APPLYING SAFETY-CRITICAL FAULT TOLERANT PRINCIPLES TO SURVIVABLE TRANSPORTATION CONTROL NETWORKS

FINAL REPORT

FEBRUARY 2006

Budget Number KLK233

N06-06

Prepared for

OFFICE OF UNIVERSITY RESEARCH AND EDUCATION

U.S. DEPARTMENT OF TRANSPORTATION

Prepared by

NATIONAL INSTITUTE FOR ADVANCED TRANSPORTATION TECHNOLOGY

UNIVERSITY OF IDAHO

Paul Oman and Axel Krings

With assistance from Brian Johnson and Ahmed Abdel-Rahim

DISCLAIMER

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the Department of Transportation, University Transportation Centers Program, in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof.

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Applying Safety-Critical Fault Tolerant Principles to Survivable Transportation Control Networks		5. Report Date February 2006
Author(s) Paul Oman, Axel Krings, with assistance from Brian Johnson and Ahmed-Abdel Rahim		6. Performing Organization Code *KLK233*
9. Performing Organization Name and Address National Institute for Advanced Transportation Technology University of Idaho PO Box 440901; 115 Engineering Physics Building Moscow, ID 838440901		8. Performing Organization Report No. *N06-06* 10. Work Unit No. (TRAIS)
12. Sponsoring Agency Name and Address US Department of Transportation Research and Special Programs Administration 400 7th Street SW Washington, DC 20509-0001		11. Contract or Grant No. *DTRS98-G-0027* 13. Type of Report and Period Covered Final Report: August 2004- December 2005
Supplementary Notes:		14. Sponsoring Agency Code *USDOT/RSPA/DIR-1*

16. Abstract

This project attempted to address the survivability of intelligent traffic control systems, with a special focus on "Design for Survivability." We feel that the city of Moscow Intelligent Transportation System (ITS) project offered a unique window of opportunity to study survivability concepts as applied to complex, real-time traffic control networks. Within the national initiative to analyze the extent of vulnerabilities of critical infrastructures to cyber treats, this research attempts to integrate the design concepts of survivability into an ITS. Under normal traffic conditions, network operation is optimized for system-wide objective functions (i.e., minimize network-wide delay or maximize throughput) and system users modify their behavior accordingly by altering their departure time, travel route, or mode of travel. However, when the system is operating under extreme events (e.g., overloaded, damaged, or impacted by accidents and weather conditions) system optimization and dynamics become much more complex due to the interaction between system users, network controls, communication networks and the physical infrastructure. These interactions are not well understood. This project explored methods to model this problem via simulation and graph theory, with layers for communication, control and physical infrastructures. The results are several analyses of the Moscow ITS project, documented in two papers and one technical report.

17. Key Words	18. Distribution Statement
information technology, safety and security, survival; reliability, complex systems, intelligent transportation systems, prevention; traffic information systems	Unrestricted; Document is available to the public through the National Technical Information Service; Springfield, VT.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	31	…

Form DOT F 1700.7 (8-72)

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This project attempted to address the survivability of intelligent traffic control systems, with a special focus on "Design for Survivability." We feel that the city of Moscow Intelligent Transportation System (ITS) project offered a unique window of opportunity to study survivability concepts as applied to complex, real-time traffic control networks. Within the national initiative to analyze the extent of vulnerabilities of critical infrastructures to cyber treats, this research attempts to integrate the design concepts of survivability into an ITS.

Under normal traffic conditions, network operation is optimized for system-wide objective functions (i.e., minimize network-wide delay or maximize throughput) and system users modify their behavior accordingly by altering their departure time, travel route, or mode of travel. However, when the system is operating under extreme events (e.g., overloaded, damaged, or impacted by accidents and weather conditions) system optimization and dynamics become much more complex due to the interaction between system users, network controls, communication networks and the physical infrastructure. These interactions are not well understood. This project explored methods to model this problem via simulation and graph theory, with layers for communication, control and physical infrastructures. The results are several analyses of the Moscow ITS[1] project, documented in two papers and one technical report.

