Table 11 identifies the threat type, and recommended (non-project-specific) actions, while also identifying the DOT area/activity most likely to perform the action.

Table 11: Recommended Non-Project Specific Actions to Mitigates Threats and Risks to Future Proofing

Threat Type	Suggested Actions & DOT Area/Activity Most Likely to Perform the Action
Universal to All Threats	***ITS Architecture and Strategic Planning*** • Plan strategically for future technologies at a programmatic level in order to understand the needs being addressed and metrics of performance for each ITS system deployed. • Conduct regular strategic ITS planning to assess current devices and systems to identify obsolescence of legacy systems and evolution opportunities. Examples of state DOT approaches to this are available in the ENTERPRISE Pooled Fund Study report titled "Evolving and Phasing Out Legacy ITS Devices and Systems"[8] ***Research & Development Actions:*** • Shorten the timeline of agency R&D choice selection and R&D performance such that agency SMEs can consider the most recent trends in ITS asset future proofing. • Influence national research efforts to focus on ITS asset future proofing. ***Professional Capacity Building Actions:*** • Ensure ITS staff have adequate time to participate in national research efforts and/or to read and process the research results to better understand trends in future proofing ITS assets. ***Procurement Actions:*** • Track national trends and success stories of other agencies including contract provisions to future proof ITS assets and incorporate these into standard procurement procedures, to the extent possible.
Natural Threats	***Research & Development Actions:*** • Participate in research activities to understand risks to ITS assets related to environmental conditions. • Participate in research to evaluate the performance of emerging technologies in mitigating impacts to ITS assets from natural threats. ***Professional Capacity Building:*** • Support awareness and education for staff regarding the impact of climate change and its potential long-term impact on assets.

Threat Type	Suggested Actions & DOT Area/Activity Most Likely to Perform the Action
Human Interaction Threats	***Research & Development Actions:*** • Participate in research activities related to minimizing vandalism risks to ITS assets. • Participate in research activities related to protecting ITS assets from crashes or other events. ***Asset Management:*** • Include protection of ITS assets and damage caused by vandalism in the overall asset management program.
Functional Performance Threats	***Research & Development Actions:*** • Participate in research that helps agency SMEs understand trends in the use of ITS assets (e.g., is the asset use trending riskier? Or less risky?) ***Professional Capacity Building Actions:*** • Support awareness and education for staff in emerging technologies. ***ITS Architecture and Strategic Planning:*** Plan strategically for end use scenarios of the ITS assets to understand the needs of users and role of ITS to address them.
Extended Use Threats	***Procurement Actions:*** • Consider developing standard procurement language to consider the risks of hardware/software support and replacement for the ITS asset during the procurement process. ***Asset Management Actions:*** • Include assessments of space for asset expansion. ***Professional Capacity Building Actions:*** • Support ITS staff awareness of open source and other non-proprietary approaches to ITS asset deployment. ***Systems Engineering:*** • Encourage regular habits of writing requirements to support scalable systems.
Financial Threats	***Procurement Actions:*** • Periodically assess procurement processes to understand risks to future proofing (e.g., forward compatibility, costs of changes, warranty period). ***Research & Development Actions:*** • Research advances in procurement processes for ITS assets to minimize risks of unexpected contract costs. ***Professional Capacity Building Actions:*** • Support ITS staff awareness of open source and other non-proprietary approaches to ITS asset deployment.
Policy / Regulatory Threats	***Professional Capacity Building:*** • Become familiar with possible changes (planned or pending) in agency policies that could impact ITS asset operations or maintenance.

Threat Type	Suggested Actions & DOT Area/Activity Most Likely to Perform the Action
Security Threats	***IT/security:*** • Provide overall guidance, resources, and education to support ITS Project Managers (PMs) in understanding how to mitigate security and cyber security threats. ***Professional Capacity Building:*** • Familiarize staff with overall cybersecurity protocols and ITS assets (in general) will be impacted by these protocols.

"Plan" Recommended Action #2:

Using Table 11 above, agencies are recommended to consider performing each suggested activity as a part of managing future proofing ITS assets within their organization.

6.3 Step 2: "Act" Managing ITS Future Proofing

During the "Act" step, agencies are encouraged to incorporate future proofing actions into project activities that include the planning, deployment, and operations of the ITS asset. For each deployment, agencies are encouraged to consider the potential threats and risks to the ITS asset. It is important to recognize that future proof risk management is not about avoiding all risks, but rather determining which risks to avoid, which risks to transfer, and which risks to mitigate.

6.3.1 Defining Project Specific Threats and Risks.

Section 3.2 defined an approach of identifying threats and defining risks as "If – Then" statements. When beginning to plan an ITS deployment, agencies are encouraged to refer to Table 3 to consider each threat and risk to determine if the threat/risk combination should be considered for the project. The outcome of this step will be list of possible future proofing risks for the project in consideration. Additionally, agencies are encouraged to explore other risks that are not included in Table 3, capturing specific aspects of the project, location, agency that might create risks.

6.3.2 Determine Whether to Avoid, Transfer, or Mitigate Each Risk.

Future proofing is really risk management. Once agencies identify risks to the ITS assets, they should not try to avoid all risks of future proofing, but rather are encouraged to manage the risks. A key aspect of risk management is determining which risks should be avoided, transferred, or mitigated.

- When you ***avoid a risk,*** it means you change your plan in order to completely eliminate the probability of the risk occurring or the effect of the risk if it does occur. This may involve not proceeding with the project or eliminating some aspects of the planned deployment. It is important to recognize that alterations to a project to avoid a risk may reduce the benefits (to travelers and DOT staff), therefore avoiding risks should be carefully considered before acting.

- ***Transferring a risk*** refers to when the negative impact is shifted to a third party, such as through an insurance policy or penalty clause in a contract. The risk may still occur however the financial impact will be somewhat displaced from the agency. Risk transference usually involves some type of contractual agreement.

- ***Risk mitigation*** occurs when you proactively change the plan to minimize the impact or probability of the risk occurring. Risk mitigation does not eliminate the risk and as such there will be some residual risk remaining. When it is not appropriate to avoid or transfer future proofing risks, mitigate by finding manageable solutions to reduce the risk.

A report titled "Project Risk Resilience" published to the Intaver Institute[9] website, suggests a scale that considers both the probability of the risk and the impact of the risk. The graphic in Figure 9 below summarizes the concept introduced by the Intaver Institute for assessing when to avoid, accept, and mitigate risks.

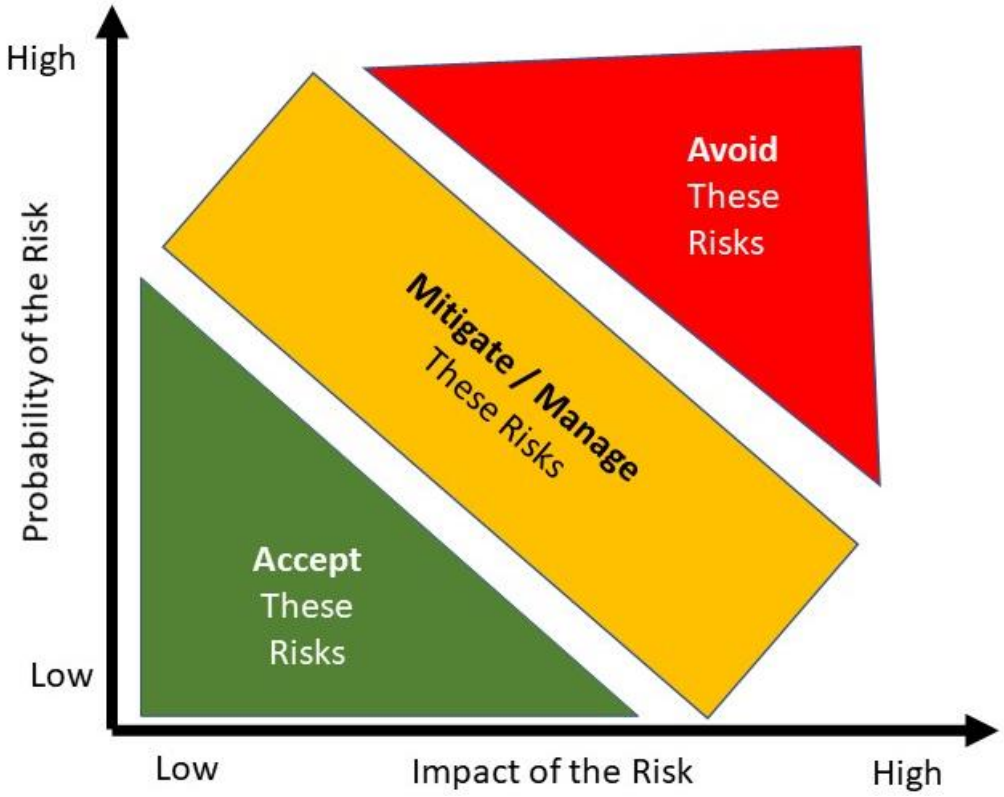


Figure 9: Illustration of the Relationship of Risk Probability and Impact
(Source: Athey Creek Consultants, based on concepts and figures in the Intaver Institute research)

During the 2018 Transportation Resilience Innovations Summit and Exchange, Colorado DOT shared their approach to assessment of risks due to threats. One interesting concept is that they described the assessment of both risks to the travelers (e.g., safety, delay, etc.) caused by threats as well as risks to the agency/owner of the infrastructure (e.g., replacement costs of equipment). Agencies are recommended to consider both types of risks when assessing risks and determining mitigating strategies.

6.3.3 Define and Execute Project-Specific Actions for Risk Mitigation

Risk mitigation is the emphasis of the recommendations of this project, and Table 12 represents the likely threats to ITS assets, risks that may result from the threats, and proposed actions that agencies are encouraged to take on a project-by-project basis to mitigate the risks (each action is identified with the suggested DOT group/activity, based on Figure 7).

Table 12: Recommended Actions to Consider During ITS Projects to Mitigate Threats and Risks to Future Proofing

Potential Threats	Risks (written as "if/then" statements)	Deployment/Project Specific Suggested Actions to Mitigate Risks to ITS Asset Future Proofing
Threat Type: Natural ***Threat: Wear and tear*** – System is exposed to elements and may cause faster than expected deterioration	• If the system is exposed to elements without proper protection, then service disruption may occur. • If the system design is excessive in protecting against rare weather conditions, then the system costs could be inflated.	**Systems Engineering:** • Clearly define the system environment, including extremes, and require the system to meet performance objectives in that environment.[9] • Clearly define external conditions that may impact the system and require the system to meet performance objectives regarding these elements (e.g., if salt, deicing chemicals, or other corrosive materials may be used near the system). **Professional Development:** • Support awareness and education for staff regarding the impact of climate change and its potential long-term impact on assets.
Threat Type: Natural ***Threat: Weather Event*** – Regular and unusual events (e.g., flood, wind, lightning) that cause inoperability of ITS assets.	• If unusual weather events occur (e.g., flooding, or severe winds), then service disruptions may interrupt access to data and information when it is most needed.	**Systems Engineering:** • Include any agency-specific requirements for housing and protecting field equipment from weather events. • Coordinate with emergency response or the group responsible for disaster recovery and backup to define requirements related to weather events. • Consider the needs for backup operations during intermittent outages that may occur with the system and develop requirements as appropriate to ensure back-up systems are included in final design, if appropriate. • Consider technologies or services that are more likely to withstand severe weather events or have increased reliability to remain operational through dedicated service offerings. For example, FirstNet offers public safety agencies dedicated services for wireless communications. **Asset Management:** • Track impacts of natural threats on assets through the asset management approach to better prepare for future threats.

