ASSESSING THE

SECURITY AND SURVIVABIILTY OF

TRANSPORTATION CONTROL NETWORKS

FINAL REPORT

February 2005

Budget Number KLK215

N05-01

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

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 Assessing the Security and Survivability of Transportation Control Networks	5. Report Date February 2005 6. Performing Organization Code
7. Author(s) Paul Oman and Axel Krings	8. Performing Organization Report No. *N05-01*
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	10. Work Unit No. (TRAIS) 11. Contract or Grant No. *DTRS98-G-0027*
12. Sponsoring Agency Name and Address US Department of Transportation Research and Special Programs Administration 400 7th Street SW Washington, DC 20509-0001	13. Type of Report and Period Covered Final Report: August 2003-December 2004 14. Sponsoring Agency Code *USDOT/RSPA/DIR-1*

Supplementary Notes:

16. Abstract

Cyber attacks and electronic sabotage targeted against these 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 and DOT's Research and Special Programs Administration, we undertook a two year study of similar vulnerabilities with the electric power infrastructure. Our analyses of cascading failures within the electric power grid demonstrate that catastrophic failure is fraught with common mode faults. Post-mortem analyses show that these vulnerabilities can be identified and modeled using methods we call Common Mode Failure Analysis (CMFA) and Survivability Systems Analysis (S/SSA). When used together CMFA and S/SSA provide effective tools to identify network vulnerabilities, and point the way toward mitigation strategies and design parameters that can be used to construct more robust and survivable control networks. In this project we adapted our CMFA and S/SSA processes to make them applicable to transportation control networks. We exemplify this work with a security and survivability analysis of the proposed City of Moscow Intelligent Transportation System.

17. Key Words Critical infrastructure protection, information networks, security, survivability, complex control systems, Intelligent Transportation Systems	18. Distribution Statement Unrestricted; Document is available to the public through the National Technical Information Service; Springfield, VT.

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

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The North American transportation grid enables our national and international commerce and supports literally all other critical infrastructures within the United States. However, increasing reliance on computer technology for improved communication and automation of traffic and transportation control networks has created vulnerabilities within those control systems that are similar to those seen in electric power control systems. Particularly vulnerable are (1) control center and dispatch communications, (2) computer controlled equipment for access, safety and monitoring, and (3) remotely accessible real-time actuators regulating transportation flow (e.g., bridges, tunnels, rail crossings, arterial routes, etc.). Especially vulnerable are IP-addressable and modem-accessible in-the-field devices used to monitor and regulate traffic flows in large urban environments.

Cyber attacks and electronic sabotage targeted against these 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 additional financial support of the National Institute of Standards and Technology (NIST), we undertook a two year study of similar vulnerabilities with the electric power infrastructure. Our analyses of cascading failures within the electric power grid demonstrate that catastrophic failure is fraught with common mode faults. Post-mortem analyses show that these vulnerabilities can be identified and modeled using methods we call Common Mode Failure Analysis (CMFA) and Survivability Systems Analysis (S/SSA). When used together, CMFA and S/SSA provide effective tools to identify network vulnerabilities and point the way toward mitigation strategies and design parameters that can be used to construct more robust and survivable control networks.

In this project, we adapted our CMFA and S/SSA processes to make them applicable to transportation control networks. We exemplify this work with a security and survivability analysis of the proposed City of Moscow Intelligent Transportation System.

DESCRIPTION OF PROBLEM

We now live in a digital society where day-to-day operations are optimized by complex real-time control systems. Our surface transportation infrastructure has evolved to a level of complexity where Intelligent Transportation Systems (ITS) are essential for large urban environments. Under normal traffic conditions, ITS operation is optimized for system-wide objective functions (i.e., to minimize network-wide delay or maximize throughput). Travelers 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., oversaturated, damaged, or impacted by accidents, malicious attack, or weather), system optimization and dynamics become much more complex due to the interaction between travelers, network controls, communication networks, and the physical infrastructure. This report documents a series of security and survivability analyses conducted on the proposed Moscow ITS project, now under development.

The standard approach for evaluating transportation systems has by tradition focused exclusively on operational, safety, and security aspects, while ignoring issues of system survivability. There are two primary factors responsible for this focus. First, transportation system components have historically existed in isolation, so the failure of one element had limited impact on the overall system. Second, the field of physical security is a well-established science, relative to the analysis of survivability of networked systems. As infrastructures become increasingly interconnected, it is necessary to reexamine traditional approaches for evaluating vulnerabilities to incorporate survivability concerns.

A typical infrastructure vulnerability assessment quantifies the physical risk of an asset based on a variety of traditional security concerns such as location, security measures, access, and in-place security personnel. This type of assessment also takes into account risk due to the availability (or unavailability) of specialized response personnel in the event of a security incident. Vulnerability assessments are first and foremost concerned with physical security, and although electronic intrusions are sometimes addressed they are applied on a case-by-case basis. In contrast, the canonical Survivable System Analysis (SSA) method, as defined in two papers published by the CMU Software Engineering Institute, primarily looks at network vulnerabilities without regard to physical disturbances like weather, vandalism, theft, etc. What is needed is a combination of traditional vulnerability assessment and the SSA process. This is what we developed and documented for this project.

The advent of ITS has led to increased connectivity of components as transportation engineers strive to improve service in the face of ever worsening traffic congestion. A consequence of this increased connectivity is that transportation systems are more vulnerable to both physical and electronic threats, as well as to cascading and network failures. The networked nature of modern transportation systems suggests that their survivability can be evaluated in a manner similar to those employed to analyze computer networks. A survivability analysis can determine the likelihood that a system will continue to operate at a given threshold, even in the face of individual component failure.

A modified SSA analysis on the proposed system was completed in conjunction with an ITS project for the City of Moscow, Idaho. This study includes both security and survivability analyses of options for: fiber optic cable routing, traffic controller network topologies, communications switchgear linking traffic controllers, computer server placement, and network connections to project stakeholders for access to data and signal control. The analysis also includes the identification of essential components, the development of stakeholder/component responsibility and access matrix, the identification of project threats, and the development of a threats/critical component matrix. Furthermore, the analysis identifies threat mitigation strategies for each threat identified and provides suggestions for improved security and survivability. The analysis has been presented to the City of Moscow ITS system planners and, hopefully, is being used to influence their design decisions.

PROJECT OBJECTIVES, TASKS, AND RESULTS

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

1. Determine the similarities between transportation control networks and other real-time complex control systems, such as the electric power grid.

Task: Analyze existing transportation control networks through visitations, literature review, and meetings with NIATT and ITD personnel.

Results: Few existing studies were found, but published evidence demonstrates that ITS security and survivability is both a major concern and an open issue.

2. Assess the state-of-the-practice with respect to the application of Information Security (InfoSec) principles within existing traffic and transportation control networks.

   Task: Complete in situ security and survivability assessments of actual control center and dispatch operations.

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

3. Adapt or develop procedures for Common Mode Failure Analysis (CMFA) and Security/Survivability Systems Analysis (S/SSA) from the electric power domain to application within traffic/transportation control networks.

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

   Results: It was determined that a combination of CMFA and S/SSA could be a valuable analytic tools with respect to ITS. 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. Identify areas within transportation control networks where existing InfoSec technologies can be applied, but are heretofore absent.

Task: Analyze fault and failure usingtrial application of CMFA and S/SSA procedures to document failure incidents and/or transportation network topological diagrams.

Results: A draft vulnerability analysis with respect to security and survivability of the proposed City of Moscow ITS was compiled (Appendix A).

5. Identify transportation domain specific vulnerabilities for which new InfoSec technologies and devices must be developed or adapted.

   Task E. Complete gap analysis documenting InfoSec applications and voids within transportation control network topologies.

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

PROJECT BENEFITS AND TECHNOLOGY TRANSFER

Our computerized control systems contain many potential sources of common mode failures, including physical components, hardware circuitry, firmware, and software. We must harden our automated transportation systems (and other critical infrastructures) against those very vulnerabilities. The hardening process—against both physical and cyber attacks—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. For this project, we applied 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.

