Vendor Cybersecurity Risk Assessment in an Autonomous Mobility Ecosystem

Albena Tzoneva[1], Galina Momcheva[2], Borislav Stoyanov[3]

[1] Department Computer Science, Varna Free University "Chernorizets Hrabar" Varna, Bulgaria (albena.tsoneva@vfu.bg)
[2] Department Computer Science, Varna Free University "Chernorizets Hrabar" Varna, Bulgaria (galina.momcheva @vfu.bg)
[3] Department Computer Science, Varna Free University "Chernorizets Hrabar" Varna, Bulgaria (borislav.stoyanov @vfu.bg)

Abstract - Vendor cybersecurity risk assessment is of critical importance to smart city infrastructure and sustainability of the autonomous mobility ecosystem. Lack of engagement in cybersecurity policies and process implementation by the tier companies providing hardware or services to OEMs within this ecosystem poses a significant risk to not only the individual companies but to the ecosystem overall. The proposed quantitative method of estimating cybersecurity risk allows vendors to have visibility to the financial risk associated with potential threats and to consequently allocate adequate resources to cybersecurity. It facilitates faster implementation of defense measures and provides a useful tool in the vendor selection process. The paper focuses on cybersecurity risk assessment as a critical part of the overall company mission to create a sustainable structure for maintaining cybersecurity health. Compound cybersecurity risk and impact on company operations as outputs of this quantitative analysis present a unique opportunity to strategically plan and make informed decisions towards acquiring a reputable position in a sustainable ecosystem. This method provides attack trees and assigns a risk factor to each vendor thus offering a competitive advantage and an insight into the supply chain risk map. This is an innovative way to look at vendor cybersecurity posture. Through a selection of unique industry specific parameters and a modular approach, this risk assessment model can be employed as a tool to navigate the supply base and prevent significant financial cost. It generates synergies within the connected vehicle ecosystem leading to a safe and sustainable economy.

Keywords—autonomous mobility, vendor risk, risk assessment, sustainable smart city

I. INTRODUCTION

Lack of engagement in cybersecurity policies and process implementation by tier companies poses a significant risk to not only the individual companies but to the ecosystem overall. Every company in the United States and globally is at risk of cyber-attacks that can disrupt and halt services essential to economy and public safety. The defense of critical infrastructure is only as strong as the weakest link. The importance of implementing cybersecurity protection on all levels, OEM, as well as tiers, is of paramount importance to economic sustainability. Last year numerous companies were targets of cybercrime. These companies were small and large, and spanning across various industries.

Cyber criminals are crossing borders and endangering countries like most recently Ukraine where destructive malware and ransom attacks resulting in website defacement and potentially destructive malware with severe impact on critical functions. Similar malware like NotPetya and WannaCry ransomware were deployed to wreak havoc and do damage to critical systems. CISA (Cybersecurity and Infrastructure Security Agency) is advising that all organizations and their senior leaders implement necessary measures to protect their operations. All organizations, regardless of their activity or size, should immediately implement recommended measures [1].

II. SUSTAINABLE MOBILITY

A. Autonomous Vehicles

There is a societal gain of immense proportion in going to autonomous mobility. It eliminates human error which is the leading cause of fatalities. In the U.S. alone there are over 35,000 fatalities every year, over 260,000 in China and over a million worldwide. Adopting the new autonomous technologies will reduce if not eliminate the fatalities caused by human error. Through autonomous braking, lane and park assist technologies, most road accidents can be avoided. These technologies are developed both as hardware and software components. OEMs and Tier suppliers have the common goal of reducing fatalities and providing reliable, safe technologies to enable autonomous driving [4].

In the Transportation industry, automation is making strong advances. According to NHTSA, the levels of automation are as follows[3]:

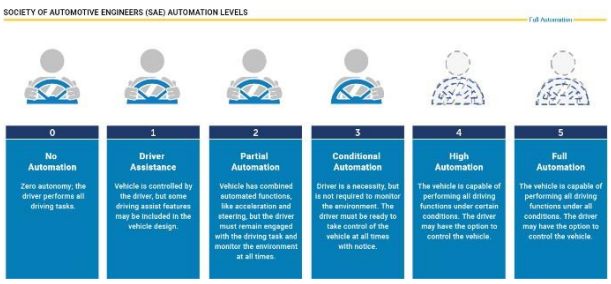

Fig. 1. NTHSA Levels of Automation. Source: [3].

