Frontiers in Emerging Computer Science and Information Technology (Open Access)

Volume 03, Issue 07, July 2026,
Publish Date: 14-07-2026
Page No.08-14

Safeguarding Next-Generation Transportation Systems: Digital Threats in Connected Automotive Networks

Dr. Liam Carter
Department of Computer Science, University of Toronto, Canada

ABSTRACT

The rapid evolution of next-generation transportation systems, characterized by interconnected automotive networks and digital infrastructures, has introduced unprecedented efficiencies and capabilities in mobility ecosystems. However, this transformation has simultaneously expanded the cyber threat landscape, exposing critical vulnerabilities within vehicle-to-everything (V2X) communication, embedded systems, and cloud-integrated automotive platforms. This research paper investigates the nature, scope, and implications of digital threats in connected automotive environments, emphasizing the need for robust cybersecurity frameworks tailored to complex, system-of-systems architectures.

Drawing upon systems engineering principles and existing competency models, this study critically analyzes how integration challenges, architectural dependencies, and data-driven functionalities contribute to emerging risks. The research synthesizes insights from transportation system development frameworks, distributed mapping technologies, and GPS-based data processing methodologies to contextualize vulnerabilities in real-world operational settings. Furthermore, it examines how large-scale integration and interoperability demands intensify exposure to cyberattacks, including data breaches, spoofing, and system manipulation.

The study proposes a multi-layered security approach grounded in systems engineering methodologies, emphasizing resilience, adaptability, and lifecycle-based protection strategies. By incorporating competency-driven frameworks and process-oriented security models, the research identifies key gaps in current practices and outlines pathways for strengthening cybersecurity governance in advanced transportation ecosystems.

The findings highlight that safeguarding next-generation transportation systems requires not only technological solutions but also organizational readiness, interdisciplinary collaboration, and continuous adaptation to evolving threat vectors. This paper contributes to the academic discourse by bridging the gap between systems engineering and cybersecurity in the automotive domain, offering a comprehensive perspective on securing future mobility infrastructures.

KEYWORDS: Connected Vehicles, Automotive Cybersecurity, Systems Engineering, V2X Communication, Digital Threats, Intelligent Transportation Systems, Network Security, Smart Mobility, Embedded Systems, Cyber-Physical Systems.

INTRODUCTION

The transformation of transportation systems into digitally interconnected ecosystems represents one of the most significant technological advancements of the 21st century. Modern vehicles are no longer isolated mechanical units; instead, they function as integral components of broader cyber-physical systems that incorporate communication networks, cloud computing platforms, and real-time data analytics. This paradigm shift, often referred to as next-generation transportation systems, has enabled innovations such as autonomous driving, real-time traffic management, and predictive maintenance. However, the integration of these technologies has also introduced complex cybersecurity challenges that demand rigorous academic and practical attention.

The foundational concept of interconnected transportation systems is deeply rooted in systems engineering principles, where multiple subsystems interact within a unified architecture. As highlighted in large-scale system integration frameworks, managing interdependencies and ensuring seamless communication among components is inherently challenging (Muller, 2007). These challenges are further exacerbated by the increasing reliance on digital communication protocols and data-

driven decision-making processes. Consequently, vulnerabilities in one subsystem can propagate across the entire network, leading to systemic risks.

A critical aspect of this transformation lies in the adoption of vehicle-to-everything (V2X) communication technologies, which facilitate data exchange between vehicles, infrastructure, and external systems. While V2X enhances operational efficiency and safety, it also creates multiple entry points for malicious actors. For instance, GPS-based navigation and mapping systems, which rely on continuous data streams, are susceptible to spoofing and data manipulation attacks (Bruntrup et al., 2005; Guo et al., 2007). These vulnerabilities highlight the inherent tension between connectivity and security in modern transportation systems.

The problem is further compounded by the increasing complexity of software and hardware integration within vehicles. Contemporary automotive systems incorporate numerous embedded components, each with distinct functionalities and communication interfaces. Ensuring the security of such heterogeneous systems requires a comprehensive understanding of system integration processes and competency frameworks (Cowper et al., 2005; Systems and Software Consortium, 2005). However, existing approaches often lack the adaptability required to address rapidly evolving cyber threats.