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 NIATT affiliate faculty Dr. Brian Johnson, UI. Electrical and Computer Engineering Department., Dr. Ahmed Abdel-Rahim, UI Civil Engineering Department, and NIATT director Dr. Michael Kyte.Other valuable assistance was obtained from several engineers from the Idaho Dept. 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.

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.

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.

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.

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.

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.

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.

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.

RELEVANCE TO THE NIATT STRATEGIC PLAN

This research project specifically addressed the security and survivability of a real-time control network supporting an advanced Center for Traffic Operations and Control, as described in NIATT’s *Strategic Plan*. Complex systems like traffic control and transportation monitoring networks form the heart of our nation’s critical infrastructures, without which our nation’s commerce and economy would collapse. Technologies exist for convenient access and intelligent control of remote devices, but that convenience and remote operations capability comes at the cost of reduced security and survivability. Our nation’s infrastructures and essential utilities are susceptible to cascading failures induced by relatively minor events such weather phenomena, accidental damage to system components, and physical or cyber attack. In contrast, survivable complex control structures should and could be designed to lose sizable portions of the system and still maintain essential control functions. This NIATT-UTC research project provided funds to develop procedures for security and survivability vulnerability assessments of Intelligent Transportation Systems. The result is an example report that can be used by any engineer involved with the development and/or assessment of real-time control systems.

Appendix A

DRAFT

Moscow ITS Survivability Analysis Report

Paul Oman, John Waite, Matt Benke

University of Idaho

Version 1.0

September 9, 2003

This document comprises a draft survivability analysis report for the Moscow Intelligent Traffic System (ITS), a project to renovate the city of Moscow traffic signaling system. The Moscow ITS project is a cooperative effort by the National Institute for Advanced Transportation Technology (NIATT), the Idaho Transportation Department (ITD), the Federal Highway Administration (FHWA), and the City of Moscow. Information from this report was obtained through meetings and personal collaboration with individuals from the above organizations, and data obtained from these reference documents:

1. Concept of Operations Task 3 Report, City of Moscow ITS Project, Traffic Signal Systems Integration and Deployment April 2002.

2. Relevant ITS Standards, Task 2 Report, City of Moscow ITS Project, Traffic Signal Systems Integration and Deployment May 2002.

This report contains a survivability analysis based on the template and process defined in a CMU SEI case study[1]. Following is the organization of the remainder of this document:

I. Mission Statement
II. Essential Needs
III. Stakeholder Needs
IV. Essential Components
V. Alternative Network Topologies
VI. Threats
VII. Mitigation Strategies

[1] *A Case Study in Survivable Network System Analysis*, R. J. Ellison, et al., CMU/SEI-98-TR-014, Carnegie Mellon, Software Engineering Institute, Pittsburgh, PA, Sept. 1998.

I. Moscow ITS Project Mission Statement

Develop an efficient traffic signal controller technology to be applied to improve traffic signal operations in the City of Moscow with a traffic operations center accessible by ITD and NIATT (and optionally City of Moscow Police) with these objectives:

- Reduce congestion and improve traffic safety along the Highway 8 and U.S. 95 corridors.
- Record actual traffic data for use in NIATT simulations for optimizing signal timing plans.
- Test coordinated/actuated signal control timing plans.
- Be exportable to other parts of District 2 and subsequently other parts of the state.

II. Moscow ITS Project Essential Needs

1. New or upgraded traffic signal control technology to:
   - provide more flexible signal setting
   - accommodate growth
   - record traffic data

2. Provide convenient means to:
   - change settings
   - collect data
   - observe data and/or visual images in real time

3. Distribute the above data and information to NIATT, ITD District 2 and (optionally) the Moscow Police Department

III. Moscow ITS Project Stakeholder Needs

In this project there are six primary stakeholders:

1. Users (Drivers and Pedestrians)
2. NIATT
3. The Moscow Police Department
4. The City of Moscow Engineering Department.
5. ITD
6. FHWA

Table 1 maps these primary stakeholders with their respective needs.

Table 1. Stakeholder Needs Matrix

Stakeholder Needs	Drivers / Pedestrian	NIATT	City of Moscow Police	City of Moscow	ITD	FHWA
A traffic signal system that safely and effectively moves people and vehicles through and within the City of Moscow	X	X	X	X	X	X
A traffic signal system that can be integrated with ITD's regional architecture and national ITS standards					X	X
A traffic signal system that is flexible and can be expanded to meet future needs				X	X	X
A traffic signal system that adapts to changing traffic conditions and responds to special events and to pedestrian and bicycle flows	X		X	X	X	
A traffic signal system that can be easily and remotely maintained				X	X	
A communications infrastructure that provides links between signalized intersections, with the central traffic operations centers, and to the city's operations center				X	X	X
A roadway sensor or detection system that monitors traffic signal system performance and changing traffic flow conditions and provides continuous system evaluation and diagnostics		X		X	X	
A data archiving system that collects, aggregates and archives traffic flow and signal timing data		X		X	X	
A surveilance system that provides real-time monitoring of the city traffic signal network		X	X	X	X	X
Highway/rail intersections that use signal preremption and interconnects			X	X	X	
A training facility that provides traffic signal system training and real-time signal timing testing capabilities.		X		X	X	X

IV. **Moscow ITS Project Essential Components**

This section lists the components which are essential to fulfilling the needs of the various stakeholders in this project. Figure 1 shows a high-level diagram of the Moscow ITS project. Table 2 shows the ownership of the various components involved in the project.

a. Signaling System
   i. Cabinets
   ii. Poles
   iii. Loop Detectors
   iv. Video Detectors
   v. CCTV
   vi. Signal Heads
   vii. Controllers
   viii. Conflict Monitor

b. Communication Infrastructure
   i. Hubs/Switches
   ii. Fiber Optic
   iii. Microwave
   iv. ITD WAN/LAN
   v. Local Wireless
   vi. Data Server
   vii. Video Server

c. Computer Database and Archiving
   i. Operations Center Archive
   ii. State Archive

d. Virtual Operations Center (VOC)
   i. Local computers
   ii. Archive

e. Traffic Controller Research Lab (TCRL)
   i. Local Computers
   ii. Archive
   iii. Testbeds & simulations

Table 2. Stakeholder x Component responsibility and access matrix

	ITD	City of Moscow	NIATT	FHWA	State of Idaho Dept. of Admin.
Signal Cabinets	X				
Poles	X	X			
Signal Heads	X				
Conflict Monitor	X				
Signal Controllers	X				
Detectors	X				
CCTV	X	X			
Switchgear	X	X			
Fiber Optic	X	X			
Fiber Cabinets					
Microwave					X
ITD WAN/LAN	X				
Local Wireless					
Data Server	X		X		
Video Server	X		X		
Operations Center Archive	X				
State Archive	X				
VOC Local Computers	X		X		
VOC Archive	X		X		
TCRL Local Computers			X		
TCRL Archive			X		
TCRL Testbed / Simulators			X		

V. **Alternative Network Topologies**

Figures 1 through 4 represent an array of routing topologies ranging from a long-run star network (Figure 1), to a short-run daisy chain network (Fig. 2), with hybrid approaches proposed by Six Mile Engineering (Figure 3), and a tree network topology (Fig. 4). At the bottom of each figure is a table containing a synopsis of the pros and cons of each of

Figures 5 through 8 represent choices for locating data and video servers (network computers). Figure 5 shows a single set of servers located at the ITD office in Lewiston, ID. Figure 6 shows an ITD-controlled set of servers located somewhere on the U.I. campus. Figure 7 shows the same configuration with server control administered through NIATT. Figure 8 shows a mirrored server configuration with dual sets of servers, one located at ITD offices in Lewiston and the other located and run by NIATT. At the bottom of each figure is a table containing a synopsis of the pros and cons of each of the four server options.