Autonomous vehicles can execute and decide when it is appropriate to use safety-critical functions without direct input from a human operator. This system can adapt to unforeseen conditions and environments in real-time. Early adopters are General Motors, Tesla, Waymo, and today most automotive OEMs in partnership with Autonomous driving companies.

This highly automated environment along with the ubiquitous connectivity of vehicles to vehicles and vehicles to infrastructure raises the importance of sustainability of this ecosystem. Operation and communication systems, global and inertial navigation satellite systems along with sensor systems are an intrinsic part of the smart city ecosystem.

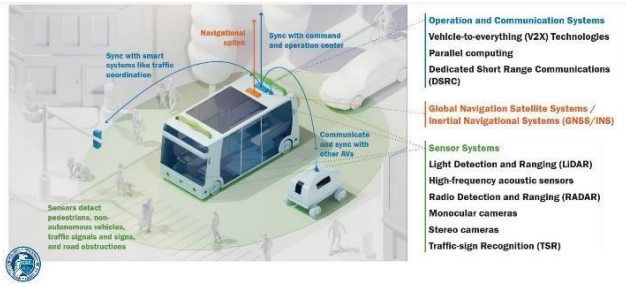

Fig. 2. Illustration by Kate McClaskey, DHS-CISA

B. Sustainability of Smart Cities

Sustainability of smart city networks is largely dependent on the secure, uninterrupted, and safe operations of all connected systems. The equilibrium between these systems can be endangered by foul play of significant impact due to the ubiquity and long reaching span of these systems. Every player in this system should be deemed responsible for the safety and security of this connected ecosystem.

Sustainable can be defined as the achievement of affordability, effectiveness and attractiveness maintained on a long-term basis economically, socially, and environmentally. Cybersecurity breaches disrupt systems on a local as well as national basis. Autonomous mobility is one of the critical infrastructures that need to be protected with utmost scrutiny. Imagine a widespread autonomous vehicles disruption where roads are blocked, people are stranded, and goods cannot reach their destination. The picture can be much grimmer with human lives taken and damages of vast proportion inflicted.

One of the strategic documents addressing sustainability is the European Commission's proposed plan. This document outlines a framework for planning and management of urban mobility. This document is the Sustainable Urban Mobility Plan (SUMP) [5]. Its objective is to improve residents' quality of life by ensuring a 'safe, reliable, integrated, multi-modal, effective and environmentally friendly transport system'[6]. Urban mobility is one important part of the fabric that includes user behavior, social policies, health, and economic growth[7]. It combines intelligent transport systems with information and communication technologies which must be sustainable, accessible, safe, and affordable for citizens, businesses, and industries[8]. Each stage of this plan is affected by the cybersecurity integrity of all participating OEMs and vendors.

Fig. 3. SUMP process diagram. Source: [8].

SUMP scenarios are inadvertently related to the technologies embedded in vehicles and infrastructure. Each technology is represented by products that are comprised of multiple components manufactured by various vendors. Unlike some components that have no relation to data communications, multiple others include electronic chips, boards, and electrical wiring. The overall electrical architecture of the component is designed to allow for the flow of data packets in and out of the component. These data packets travelling through the component, the vehicle, and the infrastructure around are vulnerable to malicious hacking and lucrative to criminals whose purposes span from financial profit to destruction on a global scale.

C. Smart Cities

Two-Thirds of the world's population (more than six billion) will live in cities and neighboring regions by 2050. It is imperative that urban development and architecture are aligned with the technological advancements bringing connectivity and autonomous mobility to the cities. This connected system needs to be designed in a sustainable manner to serve the purpose of improving human lives, functioning with optimal resources, and minimizing costly and inefficient disruptions.