Potential Threats	Risks (written as "if/then" statements)	Deployment/Project Specific Suggested Actions to Mitigate Risks to ITS Asset Future Proofing
Threat Type: Human Interactions ***Threat: Vandalism*** – Physical damage or theft of ITS assets caused by vandalism.	• If ITS assets are vandalized, then the functionality of that device and others depending upon it will be jeopardized. (Individual) • If ITS assets are stolen, then complete replacement and integration of a new device will be required. (Individual)	**Systems Engineering:** • Include requirements for housing and protecting field equipment to minimize risks of vandalism and theft to the extent possible. **Asset Management:** • Track incidents involving human interactions and responses required to restore services through the asset management system to better estimate the resources needed to restore operations after future human interactions. Use this information to estimate impacts to other ITS assets.
Threat Type: Human Interactions ***Threat: Event Exposure*** – ITS assets damaged by vehicles crashing or colliding with the assets or other non-natural events.	• Crashes or collisions with ITS assets could cause them to need to be replaced and costs for replacement would not be covered by warranty. (Individual)	**Systems Engineering:** • Include requirements for housing and protecting field equipment to minimize risks related to vehicular crashes.
Threat Type: Functional Performance ***Threat: Incompatibility*** – System is not compatible with future devices, communications, security, etc.	• If the solution deployed is not compatible with the future state of practice devices or communications, then early replacement may be needed, and unplanned costs incurred. • If the solution is only partially compatible with future devices or communications, then partial interoperability issues may cause degraded performance.	**Systems Engineering:** • Design infrastructure and field equipment as simple as possible and incorporate as many functions as feasible into software/applications for easier upgrades.[10] • When deploying devices, require forward compatibility to anticipate industry changes for at least the warranty period of the devices and avoid planned obsolescence in systems or devices.[11] • Consider the use of extensible design (i.e., a principle that allows a system to expand in functionality or include enhancements without impairing existing functions) or attempt to procure products with inherent extensibility.[12] • Include a review of the agency ITS architecture to support data exchanges and standards compatible with other current or planned systems.[13] Require forward compatibility to anticipate industry changes for at least the warranty period of the devices. **ITS Architecture & Strategic Planning:**

Potential Threats	Risks (written as "if/then" statements)	Deployment/Project Specific Suggested Actions to Mitigate Risks to ITS Asset Future Proofing
		• Add new systems to the ITS architecture to understand data exchanges and standards. • Include a review of the agency ITS architecture to support data exchanges and standards compatible with other current or planned systems. **IT/Security:** • Provide input to requirements and specifications during the project procurement and contracting period to help support IT compatibility.
Threat Type: Functional Performance ***Threat: Outdated*** – System is no longer effective compared to current state of practice.	• If future products/services are better performing or preferred by users, then users will discontinue using the deployed system (e.g., switch to Internet-based sources of data vs DOT provided).	**Asset Management:** • Conduct periodic assessments of emerging technologies to identify complementary and/or competing technology solutions to the system. • If identified, assess whether emerging technologies will impact the system and if/how they could be incorporated. • Consider the costs of implementing emerging technologies against the risks to future use of existing systems. **Professional Capacity Building:** • Support awareness and education for staff in emerging technologies. **Research and Development:** • Evaluate technologies for accuracy, efficiency, and other performance parameters, including evaluating in-place technologies against emerging alternatives.
Threat Type: Functional Performance ***Threat: Unused*** – Even when functioning properly, the system is no longer used by the primary user group	• If a majority of the general public users of the solution stop using the ITS solution and seek alternatives (e.g., switch from a DOT solution to a private offered application), then the cost per user will be substantial and could create difficult decisions for the agency.	**ITS Architecture & Strategic Planning:** • Consider the potential for multiple uses for a single type of ITS device to leverage investments (e.g., detection equipped cameras that can detect both smoke and incidents for tunnel monitoring). • Consider the role of the ITS asset in the overall programmatic plan from the agency in order to help identify the likely benefits of the ITS asset and to effectively assess the actual benefits achieved. **Systems Engineering:**

Potential Threats	Risks (written as "if/then" statements)	Deployment/Project Specific Suggested Actions to Mitigate Risks to ITS Asset Future Proofing
	• If DOT staff do not need the full functionality of the ITS solution, then portions of it may go unused.	• Adhere to a systems engineering approach and procure functionality through needs definition to avoid equipment purchases that exceed end user needs. **Procurement:** • Coordinate with the systems engineering analysis to include requirements mapped to user needs when procuring or contracting the purchase of ITS systems. **Research and Development:** • Perform usage tracking of individual devices and ITS systems as needed to determine user trends. • Perform market research and gather input on user experiences to determine user preferences. • Consider cost-benefit analysis in R&D efforts, to understand cost requirements versus usage and overall benefits.
Threat Type: Extended Use ***Threat: Exceeding Life Expectancy*** – Attempting to use ITS assets beyond the intended life expectancy.	• If ITS assets are used longer than the design life (life expectancy) then there is an increased risk of system failures without cause. (Individual & Group) • If ITS Assets are used longer than the design life, then there is risks of degraded service. (Individual & Group)	**Systems Engineering:** • Ensure that life expectancies of ITS assets are considered when developing operational concepts and plans for future replacements. **Asset Management:** • Assess lifecycles to develop a better understanding of their realistic life expectancy. • Include a description of the risks associated with operating assets beyond the life expectancy in the asset management planning process and consider this during project specific deployments.
Threat Type: Extended Use ***Threat: Limited Expansion Capacity*** – Use of ITS assets may require expansion and without capacity to expand the usefulness of the asset may be jeopardized.	• If the use of a specific ITS asset requires increasing space (e.g., cabinet space, structure space, right-of-way), power, or connections, and expansion is limited, then the full benefits of the ITS asset may not be	**Systems Engineering:** • Ensure that projected expansion needs are identified and included in requirements. **Asset Management:** • Include assessments of space needed for future asset expansion. **ITS Architecture & Strategic Planning:**

Potential Threats	Risks (written as "if/then" statements)	Deployment/Project Specific Suggested Actions to Mitigate Risks to ITS Asset Future Proofing
	recognized.	• Consider the overall programmatic plan for ITS in order to estimate potential expansion needs for the ITS asset as early in the process as possible.
Threat Type: Extended Use ***Threat: Unavailable Support*** – Hardware or software support to the ITS asset is no longer available, including replacement parts.	• If the asset supplier no longer makes hardware or software available, then maintaining and repairing the ITS asset may become impossible, time consuming, or expensive. (Group)	**Procurement:** • Include procurement considerations to minimize the risks that hardware or software replacements will not be available in the future. **Asset Management:** • Include assessments to predict future unavailability of hardware or software related to ITS assets.
Threat Type: Financial ***Threat: Excessive Cost Increases*** – System maintenance or operation costs are no longer practical.	• If the costs to maintain or operate the solution become high, then the agency may incur higher than planned costs or operations of the system may be discontinued.	**Procurement:** • Request clear declarations of what is covered by the warranty and the warranty period in the procurement process. • Include requests for maintenance and repair rates and/or costs for periods beyond the warranty period and include these in the cost portion of the decision process. • Consider requesting bidders to describe the process for agency performed maintenance of devices beyond the warranty period.
Threat Type: Financial ***Threat: Missed Opportunities*** – System does not allow agency to benefit from lower cost options.	• If the ITS asset relies on proprietary communications, maintenance, or operations, then the agency may incur higher than expected costs to maintain operations and may have to forego upgrades or expansions.	**Professional Capacity Building.** • During project conceptualization, research the technologies being procured to understand any open-source and/or non-proprietary options, and any options for combining individual components (i.e., not relying on one proprietary turnkey system). • Consider various models for ownership of software (e.g., software as a service, source code, data as a service) and select the model most appropriate.
Threat Type: Financial ***Threat: Reduced Funding*** – Agency allocation of funds to the ITS solution is reduced.	• If the agency funds available to system operation and upgrades are reduced, then the system may no longer be feasible to operate.	**ITS Architecture & Strategic Planning:** • Consider programmatic plans for ITS to anticipate potential funding gaps in future years and consider these during development of the asset. **Asset Management / Managing Assets:**

Potential Threats	Risks (written as "if/then" statements)	Deployment/Project Specific Suggested Actions to Mitigate Risks to ITS Asset Future Proofing
		• Lifecycle analysis. Conduct analysis for expected performance based on various funding scenarios to plan for prioritization. **Professional Capacity Building:** • Ensure that Project Managers have resources to research and understand current and planned funding availability (including allowed use of funds) when developing the system.
Threat Type: Policy & Regulatory ***Threat: Allowed Use*** – Licensing, policy, regulations may prevent future use of system components	• If licensing or regulatory rules change, then agency may need to replace equipment, incurring significant costs. • If licensing or regulatory rules change, then agency may discontinue service if replacement is not possible/affordable.	**Systems Engineering:** • During system design, consider the risks associated with any public or private issued licenses (e.g., FCC licenses for communications, private vendor licenses such as Google Maps) and determine if other backup options are available. • When uncertainties are identified, consider the options of "wait and see approach" (delaying deployment) and "cautious approach" (deploying supporting infrastructure that has additional benefits beyond the ITS asset.[14] **Professional Capacity Building:** • Project managers should take action to familiarize with current or pending FCC license activities. • Project managers should take action to familiarize with private vendor licenses for use of software solutions, including experiences and lessons learned of other agencies. ***IT/Security:*** • Support project managers and systems engineering team in understanding current licensing regarding communications related to the ITS asset.
Threat Type: Policy & Regulatory ***Threat: Agency/Department Policy Decisions*** – Threats that may result from changes to agency policies and/or	• If Agency or department policy decisions change, then the future technical and financial support of the ITS solution may be jeopardized.	**ITS Architecture & Strategic Planning:** • Establish a relationship between programmatic ITS plans and agency policy and decision-making to ensure risks are understood and anticipated as much as possible. **Professional Capacity Building:**

Potential Threats	Risks (written as "if/then" statements)	Deployment/Project Specific Suggested Actions to Mitigate Risks to ITS Asset Future Proofing
procedures.		• Project managers should familiarize themselves with possible changes (planned or pending) in agency policies that could impact ITS asset operations or maintenance.
Threat Type: Security ***Threat: Security threats*** – Outdated security may open devices to hackers and intentional attacks.	• If the solution deployed does not maintain adequate security, then the agency may be vulnerable to attacks, impacting not only the devices but other agency systems. • If the solution deployed does not maintain adequate security, then the agency may risk the contact details of users being jeopardized.	**Security / IT:** • Project teams should involve IT and security resources within the agency as early as possible to ensure security risks and IT requirements are included in the systems engineering process. • Security and/or IT should provide input to requirements and specifications during the project procurement/contracting period for security concerns. **Systems Engineering:** • Clearly define the agency needs for security specific to the ITS solution being deployed and include requirements to meet security needs confirmed by the IT/Security group in the agency.
Threat Type: Security ***Threat: Limited Accessibility*** – Security precautions (e.g., firewalls) could prevent use of ITS assets.	• If the functionality and/or use of the ITS asset relies on accessibility that is not allowed by a firewall or other security aspect, then the intended use and benefits of the ITS asset may not be recognized. (Individual & Group)	**Systems Engineering:** • During the user needs assessment, define all user and external system needs for access to data that may require security access and work with security and IT to initiate the process to provide access. **Security/IT:** • Support requirements for data accessibility to outside users of data and information (e.g., firewall access) as appropriate.

