United States
Department of
Agriculture

Forest Service

Forest
Products
Laboratory

General
Technical
Report
FPL–GTR–191

Remote Monitoring of Historic Covered Timber Bridges for the Prevention of Arson and Vandalism

Brent M. Phares
Michael D. LaViolette
Terry J. Wipf
Michael A. Ritter

Abstract

More than 700 historic covered timber bridges remain in the United States. In recent years, a number of these bridges have been targeted by vandals and arsonists. Obviously, prevention of future acts of vandalism and arson is important to retaining the invaluable parts of our engineering heritage.

A research team from Iowa State University, working cooperatively with the United States Department of Agriculture Forest Products Laboratory (FPL), developed a remote security and fire detection monitoring system for covered timber bridges. This system automatically notifies emergency response personnel in the event that a fire is detected or if unauthorized activity occurs. The system was installed on the Cedar Bridge in Madison County, Iowa in 2005.

Three independent detection systems were software-integrated and installed. Fiber optic sensors were installed to monitor ambient temperatures throughout the bridge. An infrared camera, which is able to detect temperatures in an electronic image, was installed near the bridge. The data from these two parts of the monitoring system are used to detect rapid temperature changes due to fire and to also identify unauthorized persons on site. In addition, an industrial flame detector, which monitors radiant emissions within infrared and ultraviolet wavelengths, was mounted within the bridge interior. All of these components were connected using an onsite, wireless computer network with custom developed system integration software.

Keywords: Wood, Timber, Bridges, Covered, Arson, Security, Fire

February 2010

Phares, Brent M.; LaViolette, Michael D.; Wipf, Terry J.; Ritter, Michael A. 2010. Remote monitoring of historic covered timber bridges for the prevention of arson and vandalism General Technical Report FPL-GTR-191. Madison, WI: U.S. Department of Agriculture, Forest Service, Forest Products Laboratory. 27 p.

A limited number of free copies of this publication are available to the public from the Forest Products Laboratory, One Gifford Pinchot Drive, Madison, WI 53726–2398. This publication is also available online at www.fpl.fs.fed.us. Laboratory publications are sent to hundreds of libraries in the United States and elsewhere.

The Forest Products Laboratory is maintained in cooperation with the University of Wisconsin.

Sponsored by U.S. Department of Agriculture Forest Products Laboratory (USDA FPL Project 04-JV-11111130-093)

Preparation of this report was financed in part through funds provided by the U.S. Department of Agriculture Forest Products Laboratory through its research management agreement with the Center for Transportation Research and Education, CTRE Project 412-17-02.

A report from Center for Transportation Research and Education, Iowa State University
2711 South Loop Drive, Suite 4700
Ames, IA 50010-8664
Phone: 515-294-8103
Fax: 515-294-0467
www.ctre.iastate.edu

Contents

Remote Monitoring of Historic Covered Timber Bridges for the Prevention of Arson and Vandalism

Brent M. Phares, Principal Investigator
Associate Director, Center for Transportation Research and Education
Associate Director, Bridge Engineering Center
Center for Transportation Research and Education, Iowa State University

Terry J. Wipf, Co-Principal Investigator
Professor of Civil Engineering
Director, Bridge Engineering Center
Center for Transportation Research and Education, Iowa State University

Michael D. LaViolette, Former Bridge Engineer
Center for Transportation Research and Education, Iowa State University

Michael A. Ritter, Assistant Director
Forest Products Laboratory, Madison, Wisconsin

Introduction

Background

Covered bridges are unique structural systems. Typically designed and constructed in the mid- to early-1800s, covered bridges were originally devised as a way of constructing longer-lived bridges. By covering the primary structural components (heavy timber trusses and floor system) with less expensive and sacrificial coverings, bridge owners could extend the life of timber bridges. The principal need for this type of construction resulted because original timber bridges were constructed without modern preservatives. Therefore, when exposed to the environment, they tended to deteriorate relatively quickly.

Worldwide there are approximately 1,600 covered bridges, with more than half of these in the United States. Almost without exception, each of these covered bridges was designed for a specific location and to serve a very specific purpose in that unique location. As such, each bridge is essentially a one-of-a-kind work of art. Unfortunately, these irreplaceable structures have recently been vandalized and in some cases completely destroyed. Because of a best-selling novel and movie that featured the bridges, the covered bridges of Madison County in central Iowa are among the most famous of all the covered bridges. Unfortunately, one of these bridges, known as the Cedar Bridge, was completely destroyed by arson in the late 1990s.