Through a wireless sensor network (WSN), a digital skin is formed over cities. Smart mobility and smart cities deploy numerous sensors enabling communication between vehicles

and infrastructure, including lidars, cameras, radars, and ultrasonic sensors just to name a few. Massive amount of data is flowing between embedded and pervasive devices and across various platforms. Data analytics and AI(artificial intelligence) are powering industries like logistics and autonomous vehicles networks.

III. Cybersecurity of Smart Cities

A. *Connected Vehicles Ecosystem*

Synergies in the connected vehicle ecosystem are necessary to achieve a sustainable system which will be functioning in an optimal way. It is of crucial importance to be aware of the security posture of both service and solution providers in the partner ecosystem. The weakest link in the chain can be low down in the tier ranks and become an entry point for security breach. This was exhibited with the case of SolarWinds network management software hack in 2020 which had a widespread impact including U.S. Government departments. Every organization must build resiliency, business continuity and disaster recovery plans. Only then the mobility ecosystem can be sustainable and safe for all citizens.

Every OEM and vendor down the chain carries the responsibility to develop a cybersecurity posture according to best practices and standards from NIST, SAE, ISO, and other industry-wide organizations. Common methodologies of risk assessment have been highlighted as a basic requirement for understanding each organization's vulnerability and for allocating adequate resources for defense in depth [9].

On the other hand, surveys convey a concerning reality. AT&T and Spiceworks research of 250 IT professionals in the summer of 2018, Charting a New Course, revealed that 60% of C level executives are disconnected from the realization of an imminent cybersecurity threat and think their current solutions keep them completely or very safe while only 29% of IT security staff agrees with this. In this research, 57% were not confident in their cybersecurity risk management strategies and only 38% said they felt completely or very safe. Only 47% felt vulnerability assessment was a high priority. This study made it apparent that data security improvements were lagging. It has been proven that business outcomes are related to confidence in Security Management. Enhancing cybersecurity should become one of the top action items for business leaders to achieve their strategic priorities.

Although most ransomware operations are opportunistic, CrowdStrike Intelligence identified the highest number of ransomware-associated data extortion operations this year in the industrial and engineering sector, closely followed by the manufacturing sector.

In Figure 4, the industries targeted by Data Extorsion by BGH Ransomware families are one of those with extensive vendor base that goes several levels down the supply chain process. If the security of even one of vendors in the chain is breached, the whole system gets out of balance. To detect and root cause a cybersecurity event often takes months. Attackers lurk in the background unnoticed while the malware ultimately reaches the OEM and the customer. It should be noted that the top targeted industries are Industrials & Engineering followed by Manufacturing. Extorted data can range from personal data to company confidential data and intellectual property. The livelihood of a company may be at stake even though all security measures have been taken. Vendor cybersecurity posture is not an isolated act, it is a part of the overall supply chain posture.

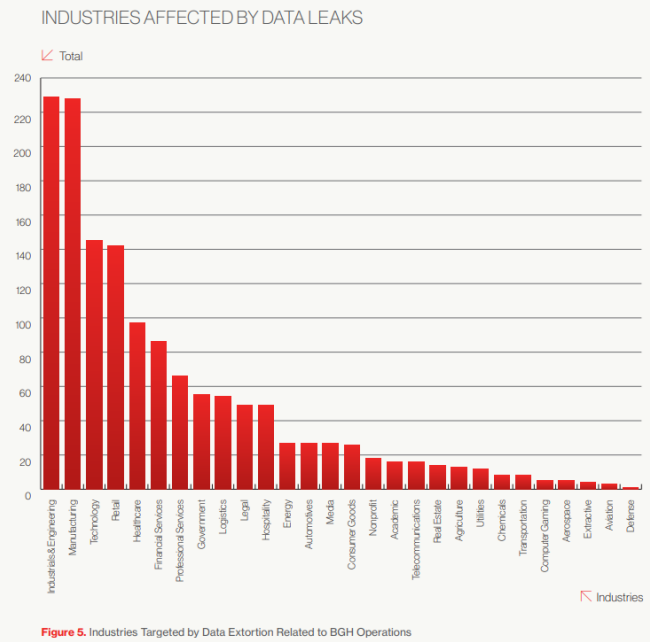

Fig. 4. Industries Targeted by Data Extortion. Source: [10].