6.4 Step 3: Assess Future Proofing

The third step in the suggested approach towards implementing ITS future proofing is to assess the future proofing activities of an agency. Ultimately, the success of future proofing activities will be a reflection of how long ITS assets remain operational, are used, and deliver benefits to the agency's operations, but this can be challenging to measure on a regular basis. Therefore, the premise of the "assess" step is based on three aspects of assessing future proof activities:

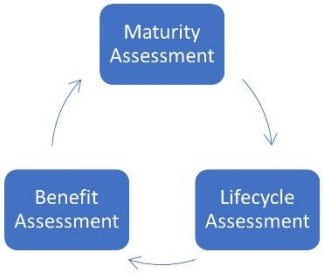
1. ***CMF Assessment.*** A Capability Maturity Framework (CMF) approach is proposed to track progress at implementing the actions proposed in the "Plan" and "Act" phases of this report. This includes seven capability factors and a self-scoring approach for agencies as noted in section 6.4.1. The self-scoring approach outlined in 6.4.1 provides summaries of three levels such that agencies can select the level that most closely matches their current situation. For example, an agency might identify themselves as "Level 1" and set a goal to reach "Level 2" in the coming year.

2. ***Lifecycle Measurement.*** A comprehensive ITS asset lifecycle measurement and recording approach to assess and document at least two areas:

    a. How long ITS assets remained functional and used for their designated purpose(s)?
    b. If the ITS asserts were not used for the anticipated lifecycle, what (threat) caused the failure and/or the ITS asset to stop being used (e.g., was it a procurement issue? An acceptance testing issue? A requirements mistake?).

3. ***ITS Benefit Assessment***. A comprehensive ITS benefit analysis with mid-course corrections that helps each agency understand if the ITS asset use is delivering benefits to operations (agency and travelers) and adjusts the use to better recognize benefits. The benefits are likely to include examples such as safety and mobility. It is recognized that agencies typically include benefit evaluations with ITS deployments, but these may not always be linked to individual assets or consideration of the longevity of asset benefits.

The inter-relations of the three aspects of assessing future proofing are illustrated in Figure 10, by illustrating hypothetical progress along two axes while the maturity of future proofing activities (depicted in the blue box) progresses from Level 1 to Level 3. The development and establishment of a mature framework for future proofing (denoted as a progression from Maturity Level 1 to Level 3) should move the agency to the "desired state" where:



- The operations groups within agencies recognize high benefits of ITS assets; and
- ITS assets have a high ability to remain operational and useful for anticipated lifecycles.

There are risks that the "desired state" will not be reached, and the black boxes illustrate two risk potentials: 1) Limited lifecycles and 2) Limited benefits.

Finally, the yellow arrows and supporting text describe the business case for two actions:

- ITS asset lifecycle measurement, recording, and assessments; and
- Comprehensive evaluation of benefits of ITS systems accompanied by midcourse corrections.

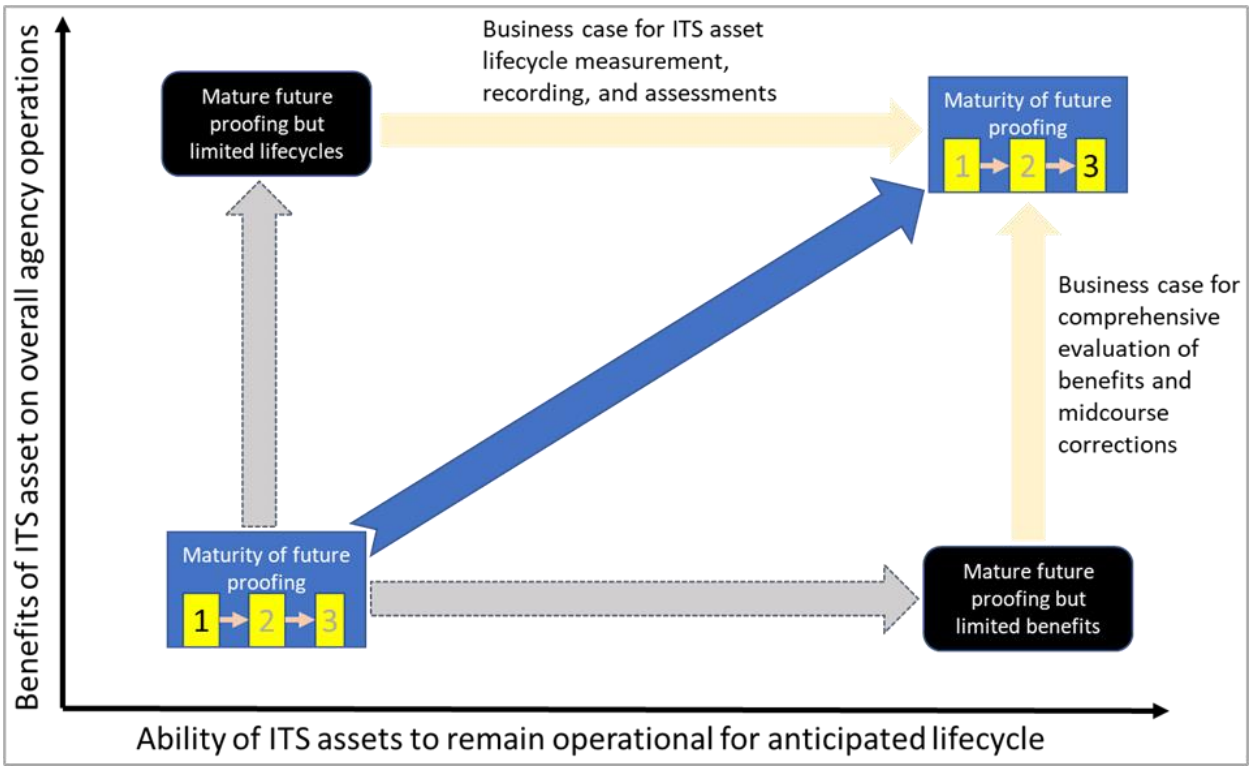


Figure 10: Graphical Representation of Desired Maturity of Future Proofing

6.4.1 CMF Assessment (Maturity of Future Proofing)

The National Academy of Sciences (NAS) report titled "Mainstreaming System Resilience Concepts into Transportation Agencies: A Guide"[15] suggests an approach of assessing capability factors and levels of maturity to monitor and manage system performance. The NAS report defined eight capability factors, with three levels of maturity to help agencies assess their resilience programs.

Building upon the concept of the NAS report, seven capability factors (one for each area/activity recommended to play a role in ITS asset future proofing) have been identified to support agencies in assessing the extent to which they are implementing the recommendations for ITS future proofing in this study. These seven capability factors include:

- **Systems Engineering.** Are systems engineering activities including an emphasis on future proofing actions when assessing user needs, defining requirements, and performing design and testing of ITS systems?

- **Procurement.** Does the procurement process now include consideration of procurement language and contract terms to help mitigate risks to the future of ITS assets procured?
- **IT & Security.** Do ITS Project Managers now work with IT and/or security to minimize ITS asset future proofing risks when planning and implementing ITS assets?
- **ITS Architecture & Strategic Planning.** Are ITS Project Managers using the local ITS Architecture when defining services, data exchanges and standards used to mitigate ITS asset future proofing risks?
- **Asset Management.** Are there activities performed by an Asset Management group within the agency to actively manage the ITS assets to minimize risks to ITS future proofing?
- **Professional Capacity Building (PCB).** Is there an emphasis on professional development in the agency ITS team to prepare them to manage the future of ITS assets?
- **Research and Development (R&D).** Is the agency considering conducting timely research to understand technology and market trends and influencing national research in these areas to better understand the risks and mitigation approaches for future proofing ITS assets?

Table 13 suggests three maturity levels for each factor that agencies might use to assess their progress in implementing the suggested approach to future proofing ITS assets. Agencies may use the descriptions of each level (Level 1, Level 2, Level 3) to understand which level they are currently at. This allows agencies to self-score by assigning the current level, and to understand what is needed to advance to the next level.

Table 13: Suggested Capability Considerations to Assess Implementation of Future Proofing Mitigation Approaches in this Report

Capability Factor	Level 1	Level 2	Level 3
Systems Engineering. Are systems engineering activities including an emphasis on future proofing actions when assessing user needs, defining requirements, and performing design and testing of ITS systems?	Our project teams performing systems engineering are aware of the recommendations for including an emphasis on future proofing ITS assets and are implementing them as appropriate.	We have examples of actions taken during the systems engineering process to future proof ITS assets, but it is not known if all systems engineering analyses are including this aspect.	Our systems engineering guidelines have been updated to include an emphasis on future proofing risk mitigation and it is now institutionalized within our organization.
Procurement. Does the procurement process now include consideration of procurement language and contract terms to help mitigate risks to the future of ITS assets procured?	Our procurement group has been briefed on the need to future proof ITS assets and the role future proofing may play. They have been encouraged to support ITS Project Managers during the procurement process to consider specific actions.	We have examples where our procurement group has considered adjusting standard procurement terms to help mitigate risks to the future proofing of ITS assets, and one or more project managers have collaborated with procurement to include specific provisions to reduce the risks to the future of ITS assets.	Our procurement team believes our procurement and contracting language provides as much future proofing risk mitigation as possible, and future proofing is discussed, and appropriate action taken with each ITS asset procured.
IT & Security. Do ITS Project Managers now work with IT and/or security to minimize ITS asset future proofing risks when planning and implementing ITS assets?	We have briefed both our IT staff and ITS project managers about the suggested actions and collaboration to help reduce future proofing risks to ITS assets.	We have one or more examples where ITS Project Managers have implemented recommendations from IT staff when designing and deploying ITS assets to reduce future proofing risks.	Our ITS Project Managers regularly collaborate with IT and security staff to plan for and maintain secure operations of ITS assets and to ensure needed access to data and servers is maintained.
ITS Architecture & Strategic Planning. Are ITS Project Managers using the local ITS Architecture when defining services, data exchanges and standards used to mitigate ITS asset future proofing risks?	We have an ITS architecture, and ITS Project Managers are familiar with the ITS architecture and the role it plays in reducing risks of incompatible data exchanges and preventing gaps in	ITS Project managers have incorporated input from the ITS architecture when defining data exchanges while deploying ITS assets.	The use of the ITS architecture at key times in the planning, procurement, and deployment of ITS assets is institutionalized throughout our ITS project managers.

Capability Factor	Level 1	Level 2	Level 3
	services.		
Asset Management. Are there activities performed by an Asset Management group within the agency to actively manage the ITS assets to minimize risks to ITS future proofing?	Our Asset Management program includes our ITS assets, and as new ITS assets are deployed, they are added to the Asset Management tracking system.	We have implemented changes to our Asset Management program to actively manage the lifecycle and condition of ITS assets and expansion needs for ITS assets. At least one ITS project has been deployed and the risks of future proofing are being minimized through the role of our Asset Management.	Our ITS assets are uniformly included, tracked, and managed through our Asset Management process, and steps have been added (as appropriate) to help reduce the future proof risks to ITS assets.
Professional Capacity Building (PCB). Is there an emphasis on professional development in the agency ITS team to prepare them to manage the future of ITS assets?	Our internal PCB activities have been briefed on the role PCB can play to minimize risks to future proofing ITS, and we are considering additional training and education resources to support ITS subject matter experts (either internally or through outside associations like ITS state chapters).	Our PCB activities have initiated 1-3 changes to better prepare ITS subject matter experts to understand technology and industry trends to help minimize risks to the future proofing of ITS assets.	Our PCB activities are recognized as playing a critical role in preparing ITS subject matter experts to understand industry and technology trends impacting the future of ITS assets.
Research and Development (R&D). Is the agency considering conducting timely research to understand technology and market trends and influencing national research in these areas to better understand the risks and mitigation approaches for future proofing ITS assets?	Our agency has included the need for research to address technology and market trends in our agency research program, and we are attempting to influence national research in this manner.	Our agency has taken steps to shorten the timeframe from research need identification until completion, at least for technology and market trend research, and at least one research initiative in this area is underway.	Technology and market trends are now a core aspect of our research program, and a process is in place for timely research and information sharing to ITS subject matter experts involved in our agency's activities.

