A Qualitative Approach to Analyze the Security and Survivability of Critical Infrastructure Networks

Ahmed S. Abdel-Rahim, Bakr M. Aly Ahmed, and Ybette Ochoa-Huaman

***Abstract*—The paper presents a qualitative approach to analyze the security and survivability of critical infrastructure networks. The analysis identifies threat mitigation strategies for each threat identified and provides suggestions for improved security and survivability. The proposed approach could be applied during the planning and design phase of new projects to evaluate different design alternatives or to assess the vulnerability and survivability of an existing system. The paper presents the results of an in-depth interview survey conducted to identify the normal usage scenarios and possible attack scenarios and their impact on the operations of transportation management centers. The proposed approach provides a significant addition to the current design practices by integration system security and survivability in the design process. A cost-benefit analysis of the proposed mitigation strategies should provide transportation officials with a decision making tool to evaluate different design alternatives and to improve the overall survivability of urban city networks. While the case-study presented in the paper focused on urban transportation networks, the proposed qualitative approach presented can be applied to any other critical infrastructure distribution, control, and monitoring networks.**

***Index Terms*—Infrastructure networks, security and survivability, transportation management, urban transportation networks.**

I. Introduction

Critical infrastructure networks have been traditionally designed and operated based on engineering practices that emphasize issues like safety, system efficiency, and maintainability with little or no consideration to the issue of network security and survivability under natural disasters, accidents, malicious or extreme events. Given the increased threats to critical infrastructure networks, it is imperative that such systems be designed not only for safety and efficiency, but also for survivability to ensure that essential transportation services will survive even in the presence of malicious faults, intrusions, accidents, natural disasters, and attacks. Further, given the fact that more and more of the critical infrastructure networks can be remotely or automatically controlled via communication infrastructures, it is no longer sufficient to consider the analysis of the physical network, its power and control networks, and the communication infrastructure in separation.

In this paper, a modified Survivable System Analysis (SSA) that can be used to assess the security and survivability of critical infrastructure networks is presented. The qualitative technique presented in this paper is based on the canonical SSA, but modified for critical infrastructures by including the development of a stakeholder-by-responsibility matrix, the enumeration of both physical and cyber threats, and the development of a threat-by-component matrix. The analysis identifies threat mitigation strategies for each threat identified and provides suggestions for improved security and survivability.

II. Background

Several approaches to assessing a transportation system for its ability to maintain essential service have been used. However, most of these approaches and strategies have focused primarily on reliability using a variety of performance measures such as connectivity and terminal reliability, capacity reliability, and travel time/travel cost reliability [1]-[3]. While reliability serves as an adequate measure for assigning the probabilities of satisfying a fixed level of performance based on the presence of benign factors, it does not consider the weakness (vulnerability) of network operating under extreme conditions. Connectivity, or terminal reliability, is defined as “the probability that nodes are connected, such that it is possible to reach a destination from a given source [4].” While connectivity is a valid measure for some networked systems (e.g., power systems or sparsely used communications networks), it does not adequately reflect capacity constraints of different links on the network.

A more accurate measure in this sense is capacity reliability, which can be defined as “the probability that the network can accommodate a specific demand level” [5]. Capacity reliability, while accounts for the ability of a system to satisfy demand through adequate service, it does not exclusively indicate how well demand is satisfied. Travel time (or cost) reliability is defined as “the probability that a trip can be successfully finished within a specified time interval (or at less than a specified cost)” [6].

Survivability, while not commonly addressed in transportation literature, forms a prominent area of active research in networked systems. Carnegie-Mellon University’s Software Engineering Institute originated an analytic approach for networked systems referred to as the Survivable Systems Analysis (SSA) in 1997 [7]-[10]. An example of such research is the Disruption Impact Estimation Tool for Transportation (DIETT) presented in NCHRP report 525,

Manuscript received May 7, 2013; revised July 24, 2013.

Ahmed Abdel-Rahim and Ybette Ochoa-Huaman are with Department of Civil Engineering, University of Idaho, PO Box 440901, Moscow, ID 83844-0901, USA, (tele: 208-885-2957, 208-885-4043; e-mail: ahmed@uidaho.edu, ocho7243@uidaho.edu).