B. *Vendor Cybersecurity Risks*

Automotive software as well as hardware supply chain risks have escalated with the new connectivity paradigm. It is very much dependent on whether manufacturers of electronic components have built in cybersecurity protection in their products. There is uncertainty and risk coming from multiple variables such as the time when the supplier was brought on board, the level of detail of cybersecurity requirements, alignment with overall industry best practices and maintaining their freshness and adequacy. These present a huge challenge to the sustainability of the mobility ecosystem. Competitive and proprietary nature of new technologies product development further exacerbates the difficulty to agree on sharing the true scope of security measures.

In the specific case of software, similar to any supply chain, several organizations or departments contribute to the creation and integration of the code. Each of them may be in a position to compromise the integrity of the product. As an example, an application can be created initially from an existing software such as open source and some over the shelf products. Each of them in turn can consists of various inputs from various sources. It can be unclear when all these inputs came into play. The complexity of this compilation can be a highly challenging activity to track, maintain, and decommission accordingly.

As it stands, OEMs are responsible for ensuring the autonomous vehicle of the future is equipped with the required

cybersecurity features. Consequently, their partners will be held to the same standard. They will have to provide evidence that they have implemented measures to meet the requirements. The areas that vendors need to pay specific attention to are security by design, early detection and response, robust over the air updates and diagnostic, and cybersecurity risk management.

IV. Industry Recommendations

A. NIST Recommendations

According to NIST, there are no well-established methods of vetting the vendor cybersecurity posture.
NIST has offered some best practices for managing vendors more effectively. Examples of Vendor Management practices include some of the following [11]:

- Priority of brand integrity over brand identity. Vulnerabilities of the supply chain need to be identified early in the life cycle product development process through a process of assessment and deliberate choice of providers.
- IT to be involved in the procurement process and sourcing to vendors. Engineering and operations to have input into sourcing decisions along with the wider multi-stakeholder team.
- Security requirements and stipulations to be included in all RFPs (request for proposal) and vendor contracts with specifics related to the particular type of business.
- Owners must be responsible for any tradeoffs, exceptions, and risks of vendor contracts.
- Supplier self-evaluation is not sufficient in the process of assessing a supplier cybersecurity posture. On-site verification and audits need to be performed to validate self-evaluation. Some companies have a representative at the supplier companies year around to perform continuous monitoring.
- New vendors must go through an assessment period. Their capabilities need to be tested along with their compliance to requirements and best practices. If the business is in a high-risk field, supplier needs to go through a couple of pilot runs before becoming approved to enter the supply chain.
- The same survey that is used by OEMs on Tier 1 suppliers should be used down the various tier levels.
- Approved vendor lists are compiled and maintained through a continuous monitoring of cybersecurity measure implementation.
- Quarterly reviews to be conducted to assess supplier adherence to requirements and their performance.
- Annual supplier meetings to be used as a forum to highlight customer needs, security goals and mitigation strategies.
- Mentoring and training programs can be shared with suppliers to ensure vendors are trained to cybersecurity materials originating from OEMs or Tier1 levels

B. NHTSA Recommendations

NHTSA (National Highway Traffic Safety Administration) is also focused on strong cybersecurity [12]. The recommendations coming from NHTSA for companies to follow are:

- Layered Approach: Identify, Protect, Detect, Respond, and Recover
- Vehicle Development Process with Explicit Cybersecurity Considerations during concept, design, production, sale, usage, maintenance, resale, and decommissioning
- Vulnerability Reporting/Disclosure Policy
- Penetration Testing and Documentation
- Risk Assessment
- Leadership Priority on Product Cybersecurity
- Information Sharing Executive Order 13691
- SAE and ISO first joint standard, ISO/SAE 21434: Road Vehicles - Cybersecurity Engineering

C. ENISA Report Recommendations

Globally, the European Union Agency for Cybersecurity (ENISA) published the ENISA Threat Landscape for Supply Chain Attacks report in July 2021. This report is dedicated to the taxonomies of assets and threats and identifies supply chain attacks as one of the nine primary cybersecurity threats for the past year.

Advanced Persistent Threat (APT) attacks are stated as one of the prominent methods. Figure 5 demonstrates an APT attack.