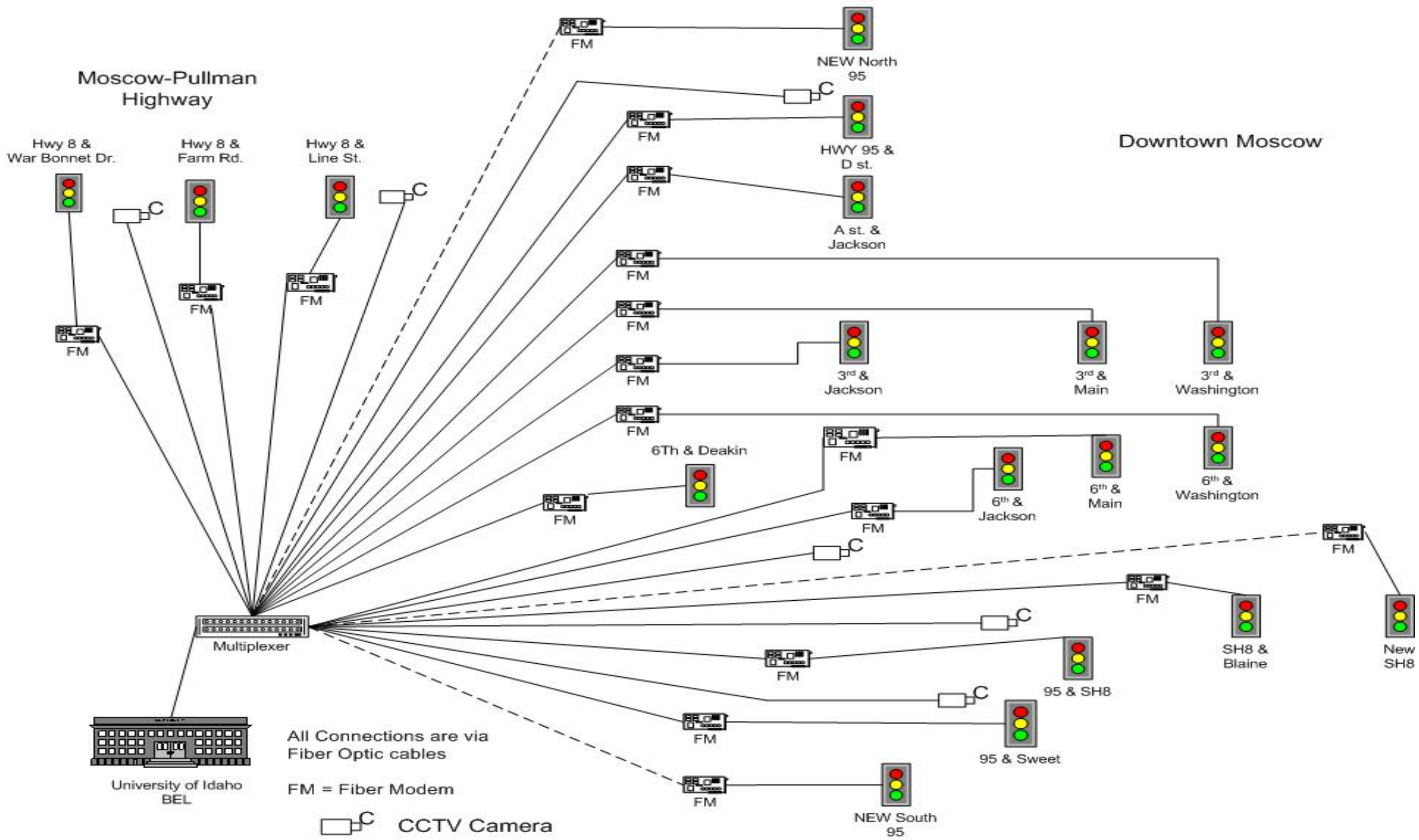

Figure 1. Full Star Topology

Pros	Cons
No line congestion	Single point of failure at Multiplexer
No line failure interference	Cost of added fiber
No signal degradation caused by fiber junctions	Expansion capability undefined

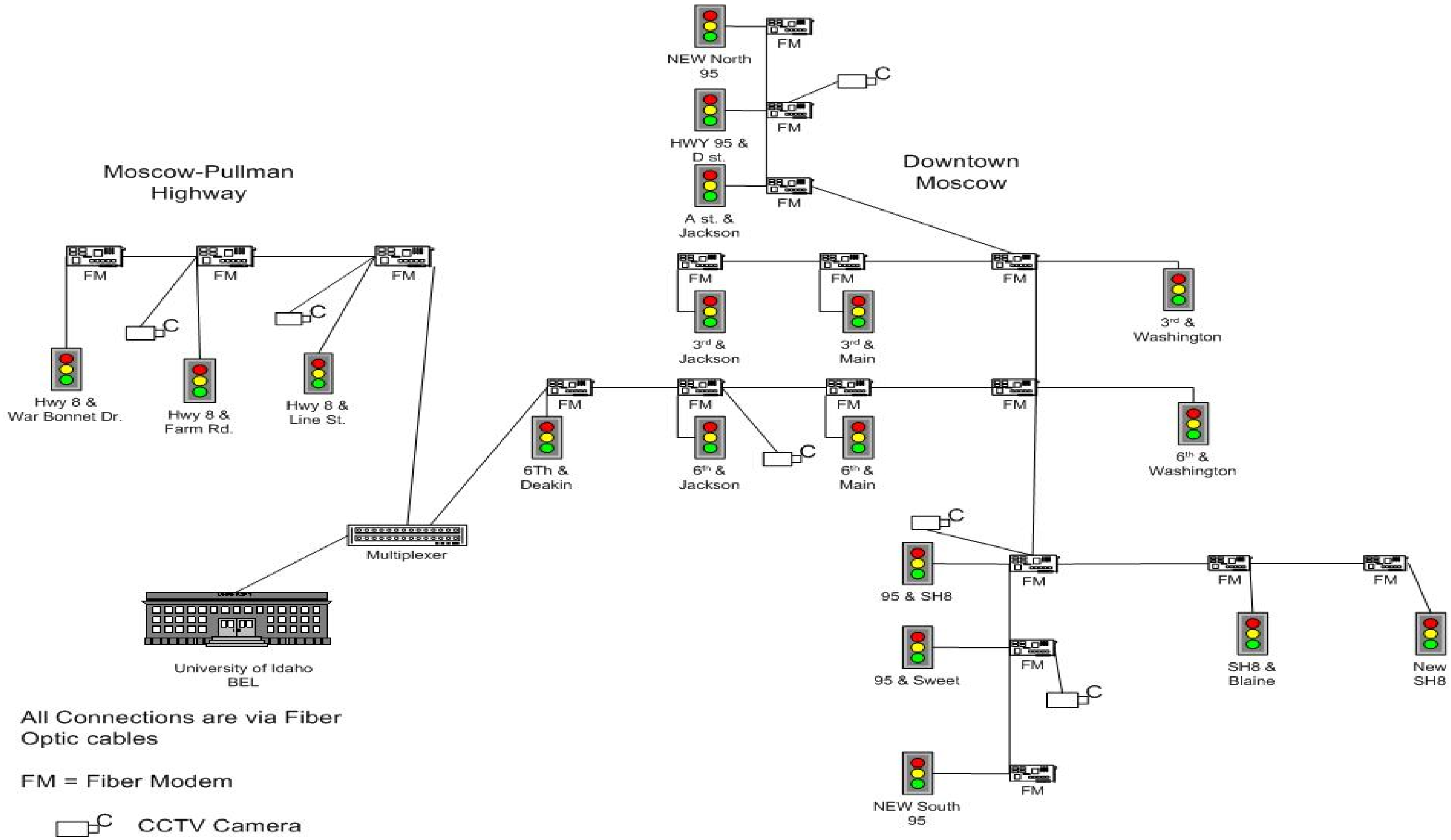

Figure 2. Full "Daisy Chain" Topology

Pros	Cons
Shortest run of fiber	Single point of failure at Multiplexer
Minimum cost of fiber	Requires compressed CCTV Signal
	CCTV broadcast storm affects signal system
	Line failures impact all downstream components
	Signal degradation at fiber junctions