6.4.2 Lifecycle Measurement

The second aspect of assessing future proofing is the suggestion to track the useful lifecycles of ITS assets, either as part of a formal asset management process or through budgeted project management activities. This section describes the importance of lifecycle measurement and offers suggestions for agencies to consider when measuring the lifecycles of ITS assets.

The importance of ITS asset lifecycle measurement

Three reasons why lifecycle measurement is important include:

To understand how long ITS assets will remain in operation and useful to the agency. When agencies replace ITS assets, the emphasis is often on defining, procuring, and deploying the new replacement asset. Therefore, agencies may not take the time to reflect on the date the asset was deployed and the duration it was used. Recording the duration of use of various ITS asset types and various locations/conditions of deployment can help agencies understand typical lifecycles. In the past 30+ years, the types of equipment deployed as part of ITS systems has changed and will continue to change. For example, wireless communications imbedded in field devices were almost unheard of in 1990. In the initial years of use of wireless communications, there was much uncertainty about the lifecycle of the devices. As these are now commonplace, agencies should have examples of actual lifecycles for their assets or may have access to resources to provide estimates of lifecycles. Given examples like this of new technologies and innovative ways to use technologies, it is important to continuously monitor and update estimates for device lifecycles.

Agencies often use manufacturer guidance and warranty length as ways to understand expected lifecycles. This can provide a baseline to compare their experience against.

To understand if the typical lifecycle of agency ITS assets is increasing or decreasing. The ultimate goal is to achieve benefits from the ITS assets, regardless of the length of the lifecycle. Nonetheless, tracking trends in the typical lifecycles of assets (i.e., are the lifecycles increasing or decreasing) is a valuable activity, and can help with planning future ITS asset replacement cycles and budgeting for system or component replacements. Introducing minimal actions to record the dates the assets were deployed and removed from service will provide a critical metric to understanding if lifecycle times are increasing or decreasing and helping to understand the benefits of the ITS assets.

To be able to reflect on contributing factors to the actual lifecycles of ITS assets. Finally, recording the lifecycle of ITS assets can help to document why the use of an ITS asset ended when it did. As noted earlier in the report, there are multiple reasons why the lifecycle of an ITS asset may be cut short, these are introduced as "threats" to the ITS assets. Some of these are outside the control of the agency, and some could not have been predicted. But clarifying why an asset is no longer used and identifying one or more threats that resulted in the end of use of the asset can provide a qualitative understanding of factors that contributed to the end use of the asset. This in turn, can allow the agency to update their list of threats to ITS assets, therefore improving their overall ITS future proofing program.

Suggestions for Lifecycle measurement

As agencies consider implementing new (or adjusting existing) measures to track ITS asset lifecycles, the following are suggestions based on the findings of this synthesis:

Track ITS assets as they were procured. The term "ITS assets" as used in this report can refer to a range of assets, including:

- Individual components, such as a cellular modem that is part of a larger device or system;
- Individual devices, such as dynamic message signs, cameras or detectors;
- Groups of devices, such as a set of dynamic message signs from the same vendor or a set of non-intrusive detectors;
- Large systems, such as an ATMS or ATIS, that includes many components and software and hardware systems.

To only track the highest-level system (or system of systems) might ignore some of the individual ITS assets that suffered shorter lifecycles than expected, especially since some of the threats to ITS assets involve interoperability with other systems. However, tracking every single component or device could be burdensome. Therefore, one recommendation is to track ITS assets as they were procured. For example, if cameras were procured to be part of an ATMS, track the lifecycle of each camera. If a traffic detection system was procured that includes field equipment, communications, and data processing/display together in one procurement, track the overall system (versus the individual components).

Consider component tracking when appropriate as part of an overall asset management system. Sometimes the failure of one component of a device (e.g., a logic board as part of a dynamic message sign) can cause the need for replacement, or by replacing one component the overall lifecycle of the device can be extended. Documenting the replacement (or lack of replacement) of individual components as part of an overall asset management system can be useful with some devices and systems.

Record key data about the deployment and use of the ITS asset

When tracking the lifecycle of ITS assets, several dates are suggested for recording:

- Planning Date: The date the ITS asset was determined to be needed. For example, this could be the date that the systems engineering analysis was performed. This date is important because the knowledge and industry trends at the time the ITS asset was decided represents the best understanding of industry state of practice.
- Procurement Date: The date that the ITS asset procurement letting occurred. This date will help understand typical pricing and product availability at the time the procurement process began.
- Deployment Date: The date the ITS asset was deployed and began use. This will be important to understand the influence of any natural threats and ultimately time in operation.

- Change Date: The date the ITS asset was changed (e.g., upgraded, repaired, altered) and the description of the change. ITS assets may have multiple change dates.
- End Date: The date the ITS asset was no longer considered a useful device or system, regardless of whether it is physically removed at this date.
- Initial warranty period: This would be the warranty offered by the vendor for the device or system. This will help compare the warranty period against the ultimate time from purchase to End Date.

Identify factors that lead the agency to evolve or eliminate the device and relate these to threats

When an ITS asset reaches the end of its lifecycle, it may result in a replacement of the same asset (e.g., replacing a device that is no longer operational to the same or newer model), it may be an upgrade to a new device/asset, or may be sunsetting a device and/or system that is no longer needed due to changes in agency needs or changes in user (e.g., traveling public) needs or preferences. It is important to determine and capture the factors that have led to sunsetting the use of the ITS asset. More specifically, it will be most useful if one or more threats can be identified as the reason behind the sunsetting of the ITS asset.

The ENTERPRISE report titled "Evolving and Phasing Out Legacy ITS Devices and Systems"[8] is a resource to help agencies determine when to evolve to a new system or phase out an existing system. The report provides case studies documenting decision factors, criteria, approaches, and tools agencies use to guide decision-making when considering how and when to evolve or phase out ITS devices and systems. The findings resulted in a set of criteria and applicable tools for ten common ITS devices and systems which can be used to assist agencies as they assess ITS devices and systems to determine evolutions or eliminations. Per findings from this research, common decision factors used when determining how and when to evolve or eliminate an ITS device or system include:

- Operational need/benefit
- Performance (e.g., accuracy, efficiency, up-time, safety improvements)
- Cost (e.g., cost comparisons among alternatives, costs versus benefits)
- Actual usage of a device or system
- Feedback from users (e.g., motorists or agency users)
- Resources required for maintenance
- Aging or antiquated devices/systems
- Availability of alternative(s)

Whenever possible track quantitative data about the asset use

At least three of the threat types include threats that could be better understood if quantitative data were available about the ITS asset use and influences. These include the following:

- Threat type – Financial: Threats such as 'excessive cost increases,' and 'funding availability' all relate to quantitative dollar amounts. If actual values are tracked (e.g., if maintenance of the ITS asset costs increase, track the amount of the maintenance; if less funding is available, track the

degree to which the funding was reduced), this will help understand the extent that one or more threats influenced the early end to the lifecycle of the ITS asset.

- Threat type – Functional Performance: Threats in this threat type include actual use of the ITS asset. For example, if a DMS is used infrequently, it may be removed or moved to another location. This would result in a shorter lifecycle because use was infrequent. If the systems have the capability to track the number of messages posted to the sign, frequency of messages, or other uses, these data may be helpful in assessing the threats and the extent to which the threats played a role in discontinuing the use. An example where DMS locations are prioritized is the Iowa DOT DMS inventory scoring matrix.[16] Iowa DOT uses this matrix as a method for identifying priorities for existing and proposed DMS sites. Criteria for assessing the priority of DMS include: DMS location type, traffic volumes, crash history, existing DMS usage, and Iowa DOT TMC staff value/input. More details on this can be found at the Iowa DOT Intelligent Transportation Systems (ITS) and Communications Systems Service Layer Plan.
- Threat type – Security: Threats specific to the security threat type may benefit if security vulnerabilities, attacks, or data exposures could be tracked.

Be sure to track human aspects when documenting factors

As noted in the earlier sections of this synthesis, future proof refers to the ITS asset continuing to provide value to the agency. While many of the threats and reasons for terminating use of an asset are functional, there are aspects of usability, usefulness, and overall use that are considered when deciding an asset is no longer providing value. Often the end user feedback (either agency staff using the device or travelers interacting with the device) is captured informally or formally. Retaining these types of feedback will be helpful to understand the impacts of threats on the lifecycle of the ITS asset.

Best Practice: Lifecycle and Cost Estimation

The following best practices were identified and documented as part of the 2020 ENTERPRISE project report entitled The Evolution of ITS in Transportation Asset Management.[17]

- As a result of limited guidance, the ENTERPRISE member agencies have developed their own strategies for estimating lifespans. Lifecycle estimates are based on staff experience, information and support from consultants and vendors. Agency practices include Michigan DOT is developing an ITS device replacement plan based on an industry scan that includes industry recommendations, as well as best practices from other agencies to generate lifecycle estimates.
- Pennsylvania DOT has used their Traffic Signal Asset Management System (TSAMS) to track lifecycle information for their ITS devices since 2018. Because this practice is still relatively new, limited lifecycle information is currently available. However, over time TSAMS will have increasingly sufficient data to generate valuable lifecycle information.
- Ontario MTO retains manufacturer information on device lifespans in cost sheets and historical maintenance data to predict how long ITS assets will last. The latest value bid price for each ITS device is also tracked. Lifecycle estimates are largely based on staff expertise and experience.

- Wisconsin DOT uses work orders and a field tracking device mechanism to track each device type. This management database tracks maintenance costs, and a separate system tracks utility costs, which are the main operations cost except for solar devices. A thorough check was conducted to estimate lifecycle costs in 2009, and new collected data is being used to validate those numbers; however, these are not used in practice given reliance on engineering judgement.
- Wisconsin DOT has also leveraged some FHWA sources as a starting point about the overall cost of ownership for ITS that staff update annually. Additionally, Wisconsin DOT has engaged with other practitioners at conferences and information exchanges, such as the Upper Midwest Conference held every 18 months to understand the ITS asset management practices, issues, challenges, and solutions used in other states.

6.4.3 ITS Benefit Assessment

The third aspect of assessing future proofing of ITS assets is to assess if desirable benefits are being achieved by the operation of the ITS asset. In other words, if we are extending the useful lifecycle of the ITS asset, are we receiving benefits from the use of the asset?

The concept of assessing the benefits of ITS systems and services is not new. There is considerable documentation surrounding three general ways that ITS benefits are assessed:

- ***Socio-economic Benefits.*** These include those benefits that are typically quantified and represent benefits to society as a whole. Reductions in emissions, reductions in delays to drivers, reduced crashes are all examples where the benefits can be quantified. While these benefits are quantified, they don't necessarily represent actual costs savings.

- ***Cost Saving Benefits.*** These represent actual cost savings to the agency or traveler. Examples might include situations where ITS assets support more efficient operations and the number of operators can be reduced or the number of on-sight inspections can be reduced.

- ***Qualitative Benefits.*** These include those benefits that are not typically quantified but are recognized. Improved quality of a trip and reduced stress to drivers by being informed of an incident are examples. Improved sense of safety is another example.

Since there are considerable resources describing ITS benefit assessment, this section will not include a deep dive into ITS benefit assessment, rather it will focus on the unique aspects of benefit assessment related to future proofing ITS.