From a strategic perspective, national and international initiatives have recognized the importance of developing secure transportation infrastructures. Programs such as the Next Generation Air Transportation System emphasize the need for coordinated planning, workforce development, and technological innovation (Joint Planning and Development Office, 2007; National Academy of Public Administration, 2008). Although these initiatives primarily focus on aviation, their underlying principles are equally applicable to automotive systems, particularly in terms of system integration and risk management.

The relevance of this research is underscored by the increasing frequency and sophistication of cyberattacks targeting transportation systems. Incidents involving unauthorized access, data breaches, and system manipulation have demonstrated the potential consequences of inadequate security measures. These threats not only compromise individual vehicle safety but also pose significant risks to public infrastructure and national security.

This study aims to address the following objectives: first, to analyze the key digital threats associated with connected automotive networks; second, to evaluate the role of systems engineering in mitigating these threats; and third, to propose a comprehensive framework for enhancing cybersecurity in next-generation transportation systems. The scope of this research encompasses both theoretical and practical dimensions, integrating insights from existing literature with conceptual models and analytical frameworks.

The significance of this study lies in its interdisciplinary approach, which bridges the gap between systems engineering and cybersecurity. By examining the interplay between technological innovation and security challenges, the research provides a holistic perspective on safeguarding future mobility systems. Furthermore, it contributes to the development of resilient and adaptive security strategies that can address the dynamic nature of cyber threats in connected automotive environments.

LITERATURE REVIEW

The existing body of literature on next-generation transportation systems and cybersecurity reveals a strong emphasis on systems engineering principles, integration challenges, and data-driven methodologies. A critical examination of the provided references highlights the interdisciplinary nature of this domain, where technological innovation intersects with organizational competencies and process frameworks.

Systems engineering competency frameworks play a central role in understanding the complexities of large-scale system integration. Cowper et al. (2005) propose a structured approach to defining core competencies required for effective systems engineering, emphasizing the importance of interdisciplinary knowledge and integration skills. Similarly, the Systems and Software Consortium (2005) introduces a competency model that underscores the need for standardized practices in managing complex systems. These frameworks are particularly relevant in the context of connected automotive networks, where multiple subsystems must operate cohesively.

The challenges associated with system integration are further explored by Muller (2007), who identifies key issues in managing large and complex environments. The study highlights the difficulties in ensuring interoperability and reliability, particularly when dealing with heterogeneous components. Cowper, Emes, and Smith (2004) extend this analysis by proposing a process model for systems integrators, emphasizing the need for structured methodologies to manage integration risks. These insights are crucial for understanding the vulnerabilities inherent in interconnected automotive systems.

In addition to integration challenges, the literature also addresses the role of data-driven technologies in transportation systems. Research on GPS-based mapping and data processing provides valuable insights into the operational aspects of connected vehicles. Bruntrup et al. (2005) and Guo et al. (2007) explore methods for generating accurate maps using GPS traces, highlighting the importance of data integrity and reliability. Similarly, Shi et al. (2006) examine data processing techniques in vehicle-based surveying, emphasizing the need for robust data validation mechanisms. These studies implicitly reveal potential

security vulnerabilities, particularly in the context of data manipulation and spoofing.

The development of transportation systems at a national level is addressed in strategic frameworks such as the Next Generation Air Transportation System (Joint Planning and Development Office, 2007). This initiative emphasizes coordinated planning, technological innovation, and workforce development as key factors in building resilient transportation infrastructures. The National Academy of Public Administration (2008) further highlights the importance of identifying and developing the workforce required to support such systems. These perspectives underscore the need for a holistic approach to cybersecurity, encompassing both technical and organizational dimensions.

Another significant aspect of the literature is the focus on software engineering and process standardization. The Graduate Software Engineering Reference Curriculum (Stevens Institute of Technology, 2008) provides a comprehensive framework for developing software engineering competencies, which are essential for designing secure automotive systems. Kepchar (1994) and Armstrong (2006) emphasize the importance of integrating systems engineering practices into existing programs, highlighting the need for continuous improvement and adaptation.

Despite the extensive research on systems engineering and transportation technologies, there are notable gaps in the literature. Specifically, there is a lack of comprehensive frameworks that explicitly address cybersecurity in connected automotive networks. While existing studies provide valuable insights into integration challenges and data processing methodologies, they often do not consider the security implications of these technologies. Furthermore, there is limited research on the interplay between organizational competencies and cybersecurity practices.