Over the past 20 years, the Iowa State University (ISU) Bridge Engineering Center (BEC) has developed and deployed long-term monitoring solutions for bridges and other structures. Most recently, these activities have led to the development of unique monitoring systems that are autonomous and use state-of-the-art sensors. Coincidentally, the Forest Products Laboratory (FPL) has increased its interest in remote monitoring in housing and other applications. Because of the unique capabilities and the prospect for significant information and capability exchange, the FPL and the BEC began a collaborative research effort to address an important security need related to covered bridges. The results of that collaboration are the subject of this report.

Scope of Work

The objective of this work was to develop a cost-effective solution for providing security to covered timber bridges. The developed system was to be autonomous and provide security against what was believed to be the two most likely threats to covered timber bridges: arson and vandalism. Further, it was the intent that the security needs would need to be defined in two time regimes. First, fire detection would need to occur during all hours of the day with no reduction in sensitivity. Second, the detection of vandalism needed to occur only during select hours of the day, specifically, overnight. The two reasons for the latter restriction are that (1) all the bridges are open to the public and (2) because of less visibility, the most likely time for vandalism to occur was after dusk and before dawn. The developed system also needed to be capable of automatically and autonomously notifying local law enforcement and fire officials of the occurrence of both of the above.

Report Content

This paper describes several aspects of our research:

- Brief introduction to the topic of covered bridge security monitoring and description of the project.
- Review of published literature related to bridge security monitoring.
- Description of components and software that were developed and integrated to meet the goals of the project.

- Description of the testing on the developed security system. This testing was performed both in the laboratory located on the ISU campus as well as on-site following installation of the sensing components.
- Summary of the overall project and recommendations for future improvements to the developed system and for future research on this topic.

Literature Review

The following provides a very brief review of literature related to general security and bridge-specific security. In general, very little literature related to bridge security predates the terrorist attacks on September 11, 2001. Since that time, there has been new interest in identifying and securing bridges and tunnels that may be potential terrorist targets.

General Security

According to Stevens (2005), most security system design is completed using a multi-layered approach with "rings" of protection. When properly designed, these rings provide the best chances for detecting, evaluating, and responding to threats. Typically, each successive ring increases the level of security. Although there are variations in design, most include three rings of security that provide for (1) deterrence, (2) detection, and (3) delay. The two areas between the individual rings provide for locations or areas for incident response. The following generally characterize the three most common rings:

The first ring is generally designed to keep threats away. This can include such features as simple barriers to card readers and intercom systems. The goal of the first ring is to make a location unattractive to would-be threats.

The second ring generally tries to classify all persons within an area. In this instance, card readers and cameras that identify persons are typically used. In this ring, technologies such as revolving doors are also typically used.

The third and final ring generally tries to slow the progression of a threat to its intended target through the integration of electronically controlled locks and dual authentication devices. In general, these measures slow the movement of persons (both authorized and unauthorized) so that their presence and authority can be verified.

Bridge Security

As mentioned previously, little public consideration was given to bridge security prior to September 11, 2001. Following that day, a Blue Ribbon Panel on Bridge and Tunnel Security was requested to be established by the American Association of State Highway and Transportation Officials (Roberts and others 2003). That panel was asked to prepare a report on how to improve the security of bridges and tunnels and to develop strategies (both short- and long-term) and general guidance for improving security of major infrastructure assets. The resulting report documents much of the methodology that was followed in developing the conclusions. The framework by which security was to be addressed can be broken down into the following elements:

- **Identification of critical bridges through prioritization and risk assessment.** Although more detail is provided by the panel, the panel advocates broadly applicable and accessible prioritization methods and risk assessment based on rigorous engineering and mathematical principles.
- **Threats.** The following threats were considered by the panel:
  - Low- and high-tech conventional explosives
  - Penetrating devices
  - Low-tech, hand-held cutting devices
  - Truck and barge size explosives
  - Chemical and biological agents (tunnels only)
  - Incendiary explosives
  - HAZMAT release (tunnels only)
  - Intentional ramming via ship or barge
- **Damage.** The types of damage that are of concern include
  - Threats to integrity
  - Damage that inhibits functionality for 30 days or more
  - Contamination
  - Failure
- **Countermeasures.** Countermeasures were generally grouped into technologies that deter attack, deny access, detect presence, defend, or structurally harden. Because of the experience of the panel, only the last technology was given serious consideration. However, the panel noted that this consideration does not imply that the others are not valid options.
- **Knowledge and codes.** The panel basically concluded that, although some information is available, current codes and specifications are inadequate, and a significant research agenda is needed to provide the needed information.