Unique aspects of ITS Benefit Assessment related to future proofing

It is common for agencies to evaluate a novel use of technology or an innovative device or system. Often these are done as part of an operational test or a model deployment. However, once the benefits are assessed and proven to be significant to merit additional deployments, there is less emphasis on ongoing evaluations. Essentially, the use of ITS (and supporting assets) becomes mainstreamed and accepted as a tool. The reduction in evaluation activities is partially because evaluations of benefits can

be expensive and time consuming, and partially because evaluations can be disruptive to ongoing operations. With regard to ITS asset future proofing, the real question is if the ongoing use of the asset is bringing value. A few suggestions for consideration with regard to assessing benefits of ITS asset use are described below.

1. **Consider ongoing, long-term assessments of impacts.**
   Agencies may consider assessing whether the ITS asset is bringing value using alternative approaches to formal evaluations, such as monitoring use of the asset by agency staff or travelers and any observed impacts. For example, if you consider a CCTV camera that is connected to the TMC and available for operators to view, there is a cost to operating each individual camera, and it is very challenging to quantify the benefits of each individual camera to be part of a quantified benefit/cost comparison. However, to the TMC operators, they likely rely on that camera as part of their overall assessment of the network.

2. **Consider the value of agency staff feedback regarding their use of the ITS asset.**
   Considering the "qualitative" types of benefits, often the role the ITS asset plays to a larger activity can serve as a surrogate for understanding the benefits of the asset. Simple questions such as "would your activities suffer if this asset was not there?" will quickly help to understand how critical a device is. Using the CCTV camera example above, brief discussions with operations staff will quickly help to understand the role and value that various cameras offer.

   Additionally, anecdotal feedback can be a great measure for capturing when ITS assets are used infrequently but very much needed during critical situations. As an example, technology to detect and warn over-height vehicles as they approach a height restriction will need to function 24/7, but the number of activations may be very small (i.e., only when an over-height vehicle approaches). While the number of activations may be small, the safety impacts and financial benefits of avoiding the vehicle to infrastructure collision are tremendous and may be better represented by information describing what vehicles activated the warning and the potential damages prevented. As another example, referring to the CCTV camera description above, some cameras may only be viewed when crashes or inclement weather conditions extend to the area near the camera. Quantitative numbers of the times operators view the cameras might not appear high, but feedback from the operators can help to explain just how critical they are when they are needed.

3. **Document and consider the role the ITS asset plays in the overall operations program of the agency.**
   Many ITS assets may not be widely visible to operators or managers. Devices may perform roles of communicating data, securing networks, performing backups. If these devices are included in asset management plans and tracked as part of asset management systems, their roles should be documented and updated when appropriate. These updates to the roles of ITS assets should include adding new roles or deleting roles that are no longer appropriate.

7.0 Applying the Model Future Proofing Process to Communications

Agencies use a variety of communications mechanisms to connect and transmit data to and from ITS devices. In some cases, multiple communications mechanisms may be implemented for critical systems for redundancy, however for other systems or groups of devices agencies generally implement only a single communications mechanism. This can carry major implications for selection and configuration of devices and costs, particularly for future decisions to change the communication mechanisms. This section details various future proofing considerations for agencies both when selecting a primary communications mechanism for ITS devices and after implementation.

DOT Activities When Selecting a Communications Mechanism

- *Identify Likely Threats and Risks to Select the Best Alternative.* The communications approach selected can help to mitigate the risks of future proofing to the ITS asset. The first step for an agency is to examine what possible threats and risks exist for possible alternatives, which may be conducted as part of a systems engineering process. The agency can then examine the likelihood of each threat and risk versus any increased cost to mitigate the threat and risk (e.g., increased security) to select the best alternative.

- *Mitigate Identified Threats in Design and Procurement.* Considerations for identified threats may be translated into specifications during procurement when determining how to implement the communications service, for example.

Table 14: Example Considerations and Actions to Consider When Deploying Communications

Potential Threats	Considerations and Possible Actions
Wear and Tear	***Considerations:*** • Any communication approach that involves devices in the field exposed to the elements has potential risks associated with wear and tear. ***Actions to consider:*** • *Systems Engineering.* Describe the location and ranges of ambient conditions in the requirements, while defining requirements for any equipment to resist corrosion or failure as a result of the conditions.
Weather Events	***Considerations:*** • Severe weather events may cause outages or disrupt commercial communications services (e.g., cellular communications) or may cause dedicated communications infrastructure (e.g., wirelines or supporting poles) to fall. Agencies may consider implementing redundant communications mechanisms for safety-critical systems or devices and examining the availability of dedicated communications channels for emergency management. ***Actions to consider:*** • *Systems Engineering.* During the needs identification, discuss the impacts of temporary periods of no communications and determine if redundancy of communications approaches is needed to support this location. If so, include

Potential Threats	Considerations and Possible Actions
	requirements for redundancy. • *Systems Engineering.* Include requirements for housing and protection of field devices used to support communications.
Vandalism	***Considerations:*** • Field equipment to support communications are often located in isolated areas and can be at risk to vandalism. ***Actions to consider:*** • *Systems Engineering*. Consider the risks of vandalism when defining requirements for the mounting and support equipment, as well as consideration of protection devices for the field equipment.
Event Exposure	***Considerations:*** • Devices located in the clear zone or protected by guardrails are typically protected from exposure to vehicles. ***Actions to consider:*** • *Systems Engineering.* Include agency requirements for crashworthiness of any towers or structures used to house the communications equipment.
Incompatibility	***Considerations:*** • If the communications are intended to perform data exchanges between agency owned devices (e.g., agency operated TMC communicating to agency owned DMS in the field) then the agency has more control over compatibility. • If the communications involve agency systems communicating with one or more external systems (e.g., broadcasts data to connected vehicles, communications to 3rd party data providers) then the agency is at increased risk of incompatibility, as the outside party may change standards versions or change communications protocols. • Both internal and external communications may encounter compatibility issues with established IT procedures and systems or may conflict with security measures. ***Actions to consider:*** • *Systems Engineering.* If establishing communications between two established (agency owned) systems, examine the warranty and expected life of current versions of both systems and include needs/requirements in the systems engineering process to be upwardly compatible to future upgrades beyond the existing versions. If establishing communications to external systems, include a review of the external system during the systems engineering process to anticipate any updates to communications standards or data formats, with the intention of capturing these changes as requirements for the communications implemented. • *ITS Architecture & Strategic Planning.* Ensure that the communications functions being added are included in the statewide architecture. Review the data exchanges and standards being considered by the communications deployment for compatibility with the architecture. Review the latest available ITS strategic planning documents to understand current and planned ITS deployments that might rely on this communications and assess compatibility needs.

Potential Threats	Considerations and Possible Actions
	• *IT/Security*. Ensure that IT/security groups are included in project discussions during the procurement and contracting period for input about IT compatibility of the communications and any security challenges that may exist.
Outdated or Ineffective	***Considerations:*** • The systems deployed to perform the communications could become outdated if new communications exceed performance (e.g., faster communications, larger bandwidth, wider coverage). It is important to understand trends and current state of the practice to mitigate risks that the selected approach will become outdated during the design life. ***Actions to consider:*** • *Asset Management.* Include the communications solutions in annual assessments of emerging technologies to identify competing communications approaches. • *Professional Capacity Building.* Conduct internal communications to other staff to understand any trends others have observed regarding emerging technologies for communications or anticipated industry changes. • *Systems Engineering.* During the needs assessment, document the needed communications speed, bandwidth, range, and other parameters. If new communications are introduced, include a mechanism to examine if there is a need to improve these parameters, as part of any upgrade consideration. • *ITS Architecture & Strategic Planning.* Review ITS strategic plans for future communications that might replace or make this communications outdated. Also, review ITS programmatic planning documents and the ITS Architecture to understand ITS systems and services that might require upgraded communications.
Unused	***Considerations:*** • There is potential that communications could function properly but not be used. For example, a 5.9 GHz roadside unit communicating data with no receivers receiving it could be considered "not used." • There is potential for some of the features/functions to not be used. For example, extremely high bandwidth or geographic range for wireless communications may not be needed, go largely unused, and therefore be considered unused. ***Actions to consider:*** • *Systems Engineering.* Include a strict needs assessment of current and planned users and uses of the communications to avoid communications that exceed needs and to avoid communicating to users that are not yet ready to receive data. • *Procurement.* Leverage systems engineering documents to focus procurement language and decision-making on specifically what the communications needs are, avoiding prioritizing bidders with excess/un-needed communications capacity.
Exceeding Life Expectancy	***Considerations:*** • If systems are in-place and functioning, there is a tendency to continue to

Potential Threats	Considerations and Possible Actions
	operate them, even if they exceed the life expectancy. This can pose problems if failures occur and there is urgency to replace equipment with the risk that equipment may not be available, or the vendor may not exist. ***Actions to consider:*** • *Asset Management.* Request a briefing from the Asset Management group on the risks of continuing to operate the system beyond life expectancy. • *Systems Engineering.* Define roles/responsibilities in the ConOps to include a review of the vendor and product at the close of the warranty period to document availability of equipment replacement (e.g., parts, components).
Limited Expansion Capacity	***Considerations:*** • If physical equipment is deployed to support communications, then it may require increased space to support updates or upgrades. • The coverage area (geographic distance or number of devices communicating with) could expand, as could the need for increased bandwidth or speed. ***Actions to consider:*** • *Systems Engineering.* During the needs assessment, consider the potential for expanded communications needs and ensure additional physical space requirements are included in requirements or if procuring communications services, ensure that potential additional capacity is included in requirements for procurements that can allow for it. • *Procurement.* Ensure that capacity increases are considered and negotiated (if required) during the procurement process. • *Asset Management.* Include input from the Asset Management group on additional capacity needs for expanded communications.
Unavailable Support	***Considerations:*** • If a vendor no longer exists or no longer supports a product, technical support and/or replacement parts could provide risks to communications. ***Actions to consider:*** • *Asset Management.* Request an assessment of the risks of either communications services or support for purchased devices not being available. Identify the feasibility of alternatives, including potentially working with the vendor to identify alternatives. • *Procurement.* Encourage procurement considerations to consider the likelihood that the vendor and/or services provided will be available in the future.
Excessive Cost Increases	***Considerations:*** • Once communications are established, it if preferable not to change communications approaches, but excessive cost increases may create situations where an agency can no longer support the costs. ***Actions to consider:*** • *Procurement.* Before completing procurement, request clear declarations of what is covered during the period of the contract and what options the agency has for increasing communications and the mechanisms to control and avoid excessive cost increases. Consider how costs are allocated in order to select

Potential Threats	Considerations and Possible Actions
	the best alternative given how the communications mechanism will be implemented and the potential for increased use over time (e.g., per device versus actual data usage). • *Systems Engineering.* Examine past trends to estimate the potential long-term cost implications for communications mechanisms.
Missed opportunities	***Considerations:*** • Communications options and related costs are continuously changing, and agencies should strive to avoid being locked into contracts that do not allow renegotiating at reasonable periods. • Similarly, agency needs for communications may change. As an example, an agency may discontinue a phone service and no longer need dedicated phone lines. If these are contracted for a firm period of time the agency could lose on the opportunity of cost savings. ***Actions to consider:*** • *Systems Engineering.* Consider a phased implementation prior to a full transition to minimize costs to upgrade deployed devices and/or provide an opportunity to procure devices that are compatible with both existing and new mechanisms. • *Systems Engineering.* Ensure that requirements and design do not unnecessarily favor any proprietary solution that prevents the agency from benefiting from lower costs to maintain or operate the solution. • *Procurement.* Involve procurement early in the process to explore options for phased implementation or contracts with renegotiating clauses.
Reduced Funding	***Considerations:*** • While there may be funds for initial deployment, ongoing operations may compete for funds and the ability to adequately fund communications may be lost. ***Actions to consider:*** • *Systems Engineering.* Use ConOps scenarios to consider the impacts on the systems that rely on the communications in the event that the communications funding is partially or completely removed in the future. Share these risks during the "go/no-go" decision period following the ConOps and requirements development. • *Asset Management.* Conduct analysis of different funding scenarios and their impacts on performance and lifecycle. • *ITS Architecture & Strategic Planning.* Review programmatic planning documents to predict potential funding issues that may impact operations of technology systems.
Allowed Use	***Considerations:*** • Changes to licensing or regulatory rules might require discontinued use and replacement of the communications mechanism. ***Actions to consider:*** • *Professional Capacity Building.* Project managers of communications deployments that utilize any portion of the spectrum should conduct a review and familiarize themselves with any changes being considered for spectrum