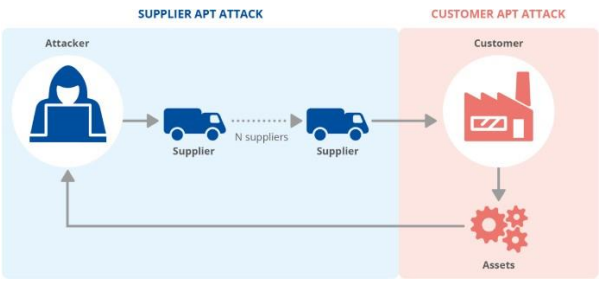

Fig. 5. APT Supply Chain Attack. Source: [14].

The report talks about both the asset and threat taxonomies and highlights the attack techniques on the supply chain including malware infections, brute-force attacks, social

engineering, and exploiting software vulnerabilities. On the other hand, the attacks used to compromise customers are phishing, counterfeiting, physical attacks, or exploiting a trusted relationship [14].

In Figure 6, the most targeted assets by a supply chain attack are identified by ENISA. Many new technological inventions and products have embedded software or firmware. One example are the sensors in the vehicle such as lidars, cameras, radars. These are smart devices that get integrated into the autonomous platform of the vehicle and provide continuous data stream of the surrounding environment. The software and firmware in these devices go through multiple iterations and upgrades during the full life of the product. If the software and firmware have not been created following a sustainable process of observance of requirements and adherence to security processes, they become a vector for intrusion into the sensor.

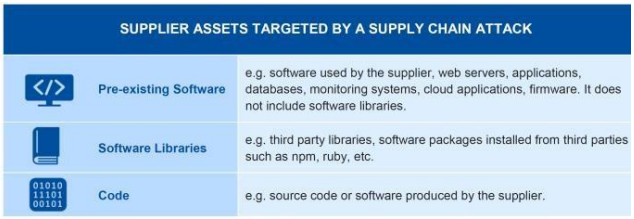

Fig. 6. Supplier Assets. Source: [14].

D. CISA and SAE/Synopsis Studies

In 2020, CISA (Cybersecurity and Infrastructure Security Agency) conducted a study on autonomous vehicle systems including their adoption timeline, potential cybersecurity threat vectors and recommended mitigation strategies. Consequently, CISA published the Autonomous Ground Vehicle Security Guide: Transportation Systems Sector [2]. The main goal of this effort was to help CSOs (Chief Security Officers) and CISOs (Chief Information Security Officer) understand the risks endangering the autonomous ecosystem and guide them to implement strategies reducing these risks.

A Study of Automotive Industry Cybersecurity Practices, Supply Chain and Third-party Component Challenges was conducted by SAE (Society of Automotive Engineers) and Synopsis. Seventy-three percent (73%) of respondents were very concerned about the cybersecurity defense of third-party automotive suppliers. Only forty four percent (44%) said their organizations have stringent cybersecurity requirements for upstream suppliers [13]

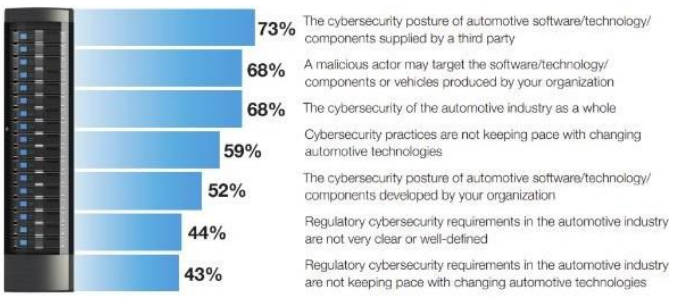

Fig. 7. SAE/Synopsis Survey. Source: [13].

Most automotive electrical components today process electronic data. Secure coding becomes of paramount importance in securing these components. Only thirty three percent (33%) of respondents indicated they train developers to secure coding practices. The integration of third-party components along with firmware and software embedded in these components, presents a significant challenge, and opens the door for intrusion. Only twenty eight percent (28%) said development, testing and validation were rigorously enforced [13].