This study seeks to address these gaps by integrating insights from systems engineering, data-driven technologies, and transportation frameworks to develop a comprehensive understanding of digital threats in connected automotive networks. By synthesizing the existing literature, the research aims to provide a foundation for developing robust cybersecurity strategies tailored to next-generation transportation systems.

METHODOLOGY

The emergence of connected automotive networks is fundamentally rooted in the evolution of cyber-physical systems, where physical components interact with computational and communication infrastructures. These systems integrate sensing, processing, and actuation capabilities, enabling vehicles to communicate with external entities such as infrastructure, other vehicles, and centralized platforms. From a systems engineering perspective, such architectures represent complex system-of-systems environments, where each subsystem maintains operational independence while contributing to collective functionality (Office of the Deputy Under Secretary of Defense for Acquisition and Technology, 2008).

The theoretical foundation of these networks is based on interoperability, modularity, and scalability. Interoperability ensures seamless communication across heterogeneous systems, while modularity allows individual components to be developed and upgraded independently. Scalability supports the expansion of network capabilities without compromising performance. However, these design principles inherently introduce security challenges, as increased connectivity expands the attack surface.

A critical component of connected automotive systems is the reliance on distributed data processing. Technologies such as real-time map generation and GPS-based navigation systems enable dynamic decision-making within vehicles. Studies on distributed mapping systems highlight the importance of scalable and real-time data processing architectures (Davies et al., 2006). However, the decentralized nature of these systems complicates the implementation of centralized security controls, thereby increasing vulnerability to cyber threats.

Furthermore, the integration of communication protocols such as V2X introduces multiple layers of interaction, each with distinct security requirements. These layers include physical communication channels, network protocols, and application-level services. Ensuring security across these layers requires a comprehensive approach that addresses both technical and organizational factors.

Architecture of Next-Generation Transportation Systems

Next-generation transportation systems are characterized by multi-layered architectures that integrate hardware, software, and communication networks. These architectures typically consist of onboard vehicle systems, roadside infrastructure, cloud platforms, and user interfaces. Each layer performs specific functions while interacting with others to enable seamless operation.

At the vehicle level, embedded systems control critical functions such as braking, steering, and engine management. These systems are interconnected through internal networks, such as Controller Area Networks (CAN), which facilitate communication between components. While these networks enhance functionality, they also introduce potential entry points for cyberattacks. Unauthorized access to internal networks can compromise vehicle safety and operational integrity.

The infrastructure layer includes traffic management systems, smart signals, and communication gateways. These components collect and process data from multiple sources, enabling real-time traffic optimization. However, their reliance on external communication networks exposes them to threats such as denial-of-service attacks and data interception.

Cloud-based platforms play a crucial role in data storage and analytics. They enable advanced functionalities such as predictive maintenance and route optimization by processing

large volumes of data. However, the centralization of data in cloud environments creates attractive targets for cybercriminals, increasing the risk of data breaches.

From a systems engineering perspective, managing these interconnected layers requires robust integration frameworks. The concept of "by-default" systems integration emphasizes the need for standardized processes to ensure compatibility and reliability (Cowper et al., 2004). However, these frameworks must be extended to incorporate security considerations, as traditional integration approaches often prioritize functionality over protection.

Digital Threat Landscape in Connected Automotive Systems

The digital threat landscape in connected automotive systems is diverse and continuously evolving. Cyber threats can be broadly categorized into data-centric, network-centric, and system-level attacks, each targeting different components of the transportation ecosystem.

Data-centric threats primarily involve the manipulation or interception of information. GPS spoofing is a prominent example, where attackers transmit false signals to mislead navigation systems. Research on GPS data processing highlights the reliance of transportation systems on accurate data inputs, making them vulnerable to such attacks (Shi et al., 2006; Zhu et al., 2003). Data integrity is therefore a critical concern, as compromised information can lead to incorrect decision-making.

Network-centric threats target communication channels between system components. These include eavesdropping, man-in-the-middle attacks, and denial-of-service attacks. The distributed nature of automotive networks amplifies these risks, as multiple communication pathways must be secured simultaneously.

System-level threats involve the exploitation of vulnerabilities within software and hardware components. These attacks can compromise critical vehicle functions, leading to potentially catastrophic consequences. The complexity of modern automotive systems, combined with the integration of third-party components, increases the likelihood of such vulnerabilities.