[1] City of Moscow ITS Projects—Traffic Signal Systems Integration and Deployment, Projects ITS-SPR-002(012) and ITS-SPR-0002(021), funded by Federal Highway Administration through the Idaho Transportation Department

APPROACH AND METHODOLOGY

Description of Problem

Malicious attacks on computing systems and networks have grown drastically over the last decade and have reached epidemic proportions. In 2002 the Computer Emergency Response Team (CERT) alone reported over 4,000 vulnerabilities resulting in more that 80,000 reported intrusion incidents, casting a shadow on the successes claimed in computer and network security research. Yet despite this paradox of increasing security and intrusion, our society has fully embraced computer and network technology for control of our critical infrastructures. As the CERT data shows, the probability of cyber intrusion and attack on an infrastructure control system is increasing. With the introduction of and increasing reliance on networked technologies in modern traffic management systems, all attached networked devices are susceptible to malicious cyber attacks.

Traffic control systems, and the transportation infrastructure in general, were not designed with malicious acts in mind, and neither were the computers and networks controlling them. To the contrary, these complex systems have been engineered in a relatively benign environment over decades of optimizing dependability parameters such as reliability, safety, availability or maintainability. Given the cyber threats to the control infrastructures, ranging from recreational hackers to foreign government sponsored cyber terrorism, a basic shift in design and operations philosophy is necessary. It is imperative that we move from "Design for Dependability" to "Design for Survivability." This means that transportation control infrastructures should be designed and operated so that essential services will survive even in the presence of malicious faults, intrusions, and attacks. Further, a system designed for survivability will maintain safe operations as long as possible, and in the end fail in a predefined safe mode of operation.

Cyber attacks and electronic sabotage targeted against vulnerabilities have the capability of inducing transportation disruptions over very large geographic areas. Loss of life, property,

production and service may result from those outages. With the financial support of the National Institute of Standards and Technology (NIST) we have concluded a two-year study of similar vulnerabilities with the electric power infrastructure. Concurrently, we have been studying security and survivability issues of transportation control networks and have come to the conclusion that the transportation and electric power infrastructure share many of the underlying threats and vulnerabilities as well as possible solutions. The research community generally agrees that survivability can be significantly improved by applying the combined principles of fault-tolerance and computer and network security.

Research in ultra-reliable systems design has produced complex computing and control systems with combined system reliabilities far exceeding the reliabilities of the individual components. Such systems have been successfully implemented in safety critical control applications such as fly-by-wire aircraft. It is important to note that different fault sources have been considered in the overall design, with typical fault assumptions ranging from benign hardware or software faults to malicious, i.e. asymmetric, faults. We have evidence that some of these technologies can be adapted to current traffic control networks and system. When combining these principles from ultra-dependable systems with principles from security and survivability, truly survivable systems can be designed allowing essential services to survive even in the presence of malicious attacks from hackers or cyber terrorists.

The integration of survivability features can be seen as

1. Part of the design specification and process or
2. As an augmentation to an existing system in order to increase survivability.

The first option is highly desirable, as it allows for the design for survivability. The latter option is of interest if little or no change to the existing infrastructure is mandated. Examples of both types of survivability design are possible within the Moscow ITS project, including fiber optic cable routing, communications protocols linking traffic controllers, placement and networking of system detection devices and CCTV cameras. This study continues our analyses of the Moscow ITS project, with the aim of developing quantitative methods for assessing the security and survivability of complex automated traffic control systems.

Project Objectives, Tasks and Results

The six specific objectives of the research project are listed below, along with the specific task relating to each objective and a synopsis of the results from that activity:

1. Determine the similarities between ultra-reliable actuator control networks in avionics systems to intelligent traffic control networks.

   Task: Analysis of existing transportation control networks through visitations, literature review, meetings with NIATT and representatives from the Idaho Transportation Department (ITD) and review of the city of Moscow ITS project.

   Results: Few existing studies were found, but published evidence demonstrates that ITS security and survivability is both a major concern and an open issue. During the specification of the ITS infrastructure model the need for the avoidance of single point of failures was recognized and addressed. Using basic reliability modeling, parallels to ultra reliable avionics systems were found which resulted in limiting the effect of single points of failures. Applying this approach was shown to improve ITS infrastructure reliability significantly, as shown in Appendix A.