Potential Threats	Considerations and Possible Actions
	use. • *Systems Engineering.* During the ConOps, include assessment of reliance on communications licenses as part of the risk assessment. Consider "wait and see" approaches if risks are identified. • *IT/Security.* Support the systems engineering team and project manager in understanding licensing and regulations around communications being considered.
Agency/Department Policy Decisions	***Considerations:*** • The procurement of communications services may involve procuring minimum communications services for a period of time (e.g., cellular service minimum charges for a 12-month period, for example). Agency changes may affect the need for these services. ***Actions to consider:*** • *Procurement.* Consider possible changes to agency or department policy decisions and include any provisions in the contract to protect these changes.
Security Threats	***Considerations:*** • Depending upon the approach, deployment of communications can introduce any number of vulnerabilities to the agency. ***Actions to consider:*** • *Systems Engineering.* Make sure requirements and design consider security of the communications mechanism itself and supporting connections to agency devices. • *Systems Engineering.* Involve the IT/security groups as early as possible in the systems engineering process to capture their input and benefit from established and documented requirements for security. • *Security/IT.* Provide input to both the systems engineering process and the eventual design and implementation.
Limited Accessibility	***Considerations:*** • Depending upon the ITS systems that the communications supports, there may be requirements for accessibility by systems or individuals inside or outside the agency firewall. Without proper considerations, the communications approach could prevent needed access and create situations where the communications is not future proof. ***Actions to consider:*** • *Systems Engineering.* Make sure requirements and design consider how the communications mechanism will connect with agency devices and verify compatibility of the communications firewall and other security aspects to ensure accessibility for functionality and use of agency devices and users (or user systems) outside the agency. • *IT/Security.* Provide input to the systems engineering process to ensure the security not only protects the agency from vulnerabilities but also does not prevent communications to partners who need access.

DOT Activities After Implementation

After the communications mechanism is deployed, agencies should periodically re-examine the use and costs of all communications mechanisms. Agencies may ultimately decide to, or be forced to, phase out older communications mechanisms in favor of an alternative that is cheaper, more secure, more reliable, and/or faster. Transitioning to a new communications mechanism will have implications on the devices that use it. Future proofing activities may include:

- *Asset Management*. This may include documentation of devices that use each communications mechanism, as well as device compatibility for using other communications mechanisms, if needed.
- *Professional Capacity Building*. This may involve training to ensure agency staff understand best practices for updating systems to maintain device reliability and security. Additionally, agency staff should keep abreast of new threats via various communications mechanisms in order to make updates and be informed about making decisions for potentially implementing a new communications mechanism and thus procuring compatible devices.
- *IT & Security*. Agency staff should keep abreast of new threats, vulnerabilities, or potential obsolescence of various communications mechanisms in order to make updates or weigh the need for additional or different communications mechanisms for some or all devices and systems being used by the agency.

8.0 Applying the Model Future Proofing Process to Detection

Agencies use a variety of ITS devices and services for the purposes of detection. In most cases, multiple generations or types of detection technologies are implemented across an agency's jurisdiction and sometimes provide redundancy with one another. New and updated detection technologies are frequently becoming available and subject to new fads. ITS devices such as CCTV and loop detection have long been used as reliable detection devices, but recent years have seen a variety of new technologies (e.g., Bluetooth and RFID tag readers) and probe data services, (e.g., INRIX and Here), which often claim to provide improvements over the existing technologies that an agency operates. However, transitioning to new technologies and services for detection can carry additional risks. A tradeoff in procuring probe data services is that by contracting out detection, an agency reduces the risks of procuring and maintaining ITS detection devices; however, this decision also reflects a choice between how much control the agency desires in obtaining information versus how much effort it is to operate the devices. This section details various future proofing considerations for agencies selecting ITS devices or services for detection and after implementation.

DOT Activities When Selecting Detection Devices or Services

- *Identify Likely Threats and Risks to Select the Best Alternative.* The selected detection device or service can help to mitigate the risks of future proofing to the ITS asset. The first step for an agency is to examine what possible threats and risks exist for possible alternatives, which may be conducted as part of a systems engineering process. An example of a risk with any deployed ITS device is that it will be damaged due to wear and tear, corrosion caused by winter materials, or pavement maintenance. Additionally, emerging technologies or newly introduced devices will have limited deployment experience for an agency to make an informed decision about reliability and durability over time. In contrast, contracted services procuring data delivery (e.g., detection using probe data) may help avoid some or all of the issues encountered by placing equipment in the field. Nonetheless, contracted services for detection data may carry other risks regarding the reliability and availability of the data (particularly for lower-volume roadways), data processing transparency, and the long-term costs and availability of the service itself. The agency can then examine the likelihood of each threat and risk versus any increased cost to mitigate the threat and risk (e.g., increased security) to select the best alternative.

- *Mitigate Identified Threats in Design and Procurement.* Considerations for identified threats may be translated into specifications during procurement when determining how to implement and maintain devices or contract a long-term detection service, for example.

Table 15: Example Considerations and Actions to Consider When Deploying Detection Assets

Potential Threats	Considerations and Possible Actions
Wear and Tear	***Considerations:*** • Any detection approach that involves devices in the field exposed to the elements has potential risks associated with wear and tear, particularly in-pavement detection devices given corrosion due to winter materials or

Potential Threats	Considerations and Possible Actions
	repaving projects. ***Actions to consider:*** • *Systems Engineering. W*hile defining requirements for detection devices, be sure to describe the ranges of ambient conditions as well as anticipated exposure to roadway chemical treatments and activities that might threaten intrusive or non-intrusive detection devices. • *Systems Engineering.* As part of the needs assessment, examine pavement program plans to understand whether any near-term projects are scheduled that would affect the detection devices. If detected, include these as external influences to be addressed in the design and deployment.
Weather Events	***Considerations:*** • Severe weather events may cause outages, disrupt probe data services, or disrupt connections to detection devices in the field. Agencies may consider implementing redundant detection for safety-critical systems or devices or have fail-safe backup plans in place. ***Actions to consider:*** • *Systems Engineering.* During the needs identification, discuss the impacts of temporary periods without detection and determine if redundancy is needed to support this location. If so, include requirements for redundancy. • *Systems Engineering.* Include hardening requirements (based on local ambient extreme conditions) for housing and protection of field devices used to support detection.
Vandalism	***Considerations:*** • Field equipment to support detection, such as cameras supporting non-intrusive detection, may be in isolated areas and can be at risk to vandalism. In-pavement detection is likely to incur less risk, but still encounters the risks to the above-ground devices that connect to the detectors. Probe data detection solutions incur lower risks of vandalism. ***Actions to consider:*** • *Systems Engineering*. Consider the risks of vandalism when defining requirements for any mounting and support equipment, as well as consideration of protection devices for the field equipment. • *Asset Management*. Ensure spare parts or components are available, if needed.
Event Exposure	***Considerations:*** • Devices located in the clear zone or protected by guardrails are typically protected from exposure to vehicles. Other forms of detection, such as in-pavement detection or probe data services would incur lower risks for this threat. ***Actions to consider:*** • *Systems Engineering.* Include agency requirements for crashworthiness of any towers or structures used to house the communications equipment.
Incompatibility	***Considerations:*** • If detection devices or services are new or from a different provider or vendor than is currently used by the agency, the data format may not be compatible

Potential Threats	Considerations and Possible Actions
	with the data provided by other existing detection devices or services. Similarly, transitioning to new devices or services that use a different data format may disrupt continuity for developing performance measures and historic trends. ***Actions to consider:*** • *Systems Engineering.* Compare the warranty and expected life of any new device with existing systems. Include needs/requirements in the systems engineering process for the provided data format, such as a stable data standard that is compatible with existing systems. Examine the flexibility of the provided data format for future updates during the systems engineering process to anticipate any updates to agency data formats or standards, with the intention of capturing these changes as requirements for the detection implemented. • *ITS Architecture & Strategic Planning.* Ensure that the detection devices or services being added are included in the statewide architecture. Review the data exchanges and standards being considered by the deployment for compatibility with the architecture. Review the latest available ITS strategic planning documents to understand current and planned ITS deployments that might benefit from detection (e.g., incident detection, traffic monitoring) and assess compatibility needs. • *IT/Security*. Ensure that IT/security groups are included in project discussions during the procurement and contracting period for input about IT compatibility of the detection device or service and any security challenges that may exist. • *Performance Measurement*. To the extent possible, develop performance measures and historic trends that are compatible with historic data and can be easily updated even when detection is added or removed, or with modifications to the provided data format.
Outdated or Ineffective	***Considerations:*** • The devices or services deployed to perform detection may become outdated if new emerging technologies become available that exceed the performance of earlier devices (e.g., longer lifecycle, better coverage area, more accurate data). It is important to understand trends and current state of the practice to mitigate risks that the selected approach will become outdated during the design life, while still remaining open to new innovations and benefitting from them as soon as possible. ***Actions to consider:*** • *Asset Management.* Include detection solutions in periodic assessments of emerging technologies to identify emerging approaches that may be more robust and effective for meeting agency needs. • *Professional Capacity Building.* Conduct internal communications to other staff to understand any trends others have observed regarding emerging technologies for detection or anticipated industry changes. • *Systems Engineering.* During the needs assessment, document the needed accuracy, reliability, and other parameters. If new detection devices or services are introduced, include a mechanism to compare the needs identified with the new industry advances to understand if it is prudent to upgrade to new

Potential Threats	Considerations and Possible Actions
	systems (e.g., if needs are sufficiently met by current systems is there a need to upgrade). • *Procurement.* Include provisions in the procurement process to weigh the extent that proposed solutions are proven technologies that address the stated needs in order to avoid devices or services that are a "fad" and may exceed agency needs (at a higher cost) or not meet agency needs for detection in the long-term. • *ITS Architecture & Strategic Planning.* Review ITS strategic plans for future planned systems that might require additional detection capabilities and include these in the documentation of user needs. Also, review ITS programmatic planning documents and the ITS Architecture to understand ITS systems and services that might include additional requirements for detection.
Unused	***Considerations:*** • There is potential that detection devices could function properly but not be used. For example, installing detection devices (or procuring a data service) to cover locations where data is not used regularly has a high likelihood of lack of use. • There is also potential for limited but critical use of detection devices. For example, existing detection in the field may not be needed for most functions if a probe data detection service is procured; in this case, the detection in the field may only be used for calibration purposes and may still be valuable. ***Actions to consider:*** • *Systems Engineering.* Include a strict needs assessment of current and planned users and uses of detection to avoid extra field installations (or procurement of probe data services beyond needed areas) that exceed needs. • *Procurement.* Leverage systems engineering documents to focus procurement language and decision-making on specifically what the detection needs are. Require integration of existing devices with any new probe data service for calibration purposes and compatibility with any new system.
Exceeding Life Expectancy	***Considerations:*** • If detection devices are in-place and functioning, there is a tendency to continue to operate them, even if they exceed the life expectancy. This can pose problems if there is degraded data quality, increased maintenance requirements, or failures occur and there is urgency to replace equipment with the risk that equipment may not be available or the vendor may not exist. ***Actions to consider:*** • *Asset Management.* Request a briefing from the Asset Management group on the risks and potential options for risk mitigation if continuing to operate the detection devices beyond life expectancy. • *Systems Engineering.* Define roles/responsibilities in the ConOps to include a review of the vendor and detection product at the close of the warranty period to document availability of equipment replacement (e.g., parts, components).
Limited Expansion Capacity	***Considerations:*** • If physical equipment is deployed to support detection, then it may require increased space to support updates or upgrades.