Bakr M. Aly Ahmed is with Department of Architecture, North Dakota State University, 650 NP Ave, Fargo, ND 58102, USA, tele: 701-231-5901 (e-mail: bakr.alyahmed@ndsu.edu).

DOI: 10.7763/IJET.2014.V6.666

[11], a tool for prioritizing high value Transportation Choke Points (TCP) according to their potential economic impact on the flow of commercial traffic.

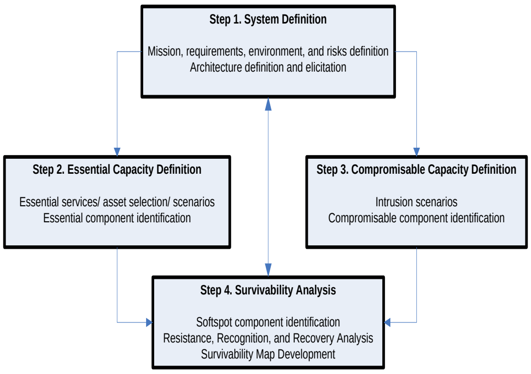
Step 1. System Definition
Mission, requirements, environment, and risks definition
Architecture definition and elicitation
Step 2. Essential Capacity Definition
Essential services/ asset selection/ scenarios
Essential component identification
Step 3. Compromisable Capacity Definition
Intrusion scenarios
Compromisable component identification
Step 4. Survivability Analysis
Softspot component identification
Resistance, Recognition, and Recovery Analysis
Survivability Map Development

Fig. 1-a. Canonical Survivable System Analysis (SSA).

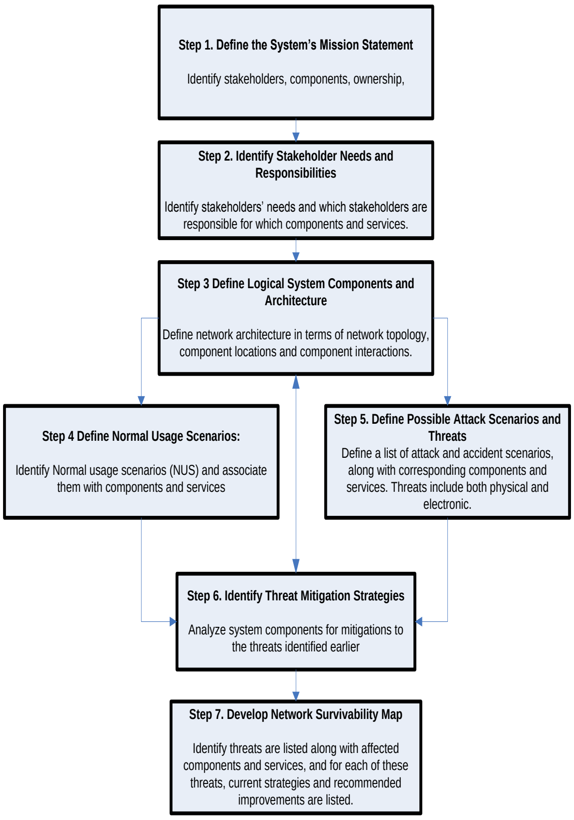
Step 1. Define the System's Mission Statement
Identify stakeholders, components, ownership,
Step 2. Identify Stakeholder Needs and Responsibilities
Identify stakeholders' needs and which stakeholders are responsible for which components and services.
Step 3 Define Logical System Components and Architecture
Define network architecture in terms of network topology, component locations and component interactions.
Step 4 Define Normal Usage Scenarios:
Identify Normal usage scenarios (NUS) and associate them with components and services
Step 5. Define Possible Attack Scenarios and Threats
Define a list of attack and accident scenarios, along with corresponding components and services. Threats include both physical and electronic.
Step 6. Identify Threat Mitigation Strategies
Analyze system components for mitigations to the threats identified earlier
Step 7. Develop Network Survivability Map
Identify threats are listed along with affected components and services, and for each of these threats, current strategies and recommended improvements are listed.

Fig. 1-b. Seven steps modified Survivable System Analysis (SSA).