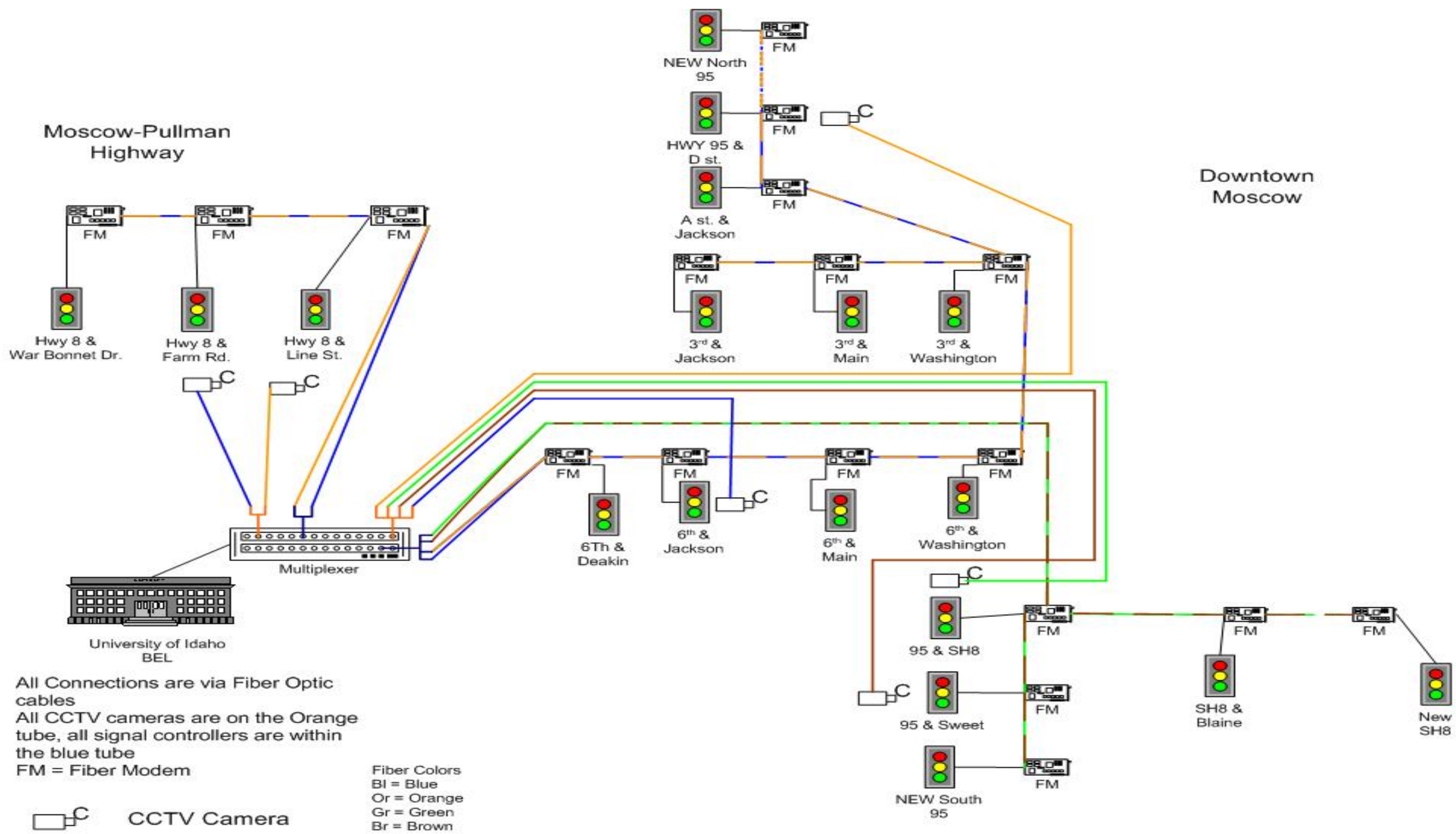

Figure 3. Six Mile Engineering Proposed Topology

Pros	Cons
Dedicated CCTV fiber (no compression required) CCTV broadcast storm does not impact signal system Less cost than full long-run star	Single point of failure at Multiplexer Line failures impact downstream components Signal degradation at fiber junctions Downtown single point of failure at 6th and Deacon

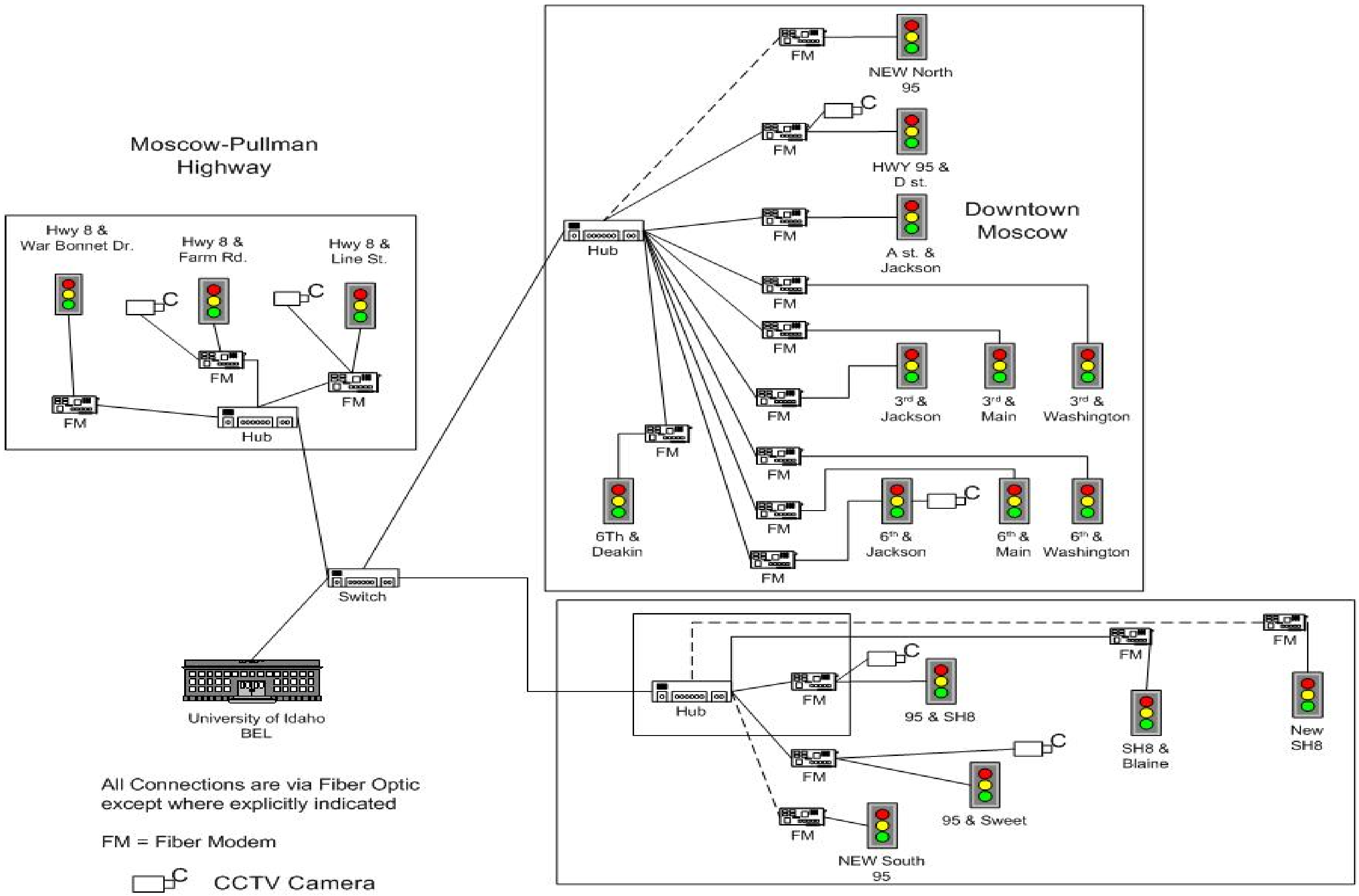

Figure 4. Tree Topology

Pros	Cons
Hub and switches can serve as firewalls Less cost than a full long-run star No downstream signal single failure modes	Single point of failure at multiplexer Requires compressed CCTV CCTV broadcast storm affects some signals Line failures affect some downstream components Added cost of hubs and switches