Potential Threats	Considerations and Possible Actions
	• The coverage area could greatly expand over time, requiring a significant number of additional detection devices. ***Actions to consider:*** • *Systems Engineering.* During the needs assessment, consider the potential need for expanded detection in the future and compare the cost to install, operate, and maintain detection devices versus procuring a probe data detection service. • *Procurement.* Consider an option to procure and install extra detection devices (if possible) during the procurement process. • *Performance Management.* Include input from the Performance Management group on additional needs for expanded detection in the future.
Unavailable Support	***Considerations:*** • If a vendor no longer exists or no longer supports a product or service, technical support and/or replacement parts could provide risks to detection devices or service that are expected to be used for a long period. ***Actions to consider:*** • *Asset Management.* Request an assessment of the risks of either the detection device or service, as well as support for purchased devices not being available and potential for discontinuation of the service. • *Procurement.* Encourage procurement considerations to consider the likelihood that the vendor devices and/or services provided will be available for the long-term.
Excessive Cost Increases	***Considerations:*** • Once detection devices or service are established, it is preferable not to change the approach unless there are assured benefits of a change, but excessive cost increases to either operating or maintaining the devices or services may create situations where an agency can no longer support the costs. ***Actions to consider:*** • *Procurement.* Before completing procurement, request clear declarations of what is covered during the period of the contract and what options the agency has for stabilizing maintenance costs of deployed detection devices or the mechanisms to control and avoid excessive cost increases for a detection service over time. Consider how costs are allocated to assist in selecting the best alternative given how the detection mechanism will be implemented and potential for increased use over time (e.g., per device versus service offerings). • *Professional Capacity Building.* Examine past trends at different agencies to estimate the potential long-term cost implications for detection devices or services.
Missed opportunities	***Considerations:*** • Detection options and related costs for both devices and services are continuously changing, and agencies may want to avoid being locked into contracts that do not allow renegotiating at reasonable periods. • Similarly, agency needs for detection may change. As an example, an agency may wish to monitor more of the network in the future that is not feasible for devices. Alternatively, the agency may require higher accuracy detection for

Potential Threats	Considerations and Possible Actions
	new safety critical systems that cannot be provided by a service. • Consistent procurement of a single type of detection device can increase efficiencies for maintenance purposes (e.g., less training for staff to maintain one vendor's devices vs. multiple, fewer parts to have in available inventory). ***Actions to consider:*** • *Systems Engineering.* Consider a phased implementation to a new device type or service that integrates existing detection prior to a full transition to leverage existing investments and provide an opportunity to procure devices that are compatible with both existing and new mechanisms. • *Systems Engineering.* Ensure that requirements and design do not unnecessarily favor any proprietary solution that prevents the agency from benefiting from lower costs to maintain or operate the solution. • *Procurement.* Involve procurement early in the process to explore options for long-term service or device maintenance contracts to protect the agencies options for renegotiating costs if industry pricing trends downward.
Reduced Funding	***Considerations:*** • While there may be funds for initial deployment or procurement, ongoing operations may compete for funds and the ability to adequately fund maintenance for detection devices or ongoing detection data services may be lost. For example, if funding for operations and maintenance of detection devices is reduced, difficult decisions may need to be reached about reducing the number/spacing of detection devices (e.g., from detectors every half-mile to every two miles). ***Actions to consider:*** • *Systems Engineering.* Use ConOps scenarios to consider the impacts on the systems that rely on the detection if funding to support device maintenance or detection services is partially or completely removed in the future (e.g., there are industry examples of agencies transitioning more widely spaced loop detectors to save operations and maintenance costs). Share these risks during the "go/no-go" decision period following the ConOps and requirements development. • *ITS Architecture & Strategic Planning.* Review programmatic planning documents to predict potential funding issues that may alter funding available for detection. If potential funding limitations are anticipated (e.g., reduced number of detectors in the future) this can be considered in the design of the system.
Allowed Use	***Considerations:*** • One risk regarding allowed use relates to potential limitations on use of probe data services (e.g., agencies procuring the data may only be able to use the data internally or publish speed maps, but not share it with partner agencies or the traveling public). ***Actions to consider:*** • *Systems Engineering.* When developing the ConOps, include needs for data sharing internally and externally. If there are specific needs for data sharing, ensure these are captured as requirements to be included in procurement.

Potential Threats	Considerations and Possible Actions
	• *Procurement*. Ensure that data sharing agreements are included in procurement process that represent the requirements developed during the systems engineering process. • *IT/Security.* Support the systems engineering team and project manager in understanding licensing and regulations around detection services being considered and potential data being exchanged with the provider.
Agency/Department Policy Decisions	***Considerations:*** • The procurement of detection services may involve procuring services for a period of time (e.g., service minimum charges for a 12-month period). ***Actions to consider:*** • *Procurement.* Consider possible changes to agency or department policy decisions and include any provisions in the contract to protect these changes.
Security Threats	***Considerations:*** • Depending upon the approach, detection devices or services have the potential to introduce vulnerabilities to the agency. ***Actions to consider:*** • *Systems Engineering.* Make sure requirements and design consider security of the detection device or service and supporting connections to the agency back office. • *Systems Engineering.* Involve the IT/security groups as early as possible in the systems engineering process to capture their input and benefit from established and documented requirements for security. • *Security/IT.* Provide input to both the systems engineering process and the eventual design and implementation.
Limited Accessibility	***Considerations:*** • There may be requirements that limit accessibility to the data provided by the detection services by systems or certain individuals inside or outside the agency firewall. Without proper considerations, the detection approach could prevent needed access and create situations where the detection service is not future proof. ***Actions to consider:*** • *Systems Engineering.* Make sure requirements and design consider how the detection service will connect with agency back-office systems or potential future uses (e.g., for traveler information or various agency individuals or groups) and verify compatibility of the firewall and other security aspects to ensure accessibility for functionality and use of agency services and users (or user systems) outside the agency. • *IT/Security.* Provide input to the systems engineering process to ensure the security not only protects the agency from vulnerabilities but also does not prevent communications to partners who need access.

9.0 Conclusions

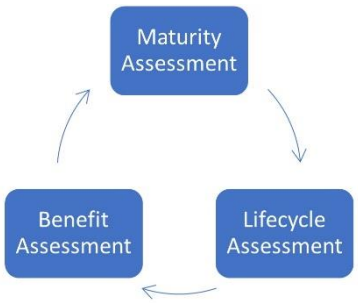
9.1 Recap of Research Findings

At the onset of this research, the initial focus was intended to examine best practices for future proofing ITS assets by extending the lifecycle of overall systems or individual components of overall systems. As the research progressed, the concept of 'future proofing ITS assets' evolved beyond the sole emphasis being duration of time the asset is deployed to also emphasizing the benefits that ITS assets are delivering.

This research revealed that future proofing ITS assets should not be an afterthought, but rather it should begin in project conception and should be managed throughout the entire process of considering, designing, procuring, installing, and operating the ITS solution.

This research suggests that future proofing should be addressed by the activities of seven existing areas/activities within each DOT, and the final report describes a series of actions to be considered by these seven areas/activities, most of which are minor changes that offer potential to minimize future proofing threats.

A CMF is introduced by this research for agencies to monitor the maturity of their actions to reduce the risks to future proofing ITS assets but is introduced with the clarification that the CMF is one of three metrics that should all be used to assess future proofing progress. These metrics include:



- Maturity assessment (i.e., CMF) of future proofing preparedness;
- ITS asset Lifecycle assessments; and
- ITS benefit assessments.

9.2 Relationship to Other ENTERPRISE Pooled Fund Study Research

The expanded focus of the research to also include lifecycle assessment and benefit assessment triggered relationships to two additional ENTERPRISE PFS projects recently completed, including:

- Evolving and Phasing Out Legacy ITS Devices and Systems – A project that researched practices that state DOTs take when considering when to phase out ITS devices and systems; and
- The Evolution of ITS in Transportation Asset Management – A project that identified best practices for estimating lifecycles and managing ITS assets in conjunction with other asset management approaches and tools.

While the earlier two projects were completed before this research, key aspects of each of the projects have been incorporated into the recommendations for mitigating future proofing risks defined for the seven areas/activities within each DOT.

9.3 Suggested Next Steps

Four recommendations for possible next steps are identified below.

9.3.1 Recommendation #1: Research to Prioritize the 17 Threats and Identify Specific Examples of Recommended Actions.

Table 1 of this report identifies 17 potential threats across seven threat types. While each of these is a threat to future proofing ITS assets, some are more critical than others. Therefore, it is proposed that research could prioritize the risks that are most likely to cause significant impacts to ITS asset use and therefore should be the primary emphasis of transportation agencies. Tables 11 and 12 of this report recommend a series of actions to help agencies reduce the future proofing risks associated with the 17 potential future proofing threats identified in this report. Each action is associated with the most appropriate DOT area or activity (e.g., systems engineering, procurement, etc.) to consider the actions. To add clarity and provide additional content for the recommendations, it is recommended that the same research activity that prioritizes the risks should also identify examples of how agencies are already performing the suggested actions to minimize the prioritized risks. Both aspects of this research could be conducted by a combination of a literature review, DOT survey, and one-on-one interviews.

Not only would this research provide more tangible insight to agencies wishing to implement actions to minimize the most critical risks, but it would also help to reaffirm the validity of the actions proposed, and possibly add, modify, or delete actions as the research searches for examples of actions already in use. This research would also summarize a variety of specific approaches to actions that could be adopted "as is" by agencies or adapted to fit each agency's unique situation and conditions.

The outcome of this research could be an additional column to Tables 11 and 12 with cited examples where agencies are already performing these actions, together with any additional details available about how the agency conducted these actions as well as benefits and any lessons learned.

Clarifications to the recommendation:

- This recommendation is that the research would seek out and find as many examples as possible, with the recognition that these actions are already happening in some DOTs prior to this research. This is not a recommendation to research changes that may result from this current ENTERPRISE project.
- While the goal would be that the research is able to identify one or more examples for each action, it is understood that it is more likely that examples will not be available (or discoverable by the research effort) for every action.

9.3.2 Recommendation #2: Research the Potential of Mainstreaming Recommended Actions

A second recommendation would be to research the potential to transition the findings of this project into mainstream operational procedures. To accomplish this, the suggestion is that once examples of the risk mitigation actions are identified and the actions are reaffirmed, Tables 11 and 12 could be translated into checklists for each of the seven DOT areas or activities referenced in the report, and

further divided by stage of asset lifecycle. While creating the checklists would be relatively straight-forward, the research aspect could include initial testing of the checklists with interested ENTERPRISE Pooled Fund Study members to help understand the usefulness, value, and effectiveness of the checklists.

Completing these checklists would also enable the research to identify the stages of the future proofing process where interactions with external systems (i.e., ARC-IT, Asset Management Tools, and others) are needed and most appropriate.