2. Assess technology transfer from the area of ultra-dependable distributed systems to improve the survivability of transportation control networks.

   Task: *In situ* security and survivability assessments of actual control center and dispatch operations. This task has dual purposes: (1) To Attempt to perform an S/SSA and (2) To compare the intrusion scenarios and critical functionalities to a conceptual model of the city of Moscow ITS project.

   Results: Experience shows that static analysis of an ITS control center is procedurally equivalent to analyses of other infrastructure control centers (e.g., electric power and water).

3. Identify hybrid fault models suitable for traffic/transportation control networks.

Task: Analysis of transportation network topologies in order to determine the suitability of adapting standard fault models and classifications.

Results: A model was derived that captures the topology of the infrastructure graph. Based on this graph, formal analysis of the ITS can be conducted leading to the specification of new reliability and survivability measures. Whereas fail rates of communication links could be derived from data extracted from the engineering report, the impact of fail rates due to malicious act remain of concern.

Furthermore, it was determined that a combination of CMFA and S/SSA could be a valuable analytic tools with respect to ITS's. CMFA was used to enumerate common failure causes of system components, while S/SSA was used to identify component criticality and responsibility. Together, a comprehensive security and survivability analysis is possible.

4. Map fault models to the topologies and protocols of traffic/transportation control networks. Use Security/Survivability Systems Analysis (S/SSA) to formalize "soft-spot" analysis of traffic/transportation control networks, including identifications of essential services and intrusion scenarios.

   Task: Adaptation of S/SSA procedures to accommodate domain specific characteristics of transportation control networks.

   Results: A draft vulnerability analysis with respect to security and survivability of the proposed City of Moscow ITS was compiled. It is attached as Appendix B.

5. Apply the concept of Design for Survivability to traffic control systems, with special focus on the city of Moscow ITS project.

   Task: A survivability architecture based on the city of Moscow ITS project, identifying the security and survivability features of the infrastructure as well as the analysis of its survivability given typical intrusion scenarios.

Results: While a plethora of potential applications of InfoSec technology within the ITS domain were found, no new InfoSec technologies needed development.

6. Utilize the Moscow ITS as a case study to derive a functionality based model for survivable ITS control infrastructures.

   Task: Develop a model capable of representing the static functionalities of an ITS and, given that, derive optimal solutions to improve the reliability of the system.

   Results: It was determined that, by applying a functionality based model of an ITS with the goal of reducing vulnerabilities, it is possible to derive optimal mitigations to the vulnerabilities, including benign faults, through the principle of redundancy. Whereas the model captured only limited, readily available, parameters from the engineering report, it was shown that the model was scalable with respect to the infrastructure graph and the parameters.

Faculty and Student Involvement

The research project was conceptualized and conducted by principal investigators Drs. Paul Oman and Axel Krings, University of Idaho (UI) Computer Science Department., with guidance and assistance from Dr. Brian Johnson, UI Electrical and Computer Engineering Department., and Drs. Ahmed Abdel-Rahim and Michael Kyte, UI Civil Engineering Department. Other valuable assistance was obtained from several engineers from the Idaho Department of Transportation.

Several UI students were involved in the project, including Matt Benke, John Waite, Patrick Merry, Neil Nguyen, Matt Phillips, Jeannine Schmidt, Vishakh Nair, and Sean Melton. Their names appear on the publications resulting from this research project, listed in the next section.

Peer Reviewed Publications and Presentations Resulting From This Funding

The following papers are a direct or indirect result of the NAITT funding of this project and were accepted as peer reviewed publications in international research venues. They are listed in chronological order.

1. A. Abdel-Rahim, P. Oman, J. Waite, M. Benke, and A. Krings, "Integrating Network Survivability Analysis in Traffic Systems Design," presented at the *IEEE Intelligent Transportation Systems Safety and Security Conference*, (March 24-25, Miami, Florida), 2004.

2. F. Sheldon, T. Potok, A. Loebl, A. Krings and P. Oman, "Management of Secure and Survivable Critical Infrastructures Toward Avoiding Vulnerabilities," presented at the *Eighth IEEE International Symposium on High Assurance Systems Engineering*, (Mar. 25-26, Tampa, FL), 2004.