From these elements, the panel developed seven primary recommendations categorized into three broad groups: institutional, fiscal, and technical. These are summarized below:

- Institutional
  - *Interagency coordination*. All stakeholders must collaborate to ensure that solutions meet the needs of all stakeholders.
  - *Outreach and communication strategies*. Information must be disseminated to decision-makers.
  - *Clarification of legal responsibility*. The Federal Highway Administration must seek to clarify the legal position of asset owners and owners must be advised of legal precedents.
- Fiscal
  - *New funding source for bridge/tunnel security.* Funds, beyond those already allocated by

federal-aid highway sources, must be allocated from the Department of Homeland Security.
    - *Funding eligibility.* Federal funding guidelines must be amended to be independent of deficiency as it is currently defined.
- Technical
    - *Technical expertise.* The Federal Highway Administration and the Transportation Security Administration must collaborate to engineer all security solutions.
    - *Research, development, and implementation.* Research and development that leads to methods and standards must be a national priority.

From these seven recommendations, the panel developed strategies for improving security of both bridges and tunnels. These strategies are broken down into short-, mid-, and long-term strategies and are further sub-categorized as follows:

- Policy and planning
- Institutional continuity
- Review and prioritization
- Research and development
- Technology development and dissemination

In terms of providing general guidance, the panel made the recommendation that all security improvements should be considered in the context of mitigating threats and consequences. Basically, the guidance is "keep the bad guys out," and if they get in, "know in advance how to deal with them."

In January 2005, the American Association of State Transportation Authorities (Crossett and Rhodes 2005) summarized the role of State Departments of Transportation (DOT) in homeland security. In that document, the authors summarize, among other things, countermeasures in basic terms as the following:

- **Deterrence and detection** of attacks by securing access to structures or mechanical systems, improving lighting, conducting frequent patrols, and installing electronic detection systems;
- **Defense** against attacks by installing physical barriers that increase stand-off distances from vulnerable structural components, such as bridge piers or tunnel ventilation systems; and
- **Design and re-design** of assets to harden them against potential attack methods, particularly explosive charges.

Although several similar accounts exist, Cho (2005) reports on the installation of cameras and sensors by the New York Metropolitan Transportation Authority for the prevention of terrorist acts. Although for obvious reasons, many details are omitted, Cho recounts that the plan is to, "… integrate proven technologies such as closed-circuit TV, motion sensors, intelligent video surveillance and perimeter sensors into one seamless system…" and that the system, "…can be expanded to include additional technologies, such as biochemical detection and explosion detection." In light of the information presented above, this installation is an example of a context-specific system design that takes into account the likely threats and the need for future expansion capabilities.

Like some of the literature cited above, Williamson and Winget (2005) describe countermeasures to address threats to bridges as the following:

- **Planning and coordination measures.** These measures generally relate to the development, communication, and re-examination of plans to deal with threats.
- **Information control measures.** These measures are all related to sharing information among people and strive to give owners guidance on to whom and to what level information should be shared.
- **Site layout measures.** These measures (e.g., using lighting, vegetation, or landscaping) strive to improve the security of an asset simply by changing the environment in which it operates.
- **Access control/deterrent measures.** These measures include technological and policy changes that make it more difficult for threats to gain access to assets.