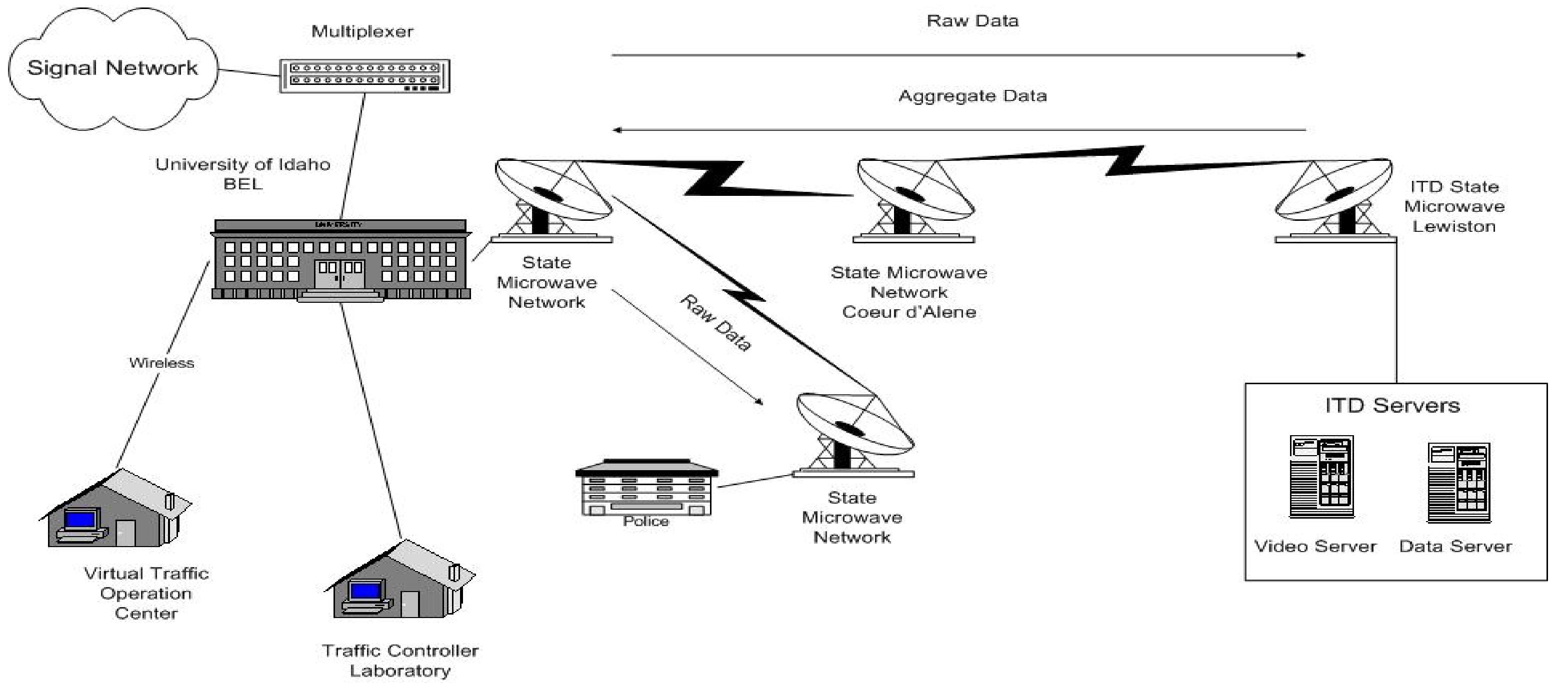

Figure 5. Single ITD Server in Lewiston

Pros	Cons
ITD gains direct control of data and video servers. ITD can monitor servers directly, with quick response time for adjustments and without need for additional employees.	Single server location introduces single point of failure for data and video archiving. For requests from NIATT, information must be re-transmitted through the state microwave network, greatly increasing the consumed bandwidth.

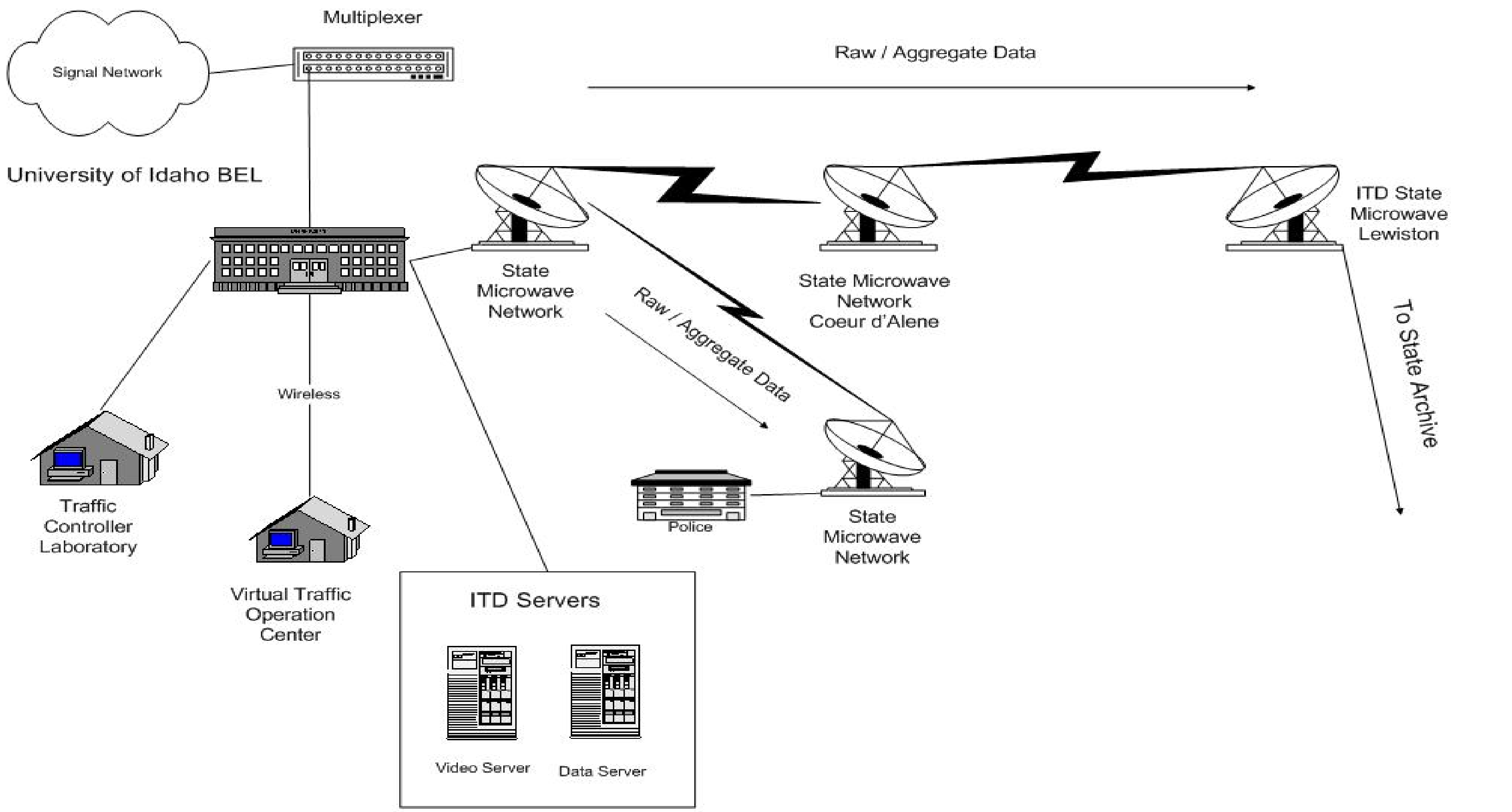

Figure 6. Single ITD Server in Moscow

Pros	Cons
Data can still be gathered and stored even if the state microwave network is down.	ITD, if it wants direct control of information, would need employees on site at the NIATT storage location. Single server location introduces single point of failure for data and video archiving.