The SSA–based qualitative technique presented in this paper modifies the canonical technique applied in survivable network analysis to make it applicable to critical infrastructures such as ITS networks. The three major modifications are: 1) including the development of a stakeholder-by-responsibility matrix, 2) the enumeration of both physical and cyber threats, and 3) the development of a threat-by-component matrix. The analysis identifies threat mitigation strategies for each threat identified and provides suggestions for improved security and survivability [12]-[14].

III. Qualitative Survivable Systems Analysis for ITS Networks

The combined security and survivability analysis process presented in this paper is based on the modified SSA process and defines seven steps, illustrated in Fig. 1-a and Fig. 1-b. The following subsections further describe each of these stages.

IV. Case Study: Traffic Management Centers

The objective of this part of the analysis was to identify typical normal usage scenarios and possible attack scenarios and their impact on traffic management centers (TMC) operations. Data were collected through phone interviews with 17 TMC operators throughout North America. An example of different components of an ITS system is presented in Figure 2. The Figure shows the Treasure Valley, Idaho ITS proposed architecture with several project components and communication architecture [15]. The multilayer representation of a typical ITS network is presented in Fig. 3 which shows three different infrastructure layers within the system: 1) power network layer, 2) communication network layer, and 3) physical (roadway) network layer. The figure also shows the failure propagation across layers that were used in the qualitative analysis presented in this paper.

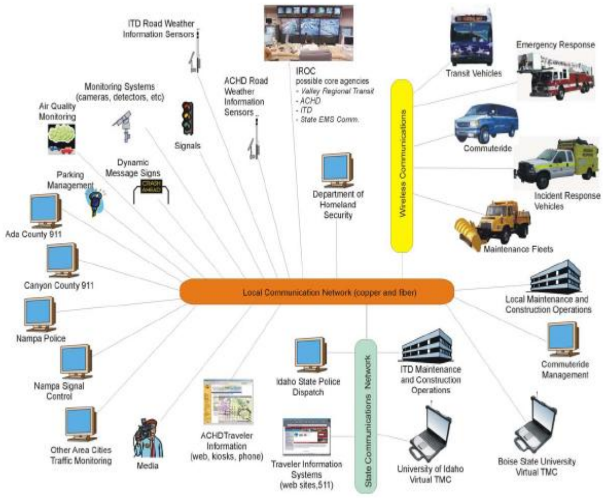
ITD Road Weather Information Sensors
IROC
possible core agencies
- Valley Regional Transit
- ACHD
- ITD
- State EMS Comm.
Transit Vehicles
Emergency Response
Monitoring Systems (cameras, detectors, etc)
Air Quality Monitoring
Signals
ACHD Road Weather Information Sensors
Commuteride
Dynamic Message Signs
Parking Management
Department of Homeland Security
Wireless Communications
Incident Response Vehicles
Ada County 911
Maintenance Fleets
Canyon County 911
Local Communication Network (copper and fiber)
Local Maintenance and Construction Operations
Nampa Police
Nampa Signal Control
Idaho State Police Dispatch
ITD Maintenance and Construction Operations
Commuteride Management
State Communications Network
ACHD Traveler Information (web, kiosks, phone)
Other Area Cities Traffic Monitoring
Media
Traveler Information Systems (web sites,511)
University of Idaho Virtual TMC
Boise State University Virtual TMC

Fig. 2. Treasure Valley, Idaho ITS architecture [15].

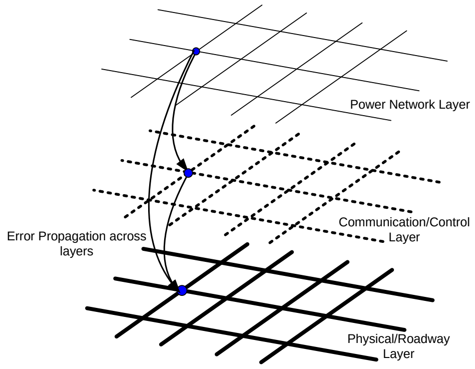

Fig. 3. Multi-Layer ITS Network Representation and Error Propagation across Layers.