An important aspect of the threat landscape is the role of human factors. Inadequate training, lack of awareness, and insufficient organizational policies can exacerbate security risks. Competency models in systems engineering emphasize the importance of skilled personnel in managing complex systems (Gelosh; Cowper et al., 2005). However, the integration of cybersecurity competencies into these models remains limited.

Systems Engineering Approach to Automotive Cybersecurity

Systems engineering provides a structured framework for addressing the complexities of automotive cybersecurity. By focusing on the entire lifecycle of a system, this approach enables the identification and mitigation of risks at various stages, from design to deployment and maintenance.

A key principle of systems engineering is the integration of security considerations into the design phase. This proactive approach, often referred to as "security by design," ensures that vulnerabilities are addressed before they can be exploited. Process models for systems integration emphasize the importance of early risk assessment and continuous monitoring (Cowper et al., 2004).

Another important aspect is the use of competency frameworks to guide the development of skilled professionals. The Systems Engineering Competency Model (Systems and Software Consortium, 2005) highlights the need for interdisciplinary expertise, including knowledge of cybersecurity principles. By aligning workforce development with technological requirements, organizations can enhance their ability to manage security risks.

The concept of system-of-systems engineering is particularly relevant in the context of connected automotive networks. This approach recognizes that individual systems must operate independently while contributing to a larger ecosystem. Managing security in such environments requires coordination across multiple stakeholders, including manufacturers, service providers, and regulatory bodies.

Furthermore, systems engineering emphasizes the importance of validation and verification processes. These processes ensure that systems meet specified requirements and perform as intended. In the context of cybersecurity, validation involves testing systems against potential threats, while verification ensures compliance with security standards.

Data-Driven Vulnerabilities and GPS-Based Systems

Data-driven technologies are central to the functionality of connected automotive systems, enabling real-time decision-making and adaptive behavior. However, their reliance on continuous data streams introduces significant vulnerabilities.

GPS-based systems, in particular, are susceptible to various forms of attack. Research on map generation and GPS data processing highlights the complexity of these systems and their dependence on accurate data inputs (Bruntrup et al., 2005; Guo et al., 2007). Any disruption or manipulation of data can have cascading effects on system performance.

One of the primary vulnerabilities is data spoofing, where attackers inject false information into the system. This can lead to incorrect navigation decisions, potentially endangering passengers and infrastructure. Additionally, data interception can compromise user privacy, as sensitive information such as location and travel patterns may be exposed.

Another challenge is the integration of data from multiple sources. While this enhances system functionality, it also increases the risk of inconsistencies and errors. Ensuring data

integrity requires robust validation mechanisms and secure communication protocols.

From a theoretical perspective, these vulnerabilities highlight the limitations of current data processing frameworks. While existing models focus on efficiency and scalability, they often overlook security considerations. Addressing this gap requires the development of integrated frameworks that balance performance and protection.

Organizational and Workforce Challenges in Cybersecurity Implementation

The implementation of effective cybersecurity measures in connected automotive systems is not solely a technical challenge; it also involves significant organizational and workforce considerations. The complexity of these systems requires a multidisciplinary approach, where expertise in engineering, cybersecurity, and management must be integrated.

Workforce development is a critical factor in ensuring the success of cybersecurity initiatives. Strategic reports emphasize the importance of identifying and training personnel capable of managing advanced transportation systems (National Academy of Public Administration, 2008). However, there is often a gap between the skills required and those available in the workforce.

Organizational structures also play a crucial role in cybersecurity implementation. Effective coordination between different departments and stakeholders is essential for managing risks. However, fragmented organizational structures can hinder communication and decision-making, increasing the likelihood of security breaches.

Another challenge is the integration of cybersecurity into existing systems and processes. Many organizations rely on legacy systems that were not designed with security in mind. Retrofitting these systems to meet modern security standards is both complex and costly.

Competency frameworks provide a valuable tool for addressing these challenges. By defining the skills and knowledge required for effective systems engineering, these frameworks can guide workforce development and organizational planning (Cowper et al., 2005). However, they must be updated to reflect the evolving nature of cybersecurity threats.

RESULTS / FINDINGS

The analysis of connected automotive networks reveals that cybersecurity vulnerabilities are deeply embedded within the structural and functional design of next-generation transportation systems. One of the primary findings is that increased interconnectivity significantly amplifies the attack surface, making systems more susceptible to multi-layered cyber threats. The integration of V2X communication, cloud platforms, and embedded systems introduces numerous access points, each requiring dedicated security mechanisms.