Deception measures. These measures complement those above by creating the appearance of a much larger web of protection. Because of the similarity in deployed technology, Wolff (2003) offers protocols for integrating bridge security into Traffic Management Centers. Although several significant barriers to this integration exist, Wolff offers the following general guidelines:

- Co-locate with law enforcement
- Co-locate with emergency management
- Determine critical bridges
- Explore methods to increase detection
- Explore methods to prevent access
- Establish alternate routes in the event that an attack occurs
- Assign a person or persons to monitor video of critical bridges
- Increase inspections and patrols of critical bridges during increased threat levels

Security System Design

Initially, a combination of three sensing systems was proposed to detect vandalism and arson at relatively remote bridge sites. The first system consisted of fiber Bragg grating (FBG) sensors. FBG sensors, which are a specific type of fiber optic sensor (FOS), could be installed at strategic locations throughout the bridge so that they could monitor ambient temperature changes throughout and within the bridge. Second, an infrared (IR) camera could be installed

Figure 1. Cedar Bridge location near Winterset, Iowa.

in a location where it could view the entire bridge site and be configured to detect both the presence of humans during restricted times as well as the presence of a fire. The third system included a standard closed-circuit TV (CCTV) camera. Later, the addition of an industrial flame detector unit was added to the system following the discovery of an independent effort to install CCTV cameras at each Madison County covered bridge.

Bridge Site Layout

The Cedar Bridge, which was the bridge selected by the owner to install and demonstrate the developed system, is located approximately 2 miles north of Iowa Highway 92 near Winterset, Iowa (Fig. 1). The bridge is situated in a county-maintained park in a somewhat remote area with limited residences nearby from which the bridge can be observed.

The bridge crosses Cedar Creek approximately 300 feet from the nearest frequently traveled road. Further complicating the preservation of the bridge is that the bridge site is screened from the view of passing traffic by a large number of mature trees (Fig. 2). This type of remote location is common for the majority of covered bridges in the United States and is one of the reasons that remote security systems are vitally important to the protection of these historic structures.

Individual Sensor Components

Based upon a significant paper review of remote monitoring technologies, the research team decided that the security system would consist of three somewhat redundant sensing systems. The three sensing systems include infrared camera technology, commercial flame detector technology, and FBG sensor technology. The three individual sensing systems were to be integrated into a single system that provided overall detection.

Infrared Camera

A detailed examination was performed to determine the capabilities and limitations of infrared camera technology. To adequately monitor both the interior and exterior of the bridge, we originally thought that at least two infrared cameras would be necessary. However, upon the basis of further design and site limitations, we decided that a single, well-placed infrared camera could provide adequate protection.

Following a search for available IR camera systems, we contacted several manufacturers and supplied them with a site plan and general requirements for this project. The manufacturers were asked to recommend and provide a price quote for specific products that satisfied the project requirements. The recommendations received from the various manufacturers were as follows:

- Company A recommended a laser infrared illuminator at an estimated cost of $13,000. The illuminator would energize the surrounding area with infrared light and allow regular monochromatic cameras to “see” the infrared spectrum.
- Company B recommended two of their cameras. These cameras measure the temperature at every pixel in the field of view and cost from $10,000 to $20,000 each,

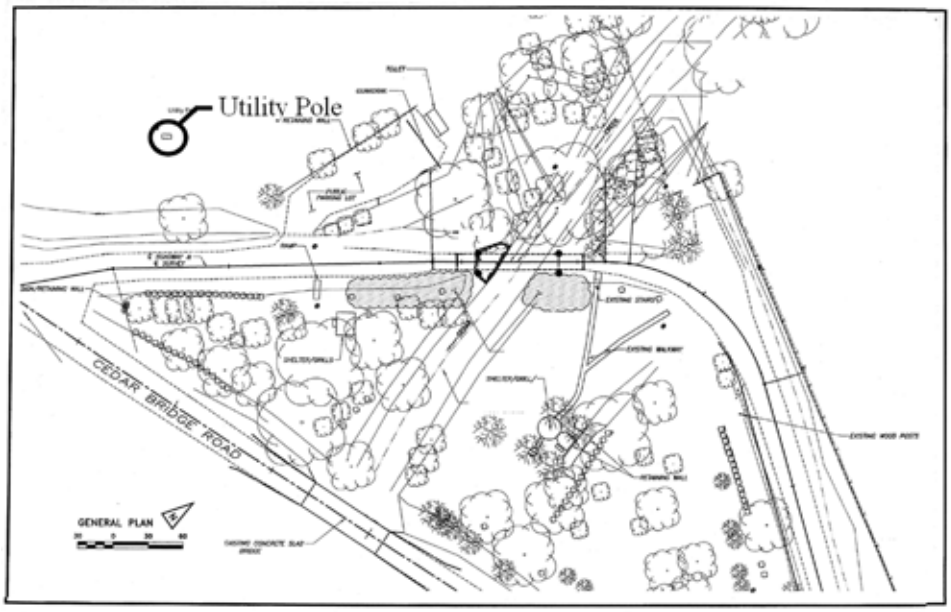


Figure 2. Bridge site plan view.

depending on field of view and programming requirements.