TMC operators identified three primary and core functions for the TMCs: 1) provide optimal traffic management and control, 2) provide surveillance and monitoring of the network operations, and 3) disseminate travel information to the public. These three functions are clearly interdependent. As part of the phone interview, TMC operators were asked to rank the effect of losing the functionality of one or more of the field devices in the network. Summary of the results is presented in Table I and Table II.

TABLE I: EFFECT OF COMMUNICATION NETWORK FAILURE ON THE FUNCTIONALITY OF DIFFERENT ITS FIELD DEVICES

Field Device	Functionality	Failure Effect	Criticality level of the Failure
Controllers/Cabinets/ramp meters	Local Control	Loss of Real-time communication with the TMC. Controllers will use default local control plans stored in the controllers	Low/moderate
Central Control System	Network wide optimal control	100 % loss of communication with all field devices. Loss of major functionality	Very high
CCTVs	Network Surveillance	100% loss of functionality	High, especially for CCTV at critical points such as major intersections/interchanges
CMSs	User Information	100% loss of functionality	Moderate/high especially during incident situations

TABLE II: EFFECT OF POWER NETWORK FAILURE ON THE FUNCTIONALITY OF DIFFERENT ITS FIELD DEVICES

Field Device	Functionality	Failure Effect	Criticality level of the Failure
Controllers/Cabinets/ramp meters	Local Control	Control will be done manually or will revert to all-way stop control operations	Moderate/high, especially at major intersections in the network
Central Control System	Network wide optimal control	100 % loss of functionality	Extremely high
CCTVs	Network Surveillance	100% loss of functionality	High, especially for CCTV at critical points such as major intersections/interchanges
CMSs	User Information	100% loss of functionality	Moderate/high especially during incident situations

Based on the survey results, loss of communication to/from a local controller will have low/moderate effect on the network operations as controllers will implement the time-of-day default control plans stored in the local controllers. However, a loss of communication to a Closed Circuit TV camera (CCTV) or a Changeable Message Sign (SMS) can have a major (high) effect on the network operations especially during peak travel periods or during incident situations.

Loss of power at a local controller will have moderate/high effect on the network operations. Intersection control in such case will be done manually, which require dispatching personnel to the site, or through an all-way-stop-control mode, which could cause excessive network delay, especially at major intersections. Effective traffic management plans for critical intersections during power outages was identified by TMC operators as the key mitigation strategy for such case. Findings from the analysis also showed that a loss of power supply or communication at the TMC could have a paralyzing effect on the ability of the network to provide several of its essential services. An operational-ready alternate TMC and a redundant communication system to the TMC were identified as possible mitigation strategies for these threats.

V. SURVIVABLE SYSTEM ANALYSIS

The primary mission of the TMC is to develop and maintain safe and efficient traffic management and operations throughout the city network. Three objectives have been identified:

a) Reduce congestion and improve traffic safety along major corridors in the network.
b) Be exportable to other parts of the region and the state.
c) Archive and maintain traffic data for continuous system monitoring and evaluation and make this information available on a real-time basis for all stakeholders.

The TMS essential needs were identified as 1) provide efficient control and surveillance operations, 2) provide convenient means to control network components, collect and archive data, and observe data and/or visual images in real time, and 3) distribute the above data and information to different stakeholders.

After the needs were mapped out to the various stakeholders, a mapping of component ownership was completed. Example of stakeholder x responsibility/access matrix is presented in Table III.

TABLE III: STAKEHOLDER X RESPONSIBILITY/ACCESS MATRIX

Stakeholder x Responsibility/Access Matrix	**Department of Transportation**	**City**	**Information Technology Services**	**Private Providers**
Signal Controller and cabinets	X			
Signal Heads	X	X		
Changeable Message Signs	X	X		
Fiber Optic Cabinets	X	X		
Microwave communication network				X
ITD WAN/LAN network	X		X	
Data/video Servers	X		X	
CCTVs	X	X		
....				

Furthermore, the stakeholders involved in the TMC operation were interviewed to establish normal usage scenarios. Example of the normal usage scenarios matrix is presented in Table IV.