Cybersecurity should be looked at as an integral part of functional safety and follow a parallel product development cadence. It should include data protection, physical protection, as well as embedded software protection. With policies and requirements being tightened by OEMs and Tier1 suppliers, all players in the field need to take necessary steps towards developing a robust cybersecurity stance. Only then the mobility system will function efficiently and provide sustainable future.

V. Proposed Model for Vendor Cybersecurity Assessment

With the disparities and imbalances of the level of cybersecurity rigor among the multi-level supply chain, how can vendors be vetted and trusted? What is the mechanism for assessing vendors on the implementation of best practices and requirement?

Various approaches exist today, many of which come down to questionnaires. These are no longer sufficient and do not reflect the demands of a complicated connected ecosystem. OEMs and Tier1s are passing on the stringent requirements to their vendors down the chain.

One of the most effective ways to assess cybersecurity posture is adherence to industry best practices and recommendations. Suppliers need to demonstrate they have developed and are following processes and procedures from the very initiation of the product development life cycle. That is not a consistent practice with some vendors due to resources and compressed timing demands. Adding security features later in the product life cycle becomes a patch work which is not all comprehensive and is difficult to continually maintain and update. This paper proposes a quantitative model for assessing vendor cybersecurity posture.

By implementing specific requirements for cybersecurity health, the model is tailored to the smart city sustainability. Vendors providing services to the autonomous vehicles OEMs need to meet these requirements to ensure continuously operating systems.

A. First Step

A Pugh matrix in Table I is used to narrow down supplier choices by vetting them on specific attributes. Attributes are industry dependent and need to be aligned with customer requirements. Attributes need to be developed first internally by the organization during the process of defining their cybersecurity goals followed by defining the attributes for an individual product then coupling these attributes with the

customer specific cybersecurity requirements. This matrix can be used to narrow down the selection of suppliers to only the ones to undergo risk assessment.

Table I. Pugh Matrix of Supply Chain

Attributes / Concept / Criteria	Import. Rating	Datum	Supplier 1	Supplier 2	Supplier 3	Supplier 4	Supplier 5	Supplier 6	Supplier 7	Supplier 8
		Work this way -->								
Secure boot	5	+	+	+	+	+	-	-	+	+
Secure in-vehicle communication	5	+	+	+	-	-	+	+	-	+
ECU component protection	4	+	+	+	+	-	+	+	+	+
Secure host flashing	3	+	+	+	-	+	+	-	+	-
Secure logging	2	+	+	+	+	-	+	-	+	+
Controlled secure access	3	+	+	+	+	-	+	+	+	+
Secure storage of data and keys	3	+	+	+	+	-	+	+	+	-
EEPROM emulation	5	+	-	+	+	-	+	+	+	-
RSA	5	+	-	-	+	+	-	+	+	-
Cryptographic services	5	+	-	+	+	-	-	-	+	-
Key exchange protocols	3	+	+	+	+	+	+	-	+	-
AUTOSAR	2	+	+	+	-	-	-	-	-	-
5+ (Sum of positives)			9	11	9	4	8	6	10	5
5- (Sum of negatives)			3	1	3	8	4	6	2	7

Examples for an ECU (electronic control unit) attributes would be the following.

Pugh matrix, as part of Six Sigma methodology, is a way to capture the unique design differences between various executions. In a similar manner, we can use this type of matrix to evaluate various vendors on their implementation of security measures.

Table II. Examples of Cybersecurity Attributes.

Secure boot
Secure in-vehicle communication
ECU component protection
Secure host flashing
Secure logging
Controlled secure access
Secure storage of data and keys
EEPROM emulation
AUTOSAR
Preemptive parallel job processing
Runtime manipulation detection
Basic cryptographic services: AES, CMAC, Hashing, key derivation, TRNG
RSA(Rivest–Shamir–Adleman – digital signature algorithm
Key exchange protocols – Diffie Hellman
Certificate support – Authenticity, parsing
Quality standards supported - ASPICE, ISO 26262, ASIL D

B. *Second Step*

Use Monte Carlo analysis to simulate attack vectors and the risk distribution. The attributes are depicted as variables and a random risk value is assigned to each one of them. The model is run numerous times and different values are assigned each time until a distribution curve is developed. The mean and variance are calculated to determine where each variable point is to the mean with anticipated normal distribution of risk.

$$\mathrm{SD} = \sqrt{\frac{\sum |x-\mu|^2}{N}} \qquad (1)$$

C. *Third Step*

Evaluate trust risk if deemed necessary and compound it with the functional vendor risk. Stated specifications by suppliers may not be fully aligned or truthful. They can be divided into actual and presumed. Vendors can be very protective of their technology and product build. It is their discretion how much they disclose about the implemented security measures. Using some historical data and experiences, certain amount of risk can be added as presumed.