9.3.3 Recommendation #3: Researching the Logic of an Automated Software Tool to Support Risk Mitigation

A further next step towards institutionalizing future proofing of ITS assets into state DOTs could be developing a software solution to automate as many activities or recommendations as possible. Prior to developing a software solution, research is suggested to better understand if this approach should encourage a new software product, encourage modifications to existing software products (some privately owned some publicly owned), or encourage a combination of new software with modifications to existing.

This recommendation is further illustrated by the following examples:

- There are several available asset management software solutions offered by private vendors. If the research findings are summarized with recommended roles for asset management solutions, it is possible that vendors of these solutions may see the value and implement some or all of the recommendations, allowing current and future clients and users of these products to benefit.

- Similarly, some public operated on-line resources and/or software solutions (e.g., ARC-IT) may have funding for software changes and research findings from this recommendation might enable them to implement these changes.

- Finally, the options for modifying existing software solutions (or interest from the public or private agencies who own the solutions) might not sufficiently advance the integration of actions recommended in this report. Therefore, a new software solution may be the best solution, although research is recommended to understand if agencies will embrace (and be willing to collaborate to support) a new software product.

The recommended approach of this step would be to research the logic of automating the actions or automating notifications of the actions to reach the appropriate staff or group to implement the actions. The logic may best be captured in a spreadsheet to allow a series of "If/Then" rules to be created as the logic of how to implement the actions is defined.

9.3.4 Recommendation #4: Develop a Software Package to Automate the Logic of Risk Mitigation

Based on research in Recommendation #3, if a new software package is required, this recommendation would be to either create the software package or to summarize the research describing the need and

potential use of the software. The software package could contain the recommendations in this report and allow users to track their progress while making use of the outputs and content from ARC-IT and other asset management solutions, assuming links to the other systems are possible.

The creation of a new software package offers the potential to specifically deliver the exact logic of activities as determined in the research, but also carries the burden of supporting both the technical and institutional aspects of a public sector software product. Therefore, the ENTERPRISE Pooled Fund Study should consider options such as AASHTO Ware or other scenarios where ongoing support can be ensured for potential users.

10.0 Summary of Literature and Resources Reviewed

There is a wealth of documentation about resilience in general, and about resilience in transportation. Most of the resilience planning involves preparations for climate change and other natural phenomena that will require substantial changes to infrastructure. This literature is briefly synthesized to capture best-practices and lessons learned that can be translated to the more specific future proofing concepts of detection and communication systems.

Resilience is a topic addressed extensively by the transportation industry. A brief overview of some of the resources reviewed as part of this project is summarized here to offer readers links to additional resources.

AASHTO Resilience Activities. AASHTO has a Committee on Transportation System Security and Resilience. This committee resides in AASHTO's Enterprise/Cross-Discipline Committees. Several activities and publications, relevant to this project, are summarized below.

September 2020 Technical Session on Resilience. As part of the AASHTO 2020 Virtual Joint Policy Conference, a technical session on resilience was hosted. Presentations included topics on lessons learned from Superstorm Sandy, performance standards for resilience, modifying agency organization and management to accommodate transportation system technologies, and deploying transportation security practices. The presentations are available for download at this site. Key takeaway:

- A quantitative formula is shared by UDOT to AASHTO Understanding Transportation Resilience: A 2016-2018 Roadmap published in 2017.[1] Key takeaways:
  - This report includes a brief but thorough background summary on resilience;
  - It describes the need (in 2017) for resilience for the transportation system in general.

NCHRP Resilience Research. NCHRP has completed multiple studies documenting planning and design guidelines for resilience, including:

- NCHRP Synthesis 527: Resilience in Transportation Planning, Engineering, Management, Policy, and Administration (2018)[18]. Key takeaways include:
  - Provides a background on the evolution of highway resilience.
  - Describes a series of case studies where three state DOT's resilience activities are described as well as one port authority and one MPO.
  - One aspect described is four goal areas that each agency should consider for resilience. These include: 1) Maintaining continuity of function, 2) Graceful degradation (instead of failure all at once), 3) Recovery of function in designated time, and 4) Inhibit a basic state of change.

- NCHRP Research Report 970 Mainstreaming System Resilience Concepts in Transportation Agencies: A Guide (2021).[15] Key takeaways include:
  - The emphasis of the report is on resilience in response to human-caused (e.g., cyberattacks) and natural disruptions (e.g., increased water levels).

- A key outcome is recognition that every major functional area within a DOT all have roles in making the system more resilient.
- A framework and assessment tool are included that help agencies understand what they are doing to address resilience, identify where modified processes are needed, and recommend steps to implement actions.

10.1 Synthesis of Future Proofing Resources

AASHTO Resource:

In AASHTO's Understanding Transportation Resilience,[1] the six key aspects of resilience identified in the 2015 National Infrastructure Advisory Report are:

- The importance of understanding the systemic risks causing system disruptions
- Incorporating resilience into operational practice
- Investing in resilient infrastructure
- The importance of conducting a quadrennial review of transportation infrastructure
- Developing tools, models, and standards to mitigate risks
- Operationalizing resilience

The second bullet above presents a key point that resilience and future proofing cannot be related simply to a device, the entire operational practice needs to support future proofing.

Forbes Article Resource:

In the Forbes article "Forget Smart Cities, 'Stupid' Infrastructure Is the Solution for Future Transportation,"[10] the author advises against putting too much functionality into the infrastructure, noting that the Internet as "dead simple" (delivering postcards from point A to B), but notes "it's essentially the same design today as 40 years ago! Even so, we've seen the greatest period of innovation in human history on top of that stupid infrastructure, and it's not a coincidence. On the internet, all the smarts are in the edge devices. Your phone. Your laptop. The web server that sent you this web page. Everything is there, even the negotiation of network link quality and speed which you might imagine should be in the infrastructure, which is much closer to those factors." An additional quote from this article is "You can't plan for 2030 in 2021 so you don't. Instead, you keep what you must build simple and put as much as possible into software. That's because you can change all your software in 2030 when you learn the reality of the future, and it's free to deploy it, even though not to write it."

Forward Compatibility and Planned Obsolescence:

Wikipedia defines forward compatibility as a "characteristic that allows a system to accept input intended for a later version of itself".[11] Forward compatibility can avoid obsolescence during the product lifetime. Planned obsolescence is defined as a type of upward compatibility, typically a commercial approach, of backwards incompatibility so that new applications require newer devices.

References

[1] Fletcher, David and David S. Ekern. Understanding Transportation Resilience: A 2016-2018 Roadmap for Security, Emergency Management, and Infrastructure Protection in Transportation Resilience. AASHTO, Washington, D.C., National Operations Center of Excellence (NOCoE), January 2017, https://transops.s3.amazonaws.com/uploaded_files/UTR-1%20book%20vers%205_0.pdf.

[2] Conway, Mark. Future-proofing Our Transportation Infrastructure. Walter P. Moore, n.d., accessed 17 Nov 2021 from https://www.walterpmoore.com/moore-infrastructure/future-proofing-our-transportation-infrastructure.

[3] Love, Peter E.D., Lavagnon A. Ika, Giorgio Locatelli, and Dominic D. Ahiaga-Dagbui. Future-proofing 'Next Generation' infrastructure assets. Frontiers of engineering management, vol. 5, no. 3, pp. 1-4, doi: 10.15302/J-FEM-2018204, 2018, retrieved 17 Nov 2021 from https://dro.deakin.edu.au/eserv/DU:30111975/ahiagadagbui-futureproof-2018.pdf.

[4] Threat Analysis Group (TAG). Threat, vulnerability, risk – commonly mixed up terms. TAG, n.d., accessed 17 Nov 2021 from https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/.

[5] Harder, Patrick and Alexander Bulkin. US Infra Faces New Stresses. Nossman, Project Finance International, January 13, 2021, retrieved from https://www.nossaman.com/assets/htmldocuments/US%20Infra%20Faces%20New%20Stresses.pdf.

[6] Rehman, Obaid Ur, Michael Ryan, and Mahmoud Efatmaneshnik. Future Proofing Process. INCOSE International Symposium, 27(1):921-934 DOI:10.1002/j.2334-5837.2017.00403.x, July 2017, retrieved 17 Nov 2021 from https://www.researchgate.net/publication/319407223_Future_Proofing_Process.

[7] Hughes, J. F. and K. Healy. Measuring the resilience of transport infrastructure. NZ Transport Agency research report 546. AECOM New Zealand Ltd, February 2014, retrieved 22 Nov 2021 from https://www.nzta.govt.nz/assets/resources/research/reports/546/docs/546.pdf.

[8] Preisen, Linda, Carla Helgeson, and Dean Deeter. Evolving and Phasing Out Legacy ITS Devices and Systems. ENTERPRISE Pooled Fund Study TPF-5(359), October 25 2019, retrieved 22 Nov 2021 from https://enterprise.prog.org/wp-content/uploads/ENT_PhasingOutLegacyITS_Report_FINAL_Oct2019.pdf.

[9] Intaver Institute. Project Risk Resilience. Accessed 22 Nov 2021 from https://intaver.com/project-risk-resilience/.

[10] Templeton, Brad. Forget Smart Cities, 'Stupid' Infrastructure Is The Solution For Future Transportation. Forbes, July 27, 2021, accessed 22 Nov 2021 from https://www.forbes.com/sites/bradtempleton/2021/07/27/forget-smart-cities-stupid-infrastructure-is-the-solution-for-future-transportation/?sh=49e973831441.

[11] Forward compatibility. Wikipedia, Wikimedia Foundation, 14 Oct 2021, accessed 22 Nov 2021 from https://en.wikipedia.org/wiki/Forward_compatibility.

[12] Extensibility. Wikipedia, Wikimedia Foundation, 25 Feb 2021, accessed 22 Nov 2021 from https://en.wikipedia.org/wiki/Extensibility.

[13] ARC-IT 9.0. Architecture Reference for Cooperative and Intelligent Transportation. United States Department of Transportation, October 13, 2021, accessed 22 Nov 2021 from https://local.iteris.com/arc-it/.

[14] WSP USA. Business Models to Facilitate Deployment of Connected Vehicle Infrastructure to Support Automated Vehicle Operations. National Cooperative Highway Research Program (NCHRP) Project 20-102(12), October 2020, accessed 22 Nov 2021 from https://www.nap.edu/read/25946/chapter/1.

[15] Dorney, Chris, Michael Flood, Time Grose, Paula Hammond, Michael Meyer, Rawlings Miller, Ernest R. Frazier, Sr., Jeffrey L. Western, Yuko J. Nakanishi, Pierre M. Auza, and John Betak. Mainstreaming System Resilience Concepts into Transportation Agencies: A Guide. National Cooperative Highway Research Program (NCHRP) Research Report 970, National Academies of Sciences, Engineering, and Medicine, Washington, DC: The National Academies Press, 2021, retrieved 22 Nov 2021 from https://doi.org/10.17226/26125.

[16] Olsson Associates, Cambridge Systematics, and Aureon. Intelligent Transportation Systems (ITS) and Communications Systems Service Layer Plan. Iowa DOT Office of Traffic Operations, January 2018, retrieved 22 Nov 2021 from https://iowadot.gov/TSMO/ServiceLayerPlan3.pdf.

[17] Weatherford, Matt and Jeremy Schroeder. The Evolution of ITS in Transportation Asset Management. ENTERPRISE Pooled Fund Study TPF-5(359), May 6, 2020, retrieved 25 Jan 2022 from https://enterprise.prog.org/wp-content/uploads/ENT-ITS-Asset-Mgmt-final-report.pdf.

[18] Flannery, Aimee, Maria A. Pena, and Jessica Manns. Resilience in Transportation Planning, Engineering, Management, Policy, and Administration. National Academies of Sciences, Engineering, and Medicine, Washington, DC: The National Academies Press, 2018, https://doi.org/10.17226/25166.