3. P. Oman, A. Krings, D. Conte de Leon, and J. Alves-Foss, "Analyzing the Security and Survivability of Real Time Control Systems," *Proceedings from the Fifth IEEE Systems, Man and Cybernetics Information Assurance Workshop*, (June 10-11, West Point, NY), IEEE Press, 2004, pp. 342-349.

4. M. Benke, J. Waite, P. Oman and A. Abdel-Rahim, "Survivable Systems Analysis for Real Time Control Systems in Critical Infrastructures," *Proceedings of the International Conference on Security and Management*, (June 21-24, Las Vegas, NV), CSREA Press, 2004, pp. 278-283.

5. J. Schmidt and V. Nair (with P. Oman and B. Johnson, advising), "A Taxonomy of Security Standards for Real-time Control Systems," *Proceedings of the 36th Annual North American Power Symposium*, University of Idaho, (August 9-10, Moscow, Idaho), 2004, pp. 59-66.

6. J. Waite, J. Oman, M. Phillips, S. Melton, and V. Nair (with P. Oman and B. Johnson, advising), "A SCADA Testbed for Teaching and Learning," *Proceedings of the 36th*

Annual North American Power Symposium, University of Idaho, (August 9-10, Moscow, Idaho), 2004, pp. 447-451.

7. J. Waite, M. Benke, N. Nguyen, M. Phillips, S. Melton, P. Oman, A. Abdel-Rahim, and B. Johnson, "A Combined Approach to ITS Vulnerability and Survivability Analyses," *Proceedings of the IEEE Intelligent Transportation Systems Council Symposium*, (October 3-6, Washington, DC), 2004.

8. Krings A. W., and Merry P. R., "A Functionality Based Hierarchical Model for Survivable Intelligent Transportation Systems," to appear in: Proc. *7th International IEEE Conference on Intelligent Transportation Systems*, October 3-6 Washington, DC, 2004.

FINDINGS; CONCLUSIONS; RECOMMENDATIONS

Our computerized control systems contain many potential sources of common mode failures including physical components, hardware circuitry, firmware and software. Automated transportation systems (and other critical infrastructures) must be hardened against those very vulnerabilities. The hardening process – against both physical and cyber attack – begins by modeling security and survivability characteristics within complex systems. In previous work we applied fault modeling and security/survivability assessment procedures to the electric power grid. In this project we apply those same techniques to transportation control networks. The resulting benefit, as demonstrated in the attached report (Appendix A), provides mitigation strategies and design parameters for more robust and survivable systems for advanced traffic operations and control.

Technologies generated by this project that have the potential for commercialization and/or institutionalization are also encapsulated in the example report. They include comprehensive checklists of physical and cyber vulnerabilities and corresponding mitigations, example stakeholder matrices and example communication network topological alternatives with differing security and survivability considerations. Institutionalization of these traffic/transportation-centric checklists, matrices and procedures can be implemented through a recognized state or local organization such as NIATT or ITD.

Technologies generated by this project that have the potential for commercialization and/or institutionalization include:

1. Traffic/Transportation control network security checklists and procedures.
2. Traffic/Transportation control network survivability maps and procedures.
3. Vulnerability and mitigation matrices, relative to traffic and transportation control networks.
4. S/SSA procedures applicable to traffic and transportation control systems.
5. Results from gap analyses conducted on traffic and transportation control systems.

Institutionalization of the traffic/transportation-centric checklists, maps and procedures could only be implemented through a recognized state or local organization such as NIATT or ITD. However, the vulnerability analyses and S/SSA procedures are of interest to a wide group of organizations and entities, including NIST, INEEL, PNNL, NSA and the new Office of Homeland Security. Further, commercial potential of new technologies identified through gap analyses would be of interest to all those organizations, plus all businesses involved in manufacturing control systems (e.g., Honeywell, GE, Siemens, SEL, etc.). All results and deliverables from the proposed project will be documented in technical reports and publications sufficient to recreate the procedures and artifacts. Commercialization and institutionalization of results will be coordinated through NIATT unless NIST has prior claim to those results.