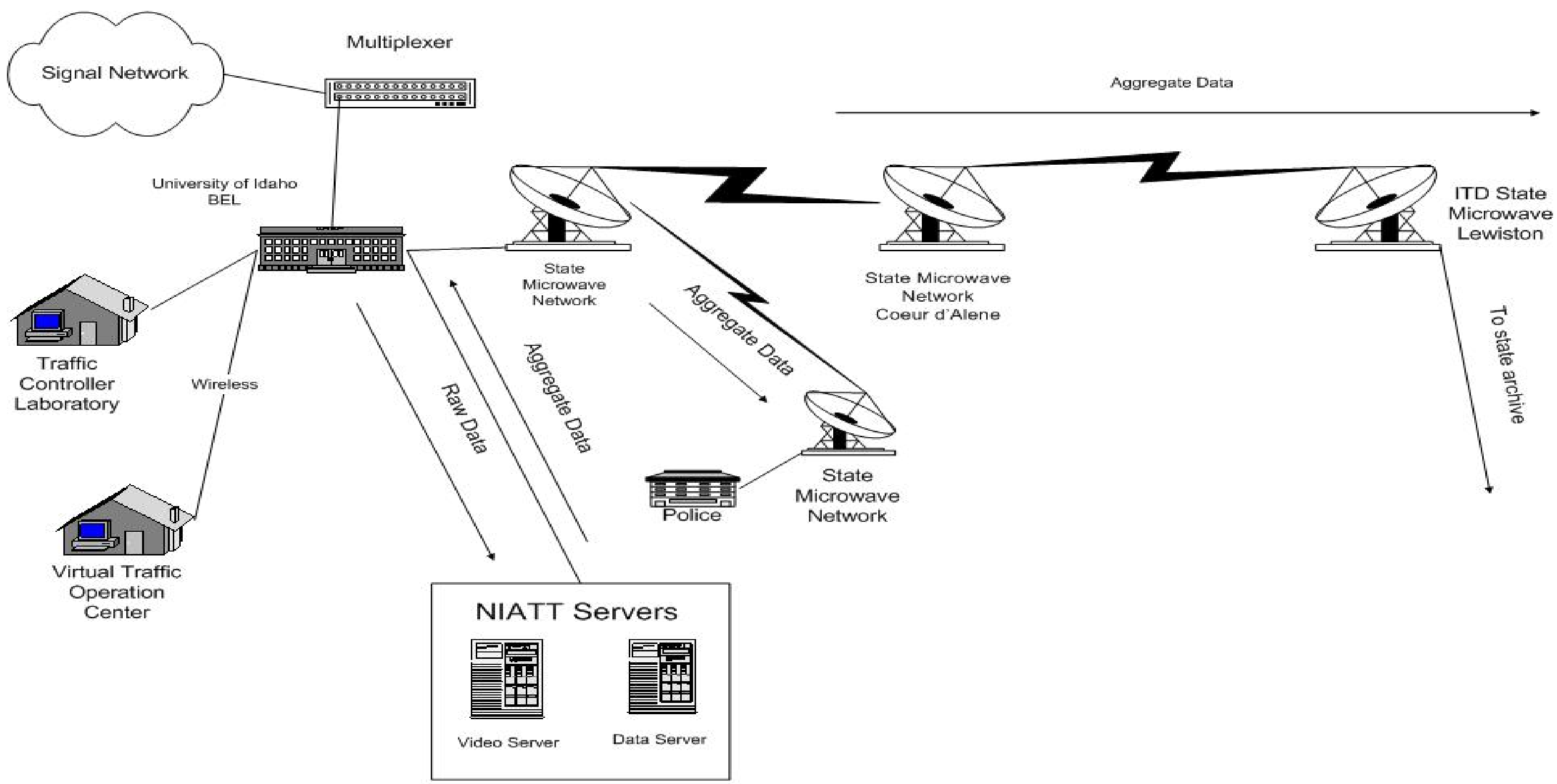

Figure 7. Single NIATT Server in Moscow

Pros	Cons
Data and video information can be quickly transmitted to the NIATT research lab for monitoring and real-time simulations. This would eliminate the added cost of transmitting information back to NIATT from ITD.	Single server location introduces single point of failure for data and video archiving. ITD would receive aggregate data processed through the NIATT servers.

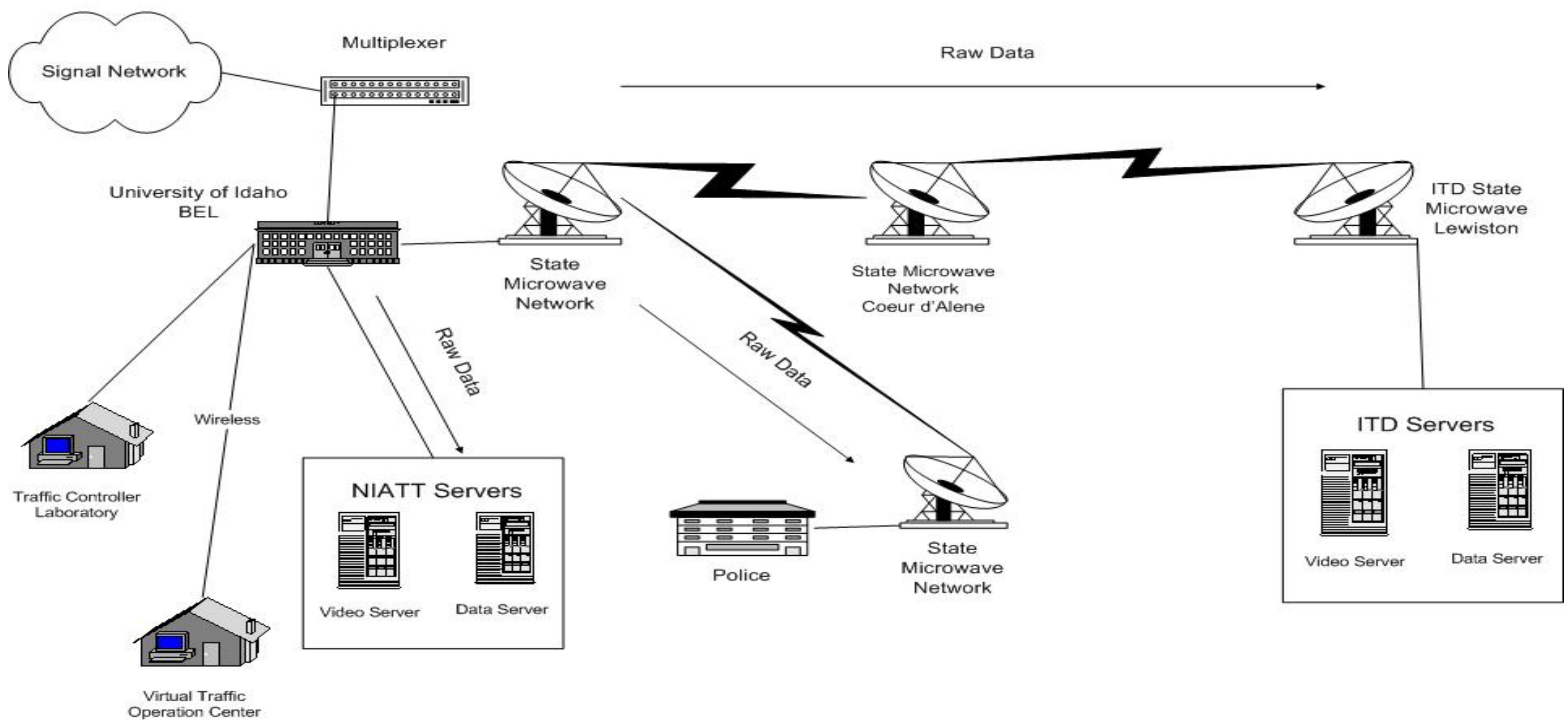

Figure 8. Dual Server ITD-Lewiston NIATT-Moscow

Pros	Cons
Redundancy of archiving eliminates single point of failure—if one archive is compromised, it can request to roll back to information from the other, operational archive. NIATT can still directly monitor information for research purposes without needing ITD to send it over the network.	Redundant archives would require synchronization, which would increase the consumed bandwidth every time archives are synchronized.