A critical observation is the strong correlation between system complexity and vulnerability exposure. As systems evolve into large-scale, system-of-systems architectures, managing interdependencies becomes increasingly challenging. This complexity often leads to gaps in security coverage, particularly at integration points where different subsystems interact. Existing systems engineering frameworks provide a foundation for addressing these challenges, but they often lack explicit mechanisms for cybersecurity integration (Muller, 2007; Cowper et al., 2004).

The findings also highlight the significant role of data integrity in ensuring system reliability. GPS-based systems and real-time data processing technologies are essential for modern transportation functionalities; however, they are highly vulnerable to spoofing and manipulation attacks. Studies on GPS data processing demonstrate that even minor disruptions in data accuracy can lead to substantial operational failures (Bruntrup et al., 2005; Shi et al., 2006). This underscores the need for robust data validation and authentication mechanisms.

Another important result is the identification of organizational and workforce-related challenges. The lack of adequately trained personnel and the absence of standardized cybersecurity practices contribute to increased risk levels. Competency frameworks emphasize the importance of interdisciplinary skills, but current implementations often fail to incorporate cybersecurity as a core component (Systems and Software Consortium, 2005; Cowper et al., 2005).

Furthermore, the research indicates that existing security approaches are predominantly reactive rather than proactive. Many systems rely on post-deployment security measures, which are insufficient in addressing sophisticated cyber threats. The concept of “security by design” is recognized as a critical requirement, yet its adoption remains limited across the industry.

Overall, the findings suggest that safeguarding next-generation transportation systems requires a holistic approach that integrates technical, organizational, and strategic dimensions. The absence of such integration poses significant risks to system reliability, user safety, and infrastructure integrity.

DISCUSSION

The findings of this study provide important insights into the challenges and opportunities associated with cybersecurity in connected automotive networks. A key implication is that traditional security models are inadequate for addressing the dynamic and complex nature of next-generation transportation systems. The shift towards interconnected and data-driven architectures necessitates a re-evaluation of existing approaches, with a focus on adaptability and resilience.

From a theoretical perspective, the integration of systems engineering and cybersecurity emerges as a critical requirement. Systems engineering frameworks offer valuable tools for managing complexity and ensuring system reliability; however,

they must be extended to incorporate security considerations at every stage of the system lifecycle. This aligns with the concept of system-of-systems engineering, which emphasizes the need for coordinated management of independent yet interconnected systems (Office of the Deputy Under Secretary of Defense for Acquisition and Technology, 2008).

The discussion also highlights the importance of data-centric security strategies. Given the reliance on real-time data processing, ensuring data integrity and authenticity is essential for maintaining system functionality. The vulnerabilities identified in GPS-based systems illustrate the potential consequences of inadequate data protection. Addressing these challenges requires the development of advanced cryptographic techniques and secure communication protocols.

Another significant implication is the role of organizational and human factors in cybersecurity implementation. Technical solutions alone are insufficient without the support of skilled personnel and effective governance structures. The gap between required and available competencies represents a major barrier to achieving robust security. This underscores the need for comprehensive training programs and the integration of cybersecurity into existing competency frameworks.

However, the study also identifies several limitations. The reliance on existing literature restricts the scope of empirical validation, and the absence of real-world case studies limits the ability to generalize findings. Additionally, the rapidly evolving nature of cyber threats means that proposed solutions may require continuous adaptation.

Despite these limitations, the research contributes to a deeper understanding of the interplay between connectivity and security in modern transportation systems. It emphasizes the need for interdisciplinary collaboration and continuous innovation to address emerging challenges. By aligning theoretical frameworks with practical requirements, the study provides a foundation for developing more resilient and secure automotive networks.

CONCLUSION

This research has examined the critical issue of cybersecurity in next-generation transportation systems, with a specific focus on connected automotive networks. The study highlights that while technological advancements have significantly enhanced mobility and efficiency, they have also introduced complex vulnerabilities that cannot be addressed through conventional security approaches.

A key contribution of this research is the integration of systems engineering principles with cybersecurity strategies. By adopting a holistic perspective, the study demonstrates that effective security requires consideration of technical architectures, data integrity, organizational structures, and workforce competencies. The findings underscore the importance of proactive approaches, such as security by design, in mitigating risks and ensuring system resilience.