TABLE IV: NORMAL USAGE SCENARIOS

Task	Scenario	DOT	City	IT Services
System Monitoring/Control	Update traffic control plans	X		
	Verify loop/video input	X	X	
	Monitor CCTV operations	X	X	X
	Monitor network operations	X	X	X
	Collect and archive traffic data	X	X	X
	Identify incident situations	X	X	
	Respond to incident situations	X	X	
	Special event traffic control	X	X	
	Develop optimal control plans	X		X
	....			
System Maintenance	Change bulbs/pole maintenance		X	
	Flashing operations	X	X	
	Troubleshoot controllers/cabinets remotely	X	X	
	Troubleshoot controllers/cabinets on-site	X		
	....			

A. Attack Scenarios and Threats

Based on surveys of various electronic and physical components of the TMC components, anecdotal observations, and evidence of relaxed security, 18 attack scenarios were formulated. Physical and electronic threats are then listed under the appropriate compromised component category. Physical threats include such events as accidental digging into fibers, lightning, flood, projectiles, and traffic accidents. Electronic threats consist of data storms, insufficient bandwidth, unauthorized access, and signal degradation. Signal heads also attract lightning, which is a well-known cause of malfunction in signal controllers. These threats are then organized into a Threat-Component Matrix to illustrate the amount of components that each threat potentially possesses.

B. Threat Mitigation Strategies

By combining information from the project concept of operations with prior knowledge of communications networks in the electric power grid, it was possible to categorize a wide variety of components used in a local intelligent transportation system. Also with prior knowledge, it was easy to categorize numerous potential threats to these components, and appropriate mitigation for each of these threats.

Components were categorized into 15 types, and listed potential physical and electronic threats to each of these components. In full analysis, 32 classes of threats were identified, each affecting from 1 to 12 or more components. Between 1 and 7 mitigation strategies were identified for each class. Components and mitigations overlapped, but this still produced a very large mapping of threats to components and mitigations, a portion of which is shown in Table V.

TABLE V: EXAMPLE OF PHYSICAL AND ELECTRONIC THREATS MITIGATION STRATEGIES

	Threat	Component	Mitigations
Physical Threats	Vehicles	Fiber Optics	Height, Barriers for poles, Pole location, and Periodic automated testing
		Fiber Cabinets	Cabinet structure, Color, Signage, Location
		Signal Heads	Height, Warning signs, Chains, Sag mitigation, Color
	Malicious Cutting	Fiber Optics	Shielding, Location, Height, Signage, Periodic automated testing, Climbing, safeguards, Burying
		CCTV / Video Detectors	Conduit, Height, Location, Climbing , safeguards
	Vandalism	CCTV / Video Detectors	Height, Location, Shielding, Signage, Periodic manual testing
	Break-ins	Fiber Cabinets	Location, Shielding, Tactile deterrent, Lock mechanisms, Signage, Clean junctions, Perimeter fencing
		Signal Cabinets	Same as Fiber Cabinets
	Flooding	Communication Switchgear	Waterproof Shielding, Location Elevated rack mounting
		Loop detectors	Waterproof Shielding
		Fiber splices	Waterproof Shielding, Elevated rack mounting
		Fiber and signal cabinet	Complete junctions, Waterproof Shielding
		Servers and Wireless	Elevated rack Mounting
	Power Outage	Switchgear	Battery backup
		CCTV / Video detectors	Multiple Power feeds
		Signal controller/Signal heads	UPS
		Data Archive	UPS
		IT	UPS
		Servers	UPS
		Wireless	Battery backup
Electronic Threats	Denial of Service	Switchgear	IP filtering, Access restrictions, Programmable switch
		CCTV / Video Detectors	Port restrictions, IP restrictions, Periodic self test
		Signal Controllers	Same as CCTV / Video Detectors
		IT	IP filtering, Access restrictions, Port restrictions, Intrusion detection system, Firewall, Drive partitioning, Redundant IT servers, Formal periodic OS patch procedures
		Servers	Same as IT
		Wireless	Defensive sniffing, Encryption, Port restrictions, IP restrictions
	Settings Changes	Switchgear	Set / Reset procedures, Initial testing, Overburdened test
		Signal Controllers	Same as Switchgear
		Conflict Monitor	Same as Switchgear
	Data Storm	Switchgear	Self test, Failover switch with isolation logic Remote test / resets
		Signal Controllers	Remote test / reset procedures, Self test Failover controller with isolation logic
	Signal Degradation	Fiber optics	Periodic automated testing
		Fiber splices	Periodic automated testing
		Signal Controllers	Periodic automated testing
	Unauthorized Access Unauthorized Access cont.	Switchgear	Password protection IP Filtering
		CCTV / Video Detectors	Same as Switchgear
		Signal Controllers	Password protection, IP Filtering, Audit logging
		Archive	Audit logging, Intrusion Detection System Firewall, System Log monitoring, Backup & restore procedures, Password protection IP Filtered, Defensive sniffing
		IT	Same as Archive
		Wireless	Encryption, Defensive sniffing