VI. **Moscow ITS Project Threats**

The threats to this project can be split into two categories, physical threats and electronic threats. The following outline shows threats to each critical component. Table 3 contains Threats by Critical Components mapping.

Physical Threats

a. Fiber Optics
   i. Digging
   ii. Vehicles
   iii. Wire Snagging
   iv. Malicious Cutting
   v. Accidental Cutting
   vi. Weather
b. Switchgear
   i. Single Node failure
   ii. Multi Node failure
   iii. Flooding
   iv. Lightning
   v. Vibration
   vi. Power Outage
c. CCTV / Video Detectors
   i. Malicious Cutting
   ii. Weather
   iii. Vandalism
   iv. Projectiles
   v. Birds
   vi. Lightning
   vii. Vibration
   viii. Power Outage
d. Loop Detectors
   i. Digging
   ii. Flooding
   iii. Power Outage
e. Fiber Splices
   i. Bad Splices
   ii. Flooding
f. Fiber Cabinets
   i. Vehicles
   ii. Weather
   iii. Projectile
   iv. Animals
   v. Break-ins
   vi. Flooding
   vii. Vibration
g. Signal Heads
   i. Vehicles
   ii. Weather
   iii. Projectile
   iv. Lightning
   v. Power Outage
h. Signal Cabinets
   i. Vehicles
   ii. Weather
   iii. Projectiles
   iv. Animals
   v. Break-ins
   vi. Flooding
   vii. Vibration
i. Signal Controllers
   i. Vehicle
   ii. Projectile
   iii. Flooding
   iv. Lightning
   v. Vibration
   vi. Power Outage
j. Conflict Monitor
   i. Vehicle
   ii. Projectile
   iii. Flooding
   iv. Lightning
   v. Vibration
   vi. Power Outage
k. Archive
   i. Flooding
   ii. Lightning
   iii. Power Outage
l. IT
   i. Flooding
   ii. Lightning
   iii. Power Outage
m. Servers
   i. Flooding
   ii. Lightning
   iii. Power Outage
n. Wireless
   i. Flooding
   ii. Lightning
   iii. Power Outage
o. Microwave Transceiver
   i. Weather
   ii. Bad Splices
   iii. Single Node Failure
   iv. Multi Node Failure
   v. Vandalism
   vi. Projectiles
   vii. Birds
   viii. Animals
   ix. Break-ins
   x. Lightning
   xi. Vibration
   xii. Power Outage

Electronic Threats

a. Fiber Optics
    i. Signal Degradation
b. Switchgear
    i. Denial of Service (DoS)
    ii. Settings changes
    iii. Data Storm
    iv. Unauthorized Access
c. CCTV / Detectors
    i. DoS
    ii. Unauthorized Access
    iii. Bandwidth
d. Fiber Splices
    i. Signal Degradation
e. Signal Controllers
    i. DoS
    ii. Settings Changes
    iii. Data Storm
    iv. Signal Degradation
    v. Unauthorized Access
    vi. Timing
f. Conflict Monitor
    i. Settings Changes
g. Archive
    i. Unauthorized Access
    ii. Sabotage
    iii. Media Failure
    iv. Malicious Code and Viruses
h. IT system
    i. DoS
    ii. Unauthorized Access
    iii. Timing
    iv. Bandwidth
    v. Protocols
    vi. Malicious Code and Viruses
i. Servers
    i. DoS
    ii. Media Failure
    iii. Malicious Code and Viruses
    iv. Inadequate OS Resources
    v. NIC Failure
j. Local Wireless
    i. DoS
    ii. Unauthorized Access
    iii. Packet Injection
k. Microwave Transceiver
    i. DoS
    ii. Settings Changes
    iii. Data Storm
    iv. Signal Degradation
    v. Unauthorized Access
    vi. Timing
    vii. Bandwidth
    viii. Protocols
    ix. Sabotage
    x. Media Failure

Table 3. Threats x Critical Components Matrix

Threats per Componant	Fiber Optics	Switchgear	CCTV / Video Detectors	Loop Detectors	Fiber Splices	Fiber Cabinet	Signal Heads	Signal Cabinet	Signal Controller	Conflict Monitor	Archive	IT	Servers	Wireless	Microwave Transceiver
Physical Threats															
Digging	X			X											
Vehicles	X					X	X	X	X	X					
Wire Snagging	X														
Malicious Cutting	X		X												
Accidental Cutting	X														
Weather	X		X			X	X	X							X
Bad Splices					X										X
Single Node Failure		X													X
Multi Node Failure		X													X
Vandalism			X												X
Projectiles			X			X	X	X	X	X					X
Birds			X												X
Animals						X		X							X
Break-ins						X		X							X
Flooding		X		X	X	X		X	X	X	X	X	X	X	
Lightning		X	X				X		X	X	X	X	X	X	X
Vibration		X	X			X		X	X	X					X
Power Outage		X	X	X			X		X	X	X	X	X	X	X
Electronic Threats															
Denial of Service		X	X						X			X	X	X	X
Settings Changes		X							X	X					X
Data Storm		X							X						X
Signal Degradation	X				X				X						X
Unauthorized Access		X	X						X		X	X		X	X
Timing									X			X			X
Bandwidth			X									X			X
Protocols												X			X
Sabotage											X				X
Media Failure											X		X		X
Malicious Code and Viruses											X	X	X		
Inadequate OS Resources													X		
NIC Failure													X		
Packet Injection														X	

VII. **Threat Mitigation Strategies**

Every threat to a critical component (documented in Table 3) needs to be addressed with mitigating technologies and/or strategies. Consistent with Table 3 we have segregated the physical and electronic threats into two groups. Physical threat mitigation are presented in Table 4; electronic threat mitigations are shown in Table 5.

Table 4 Physical Threats

Threat	Component	Mitigations	Owner
Digging	Fiber Optics	Depth Signage Conduit Periodic testing Diagrams / Maps	ITD City of Moscow
	Loop Detectors	Diagrams / Maps	ITD
Vehicles	Fiber Optics	Height Barriers for poles Pole location Periodic automated testing	ITD City of Moscow
	Fiber Cabinets	Cabinet structure Color Signage Location Bury	
	Signal Heads	Height Warning signs Chains Sag mitigation Color	ITD
	Signal Cabinets	Same as Fiber Cabinets	ITD
	Signal Controllers	Subordinate to Signal Cabinets	ITD
	Conflict Monitor	Subordinate to Signal Cabinets	ITD
Wire Snagging	Fiber Optics	Height Location Color Signage Periodic automated testing Strength of support wire Elastic / Shock mount	ITD City of Moscow
Malicious Cutting	Fiber Optics	Shielding Location Height Signage Periodic automated testing Climbing safeguards Burying	ITD City of Moscow
	CCTV / Video Detectors	Conduit Height Location Climbing safeguards	ITD
Accidental Cutting	Fiber Optics	Diagrams / Maps Signage Color Conduit Periodic automated testing	ITD City of Moscow