The research also identifies significant gaps in existing practices, particularly in the areas of data protection, system integration, and workforce development. Addressing these gaps requires coordinated efforts from industry stakeholders, policymakers, and academic institutions. The development of standardized frameworks and competency models is essential for building a robust cybersecurity ecosystem.

Looking forward, future research should focus on empirical validation of proposed frameworks and the exploration of emerging technologies such as artificial intelligence and blockchain in enhancing automotive cybersecurity. Additionally, the integration of real-world case studies can provide valuable insights into practical challenges and solutions.

In conclusion, safeguarding next-generation transportation systems is a multifaceted challenge that demands continuous innovation and collaboration. By bridging the gap between systems engineering and cybersecurity, this study contributes to the development of secure and resilient mobility infrastructures capable of supporting future technological advancements.

REFERENCES

1. Armstrong, J., "Giving the Integrator Role a Sporting Chance", INCOSE, 2006
2. Cowper, D., (et al), "Systems Engineering Core Competencies Framework". INCOSE UK, 2005
3. Cowper, D., Emes, M, Smith, A., ""is he in heaven or is he in hell that illusive Systems Integrator?" - Who's Looking After Your Systems Integration?
4. Cowper, D., Emes, M, Smith, A., "A Systems Engineering Process Model for 'By Default' Systems Integrators", INCOSE, 2004
5. Federal Aviation Agence, ATO Operations Planning "National Airspace System Systens Engineering Manual", , October 11, 2006
6. Gelosh, D., Development and Validation of a Systems Engineering Competency Model, Undated briefing
7. Joint Planning and Development Office, "Concept of Operations for the Next Generations Air Transportation System, Version 2.0", 13 June, 2007
8. Jonathan J. Davies, Alastair R. Beresford, Andy Hopper, “Scalable, Distributed, Real-Time Map Generation,” IEEE Pervasive Computing, vol. 5, no. 4, pp. 47–54, Oct.–Dec. 2006
9. Kepchar, K.J., "Breathing SE Life into Existing DOD Programs", INCOSE, 1994
10. Muller, G., "Coping With System Integration Challenges in Large Complex Environments", INCOSE, 2007
11. National Academy of Public Adminitration, "Volume 2: Identifying the Workforce to Respond to a National

Imperative .The Next Generation Air Transportation System (NestGen)", September 2008
12. Office of the Deputy Under Secretary of Defense for Acquisition and Technology, "Systems and Software Engineering. Systems Engineering Guide for Systems of Systems, Version 1.0." Washington, DC: ODUSD(A&T)SSE, 2008.
13. R. Bruntrup, S. Edelkamp, and S. Jabbar, “Incremental map generation with GPS traces ”, Proc. of the 8th IEEE Intelligent Transportation Systems Conf, Vienna, Austria, 2005, pp. 413–418.
14. Rogers, S., Langley, P., Wilson, C., “Mining GPS data to augment Knowledge Discovery and Data Mining (pp. 104–113). San Diego, CA : ACM Press. 1999
15. S. Shi, Z. Lü, H. Chen and D. Zhao, “Data processing technology in road surveying by vehicle-borne GPS ”, Journal of Zhengzhou Institute of Surveying and Mapping, vol. 23, no. 4, August 2006, pp. 275–277, 283. (in Chinese)
16. Squires, A., Larson, W., Sauser, B., "MAPPING SPACE-BASED SYSTEMS ENGINEERING CURRICULUM TO NASA-INDUSTRY DEVELOPED COMPETENCIES FOR IMPROVED ORGANIZATIONAL PERFORMANCE"
17. Stevens Institute of Technology, "Graduate Software Engineering Reference Curriculum [GSwERC], Version 0.50", October 31, 2008
18. Systems and Software Consortium, "SSCI Competency Model v1.0", 8/31/2005
19. T. Guo, K. Iwamura, and M. Koga, “Towards high accuracy road maps generation from massive GPS traces data ”, Proc. of IGARSS, 2007, pp. 667–670.
20. Z. Zhu, Q. Wang and D. Wan, “A study on automatic generation road center-lines algorithm based on road contour ”, Journal of Image and Graphics, vol. 8(A), no. 7, 2003, pp. 792–797. (in Chinese)