C. Survivability Map

Improved or additional mitigation strategies to the attack scenarios and physical/electronic threats are summarized in the survivability map. Current strategies and recommended strategies accompany the resistance, recognition, and recovery of each attack scenario. The study determined that the most significant threat the traffic system is a large-scale power outage. As a result of such outage, traffic conditions on an already congested system can lead to full system congestion. Emergency traffic management plans for such situations need to be developed and continuously updated. A cost-benefit analysis of each recommended strategy would naturally progress henceforth.

VI. SUMMARY AND CONCLUSIONS

The paper presented a qualitative approach to assess the security and survivability of a transportation management network as an example of critical infrastructure networks. The process presented in this paper consists of seven steps: mission statement, stakeholder needs, responsibility, and access, logical system components and architecture, normal usage scenarios, attack, scenarios and threats, threat mitigation strategies, and survivability map. The proposed approach could be applied during the planning and design phase of critical infrastructure networks to evaluate different design alternatives or to assess the vulnerability and survivability of an existing network.

To identify typical normal usage scenarios and possible attack scenarios and their impact on traffic management centers (TMC) operations, in-depth interviews with 17 TMC operators throughout North America were conducted. Findings from the survey analysis showed that a loss of power supply at the TMC or at critical network intersections could have a paralyzing effect on the ability of the network to provide several of its essential services. An operational-ready alternate TMC and effective traffic management plans for critical intersections during power outages were identified as possible mitigation strategies for these threats. The proposed survivability analysis was also applied to the TMC operations. The analysis identified attack scenarios and threats, threat mitigation as well as survivability map with improved or additional threat mitigation strategies for different design alternatives.

The proposed approach provides a significant addition to the current design practices of different critical infrastructure networks by integration system security and survivability in the design process. A cost-benefit analysis of the proposed mitigation strategies should provide officials with a decision making tool to evaluate different design alternatives and to improve the overall security and survivability of critical infrastructure networks.

ACKNOWLEDGMENT

The authors wish to acknowledge that this collaborative-research project was funded by the U.S. Department of Transportation's University Transportation Centers program Grant DTR 598-6-0027. This research was conducted within the University of Idaho's National Institute for Advanced Transportation Technology (NIATT). The authors wish also to acknowledge the staff of ADA County Traffic Management Center for their valuable contribution to this analysis.

REFERENCES

[1] National Security Telecommunications Advisory Committee (NSTAC). (March, 1997). Information Assurance Task Force, Electric Power Risk Assessment. [Online]. Available: http://www.ncs.gov/nstac/nstac_publications.html

[2] Y. Sheffi, "Urban Transportation Networks," Englewood Cliffs, New Jersey, Prentice Hall, 1985.

[3] A. J. Nicholson, J. D. Schmöcker, M. G. H. Bell, and Y. Iida, "Assessing transport reliability: malevolence and user knowledge," *The Network Reliability of Transport*, The Netherlands, Pergamon, pp. 1-22, 2003.

[4] I. Wakabayash and Y. Iida, "Upper and lower bounds of terminal reliability of road networks: an efficient method with boolean algebra," *Journal of Natural Disaster Science*, vol. 14, pp. 29-44, 1992.

[5] A. Chen, H. Yang, H. K. Lo, and W. H. Tang, “A capacity related reliability for transportation networks,” *Journal of Advanced Transportation*, vol. 33, no. 2, pp. 183-200, 1999.