D. *Fourth Step*

Enterprise level aggregate loss probability – loss exceedance probability for Total Cost can be calculated.

Loss exceedance graph shows the annual probability that one or more of the risks will materialize and what the cost impact to the organization would be.

Can I tolerate a 10% chance that our Total Losses exceed $800 million per quarter? Figure 6 and Figure 7 represent examples of calculating vendor cyber security risk impact on the organization.

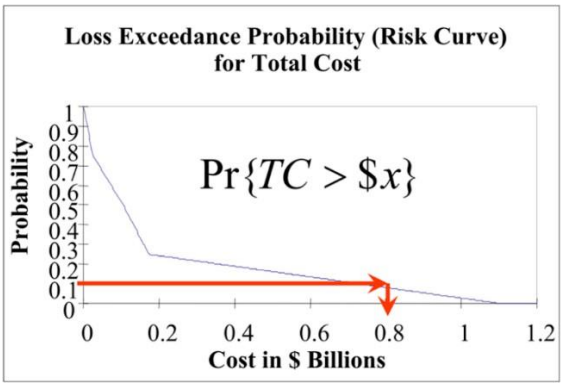

Fig. 8. Total Cost Loss Exceedance.

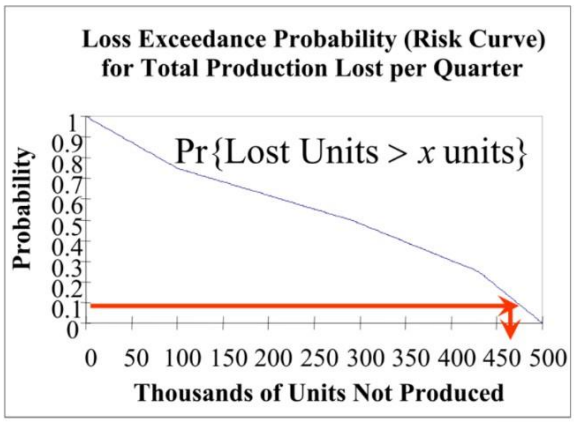

Fig. 9. Total Production Loss Exceedance.

Similarly, the loss exceedance graph for the probability of production loss can be generated after careful internal organizational analysis. A metric for assessing the risk needs to be established. This metric needs to tie to sustainability objectives. The primary goal is to achieve a balanced, uninterrupted eco system of smart city vendors who abide by the requirements for cybersecurity posture. Best recommendation is to follow the ISO21434. A risk matrix with red, yellow, green quadrants and based on probability of occurrence and severity of the impact is a sound way to go about it.

VI. Model Usage

Management decisions would be better formulated if based on this probabilistic risk method. Resource allocated to cybersecurity should be adequate to the risk level of the company.

The innovative approach of the proposed risk assessment model allows OEMs to calculate compound cybersecurity risk at all tiers, then assess this compound risk as part of the overall enterprise risk. This unique approach allows to vet vendors based on tangible and specific to the industry requirements. This aspect is important to sustaining systems comprised of products that have been securely developed. Its significance lies in its applicability to industry demands. Requirements are derived from the very initiation of the product development process. These requirements are then embedded in the risk assessment tool and tracked periodically throughout the life of the product.

The model can be used modularly where the number of vendors and systems under evaluation can be chosen by the organization. It can easily be modified and customized in accordance to the industry and product. Several scenarios can be developed based on this model. Decisions about sourcing of parts can now be based not only on product characteristics but also on the cybersecurity posture of the company. How many parts to source through the same vendor can be strategically analyzed and evaluated through this method.