Threat	Component	Mitigations	Owner
Weather	Fiber Optics	Shielding Support cables Burying underground Elastic mount	TD City of Moscow
	CCTV / Video Detectors	Shielding Weather resistant components Temperature tolerant components Fiber Cabinets Weather proof	ITD
	Signal Heads	Weather proof Temperature tolerant components	ITD
	Signal Cabinets	Weather resistant	ITD
	Microwave Transceiver		ID Admin
Bad Splices	Fiber Splices	Certified equipment Training Initial testing Periodic automated signal testing	ITD City of Moscow
	Microwave Transceiver		ID Admin
Single Node Failure	Switchgear	Initial testing Periodic testing Redundant / Secondary port Failover port	ITD City of Moscow
	Microwave Transceiver		ID Admin
Multi Node Failure	Switchgear	Redundant hub / switch Failover hub / switch	ITD City of Moscow
	Microwave Transceiver		ID Admin
Vandalism	CCTV / Video Detectors	Height Location Shielding Signage Periodic manual testing	ITD
	Microwave Transceiver		ID Admin
Projectiles	CCTV / Video Detectors	Height Location Shielding Signage Periodic manual testing	ITD
	Fiber Cabinets	Location (burying) Shielding Signage	
	Signal Heads	Shielding	ITD
	Signal Cabinets	Location Shielding Signage	ITD
	Signal Controllers	Subordinate to signal cabinets	ITD
	Conflict Monitor	Subordinate to signal cabinets	ITD
	Microwave Transceiver		ID Admin
Birds	CCTV / Video Detectors	Shielding Visual and tactile deterrent	ITD
	Microwave Transceiver		ID Admin
Animals	Fiber Cabinets	Location Perimeter Complete junctions Shielding Visual and tactile deterrent	

Threat	Component	Mitigations	Owner
Animals cont.	Signal Cabinets	Location Perimeter Complete junctions Shielding Visual and tactile deterrent	ITD
	Microwave Transceiver		ID Admin
Break-ins	Fiber Cabinets	Location Shielding Tactile deterrent Lock mechanisms Signage Clean junctions Perimeter fencing	
	Signal Cabinets	Same as Fiber Cabinets	ITD
	Microwave Transceiver		ID Admin
Flooding	Switchgear	Waterproof Shielding Location Elevated rack mounting	ITD City of Moscow
	Loop detectors	Waterproof Shielding	ITD
	Fiber splices	Waterproof Shielding Elevated rack mounting	ITD City of Moscow
	Fiber cabinet	Complete junctions Waterproof Shielding	
	Signal cabinet	Same as Fiber cabinet	ITD
	Signal controller	Same as Fiber cabinet	ITD
	Conflict monitor	Same as Fiber cabinet	ITD
	Archive	Elevated rack Mounting	ITD / NIATT
	IT	Elevated rack Mounting	ITD / NIATT
	Servers	Elevated rack Mounting	ITD / NIATT
	Wireless	Elevated rack Mounting	
Lightning	Switchgear	Recloseable relay	ITD City of Moscow
	CCTV / Video Detectors	Recloseable relay	ITD
	Signal heads	Lightning rod	ITD
	Signal controller	Recloseable relay	ITD
	Conflict monitor	Recloseable relay	ITD
	Archive	UPS	ITD / NIATT
	IT	UPS	ITD / NIATT
	Servers	UPS	ITD / NIATT
	Wireless	UPS	
	Microwave Transceiver		ID Admin
Vibration	Switchgear	Shock mounting	ITD City of Moscow
	CCTV / Video Detectors	Periodic manual testing	ITD
	Fiber splice	Periodic automated signal testing	ITD City of Moscow
	Fiber Cabinet	Shock mounting	
	Signal cabinet	Shock mounting	ITD
	Signal controller	Shock mounting	ITD
	Conflict monitor	Shock mounting	ITD
	Archive	Shock mounting	ITD / NIATT
	IT	Shock mounting	ITD / NIATT
	Servers	Shock mounting	ITD / NIATT
	Wireless	Shock mounting	
	Microwave Transceiver		ID Admin

Threat	Component	Mitigations	Owner
Power Outage	Switchgear	Battery backup	ITD City of Moscow
	CCTV / Video detectors	No known mitigation	ITD
	Loop detectors	No known mitigation	ITD
	Signal heads	No known mitigation	ITD
	Signal controller	No known mitigation	ITD
	Conflict monitor	No known mitigation	ITD
	Archive	UPS	ITD / NIATT
	IT	UPS	ITD / NIATT
	Servers	UPS	ITD / NIATT
	Wireless	Battery backup	
	Microwave Transceiver		ID Admin

Table 5 Electronic Threats

Threat	Component	Mitigations	Owner
Denial of Service	Switchgear	IP filtering Access restrictions Programmable switch	ITD City of Moscow
	CCTV / Video Detectors	Port restrictions IP restrictions Periodic self test	ITD
	Signal Controllers	Same as CCTV / Video Detectors	ITD
	IT	IP filtering Access restrictions Port restrictions Intrusion detection system Firewall Drive partitioning Redundant IT servers Formal periodic OS patch procedures	ITD / NIATT
	Servers	Same as IT	ITD / NIATT
	Wireless	Defensive sniffing Encryption Port restrictions IP restrictions	
	Microwave Transceiver		ID Admin
Settings Changes	Switchgear	Set / Reset procedures Initial testing Overburdened test	ITD City of Moscow
	Signal Controllers	Same as Switchgear	ITD
	Conflict Monitor	Same as Switchgear	ITD
	Microwave Transceiver		ID Admin
Data Storm	Switchgear	Self test Failover switch with isolation logic Remote test / resets	ITD City of Moscow
	Signal Controllers	Remote test / reset procedures Self test Failover controller with isolation logic	ITD
	Microwave Transceiver		ID Admin
Signal Degradation	Fiber optics	Periodic automated testing	ITD
	Fiber splices	Periodic automated testing	ITD City of Moscow
	Signal Controllers	Periodic automated testing	ITD
Unauthorized Access	Switchgear	Password protection IP Filtering	ITD City of Moscow
	CCTV / Video Detectors	Same as Switchgear	ITD
	Signal Controllers	Password protection IP Filtering Audit logging	ITD
	Archive	Audit logging Intrusion Detection System Firewall System Log monitoring Backup & restore procedures Password protection IP Filtered Defensive sniffing	ITD / NIATT
	IT	Same as Archive	ITD / NIATT

Threat	Component	Mitigations	Owner
Unauthorized Access cont.	Wireless	Encryption Defensive sniffing	
	Microwave Transceiver		ID Admin
Timing	Signal Controllers	Overburdened test	ITD
	IT	Overburdened test System log monitoring	ITD / NIATT
	Microwave transceiver		ID Admin
Bandwidth	CCTV / Video Detectors	Overburdened test	ITD
	IT	System log monitoring Overburdened test	ITD / NIATT
	Microwave Transceiver		ID Admin
Protocols	IT	Initial tests Overburdened tests Settings standards	ITD / NIATT
	Microwave Transceiver		ID Admin
Sabotage	Archive	Offsite storage Access restrictions System log monitoring Audit logs Back & recovery process Mirrored systems	ITD / NIATT
	Microwave Transceiver		ID Admin
Media Failure	Archive	Remote site storage Redundant backups Mirrored systems	ITD / NIATT
	Servers	Mirrored systems	ITD / NIATT
	Microwave Transceiver		ID Admin
Malicious Code and Viruses	Archive	Backup and restore procedures Automated anti-virus screening Access restriction Download restrictions Audit logs	ITD / NIATT
	IT	Same as Archive	ITD / NIATT
	Servers	Same as Archive	ITD / NIATT
Inadequate OS Resources	Servers	Overburden testing System log monitoring Failover servers	ITD / NIATT
NIC Failure	Servers	Redundant card Failover card	ITD / NIATT
Packet Injection	Wireless	Timestamp Encryption Defensive sniffing	