[6] J. D. Schmöcker and M. G. H. Bell, “The PFE as a tool for robust multi-modal network planning,” *Traffic Engineering & Control*, vol, 42, pp. 108-114, 2001.

[7] J. R. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, and R. Mead, “Survivable network systems: an emerging discipline, software engineering institute,” *Technical Report: Software Engineering* Institute, Carnegie Mellon University, 1997.

[8] P. G. Neumann, “Practical architectures for survivable systems and networks -phase two final report,” *Computer Science Laboratory, SRI International*, 2000.

[9] J. R. Ellison., R. C. Linger, T. Longstaff, and N. R. Mead, *A Case Study in Survivable Network System Analysis*, Technical Report: Software Engineering Institute, Carnegie Mellon University, 1998.

[10] N. R. Mead, R. J. Ellison, R. C. Linger, R. C. Longstaff, T. Longstaff, and J. McHugh., *A Survivable Network Analysis Method,* Technical Report: Software Engineering Institute, Carnegie Mellon University, 2000.

[11] Transportation Research Board, “Disruption Impact Estimation Tool-Transportation (DIETT): a tool for prioritizing high-value transportation choke points,” *NCHRP Report 525*, vol. 11, TRB, National Academies, Washington D.C., 2006.

[12] A. A. Rahim, P. Oman, J. Waite, M. Benke, and A. Krings, “Integrating network survivability analysis in traffic systems design,” in *Proc. Intelligent Transportation Systems Safety and Security Conf.*, March 2004, Paper #SS46, Miami, FL.

[13] 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,” in *Proc. 7th Annual IEEE Conf. on Intelligent Transportation Systems,* Washington D.C., October 2004, pp. 262-267.

[14] P. Oman, M. Benke, S. Melton, P. Merry, N. Nguyen, M. Phillips, and J. Waite, “*Applying* safety-critical fault tolerant principles to survivable transportation control networks,” *Publication N06-06 National Institute for Advanced Transportation Technology*, University of Idaho, Moscow, ID, 2004.

[15] McFarland Management and ITERIS, “Treasure valley ITS plan,” Ada County Highway District, Boise, ID, 2006.

Ahmed Abdel-Rahim is a associate professor in UI. He obtained the Ph.D. in Michigan State University in 1998, M.S. in Minia University, Egypt in 1990, B.S. in Assuit University, Egypt in 1984.

Dr. Ahmed’s research area focuses on Intelligent Transportation Systems, network modeling and survivability analysis, highway design and traffic safety, and traffic operation and control. He teaches several transportation engineering related courses such as fundamentals of transportation Engineering, highway design, traffic systems design, traffic flow theory, transportation modeling and simulation and traffic safety. He is a professional engineer (PE)-State of Idaho, and a member of the American Society for Civil Engineers (ASCE) and the Egyptian Syndicate of Engineers.

Dr. Ahmed received several honors and awards including University of Idaho Mid-Career award (2012), Outstanding Faculty award (2010) outstanding Young Faculty Award (2007), Faculty Excellence Award (2005); and an ASCE ExCEEd (Excellence in Civil Engineering Education) Fellowship (2003).

Bakr M. Aly Ahmed is an assistant professor in NDSU. He obtained the Ph.D. in Environmental Design and Planning, Virginia Tech, Virginia, USA in 2001, M. Sc. in Architecture, Minia University, Egypt in 1990, and B. Sc. in Architecture, Building Technology, Minia University, Egypt in 1984.

Dr. Bakr has 27 years of academic and teaching experience in architecture. His primary teaching courses at NDSU are: structural design, environmental control systems, high-rise design studio, and master thesis.

He worked in numerous projects: beach resorts, housing developments, and mix-use urban projects. His research interest focuses on sustainable design modeling, environmental capacity measurements, and simulation modeling for pedestrian movement in large buildings.

Dr. Bakr is a licensed member of the Syndicate of Egyptian Engineers since 1984 and an associated member of the American Institute of Architecture. Selected publications: “The Good, Bad, and Ugly” in Architectural Case Studies, DEFSA, 2007, and “Means of Egress Building Code Compliance Diagrams”, AEI, 2006.