The proposed risk assessment method addresses the demand of supply chain management of cybersecurity risk. The automotive industry is in a transformation stage of immense proportion as it is transitioning to autonomous driving, IoT, cloud data processing and artificial intelligence. The new architecture of smart cities requires in depth analysis of risk. Supply chain issues stem from the uneven levels of technological development, reluctance to add overhead cost for cybersecurity, competitive pressures, and sheer lack of skill. OEMs will not carry the whole liability but rather will transfer it to their suppliers. Every C-staff needs to make informed decisions on which vendors meet the requirements and which to bring on board. Continuous monitoring and adherence to best practices should be embedded in the organization's processes and procedures.

The challenges associated with this method come with the quality of the data used, the uncertainty about the truthfulness of supplier disclosure, and the unpredictability of future events. These three aspects require monitoring and participation in industry data exchange. They need to be further analyzed and defined to serve as a reliable basis for implementation.

The value of this proposal lies in providing a unique methodology that evaluates vendor risk. This method is essential in assessing vendors and making the right choices in the supplier process. It offers a structure that can be applied to vendors on a global scale and vetting them on the same set of parameters. It provides an opportunity for competitive advantage and establishing long lasting tier relations with OEMs. Awareness of the potential financial impact on the organization is fundamental for making sound business decisions.

VII. Conclusion

Bringing all vendors who are participating in the autonomous smart city ecosystem to the desired level of cybersecurity protection is pivotal to the sustainability of the system. Vulnerable vendors can become an intrusion vector for criminals allowing them to disrupt the whole ecosystem. Smart cities can only be sustainable if they are safe and functioning efficiently. Recognizing that new technologies enable the development of smart cities; they also need to be scrutinized for their safety and security compliance. Every OEM and vendor has a role in keeping smart cities in a sustainable state of operation.

References

[1] CISA, "Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats," Jan18, 2022, www.cisa.gov, 2022.

[2] AUTO-ISAC, November 2021 Community Call https://automotiveisac.com/community-call/november-2021-community-call, 2021.

[3] NHTSA, "Automated Vehicles for Safety," https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety#topic-road-self-driving, 2022.

[4] Hazel Si Min Lim and Araz Taeihagh, "Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications," Lee Kuan Yew School of Public Policy, National University of Singapore, 469B Bukit Timah Road, Li Ka Shing Building, Singapore 259771, Singapore; a0129822@u.nus.edu.

[5] Romanika Okraszewska, Aleksandra Romanowska, Marcin Wołek, Jacek Oskarbski, Krystian Birr and Kazimierz Jamroz ,Gdansk University of Technology, Poland; mwol@wp.pl, 11 February 2018.

[6] Wefering, F.; Rupprecht, S.; Bührmann, S.; Böhler-Baedeker, S.; Granberg, M.; Vilkuna, J.; Saarinen, S.; Backhaus,W.; Laubenheimer, M.; Lindenau, M.; et al. Title: "Guidelines. Developing and Implementing a Sustainable Urban Mobility Plan," European Commission: Brussels, Belgium, 2014.

[7] Banister, D., "The sustainable mobility paradigm," Transp. Policy 2008, 15, 73–80. [CrossRef]

[8] European Commission, "A Concept for Sustainable Urban Mobility Plans," European Commission: Brussels, Belgium, 2013.

[9] Vanshika Madan, "Cybersecurity: A Key to Organizational Success," https://isg-one.com/articles/cybersecurity-a-key-to-organizational-success,2021.

[10] 2021Global Threat Report, https://www.crowdstrike.com/resources/reports/global-threat-report/, 2021.

[11] NIST, “Best Practices in Cyber Supply Chain Risk Management Conference Materials”, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Vendor-Selection-and-Management.pdf, 2021.

[12] NHTSA, “Cybersecurity Best Practices for Modern Vehicles” https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf, 2016.

[13] SAE and Synopsis Independent Study, “Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices”, https://www.sae.org/binaries/content/assets/cm/content/topics/cybersecurity/securing_the_modern_vehicle.pdf.

[14] ENISA Threat landscape for Supply Chain Attacks Report, July 2021.