- Company C recommended a 3-camera system (with proprietary software) with an estimated cost of $140,000.
- Company D recommended their camera, which produces infrared images but does not permit the user to measure specific temperatures within the field of view. The estimated cost of these cameras was $8,000–$9,000 each.
- Company E recommended their camera, which has a regular visual camera integrated with an infrared camera and is provided with a customizable software package. The camera has an estimated cost of $50,000–$60,000.

Consideration was narrowed to two manufacturers based on the following criteria for this project:

- To detect the presence of humans during the hours of darkness, the camera must be able to measure specific temperatures within the IR range.
- The price of the IR camera must fit within the overall project budget.

The cost estimate for the Company C system exceeded the entire project budget; thus, this unit was eliminated from consideration. The Company D camera and Company A illuminator did not permit specific temperature readings within an image and would not have been adequate for the detection of a fire event and were eliminated from further consideration.

The two remaining companies were asked to demonstrate the capabilities of their respective cameras. Company E demonstrated their camera (Fig. 3) using an online Web link and Company B brought their camera (Fig. 4) to the BEC and provided indoor and outdoor demonstrations of the camera, including a summary of the software available with the camera.

Figure 3. Infrared camera.

I-rule.net, a small internet service provider in Winterset, Iowa, working independently of the research team, received a grant to install Web-based video cameras at all five covered bridge sites in Madison County. These cameras were also installed and maintained by I-rule. The BEC/FPL research team negotiated an agreement to work in cooperation with I-rule.net on the security monitoring of the Cedar Bridge.

Figure 4. Infrared camera.

The original research plan included the purchase and installation of CCTV cameras to observe the interior and exterior of the bridge. The high cost of the cameras, combined with the existing plans to install and maintain a Web-based CCTV camera at the site, allowed the research team to eliminate this part of the overall security system.

The Company E camera was eliminated from future consideration because the integrated visual spectrum video camera would no longer be needed. In addition, the proprietary software package supplied with this unit would not be able to interface with the custom software needed to control the various other sensing systems to be installed elsewhere on the bridge.

The selected infrared camera offered a number of advantages for the Cedar Bridge project:

- Optional software package
- Interchangeable lens with varying fields of view (12, 25, or 45 degrees from the axis)
- Lower price than the comparable, but newer, model camera
- Pole-mountable weather-proof camera enclosure included

The camera was purchased for approximately $15,000 and came with a pole-mountable camera enclosure, specifically designed for use with infrared cameras. The infrared camera was mounted on an existing utility pole approximately 300 feet southwest of the bridge (Fig. 2) to monitor the exterior of the bridge and the approach roadway. However, from this location, the camera is not able to monitor activities within the covered portion of the bridge.

Flame Detector

Recommendations from the ISU Department of Environmental Health and Safety (EHS) were used to quickly eliminate possible alternative fire detection systems for the interior of the Cedar Bridge. The alternatives that were considered and rejected included the following:

- **Standard smoke detectors**. They are considered unreliable in this environment, as road dust would likely result in numerous false alarms. **Electronic temperature gauges**. These would function quite well in this application, but would need to be located at numerous locations throughout the bridge and would essentially duplicate the function of the fiber optic sensors.

Based on recommendations from EHS, we searched for industrial fire detection sensors that would function reliably in a semi-harsh environment. In particular, focus was placed on flame detector devices that are designed to detect a fire based on the characteristic signature of a burning flame in three wavelength spectra (infrared, ultraviolet, and visible light) quickly and while the fire is still very small. The use of multiple light spectra sensors within a single detector unit, as it turns out, greatly reduces the occurrence of false alarms. These types of flame detector units are widely used in industrial applications (factories, warehouses) around the world.

In fall 2004, two industrial flame detector manufacturers were contacted. These two manufacturers offer very similar products, although one model was slightly less expensive. We ultimately purchased an ultraviolet–infrared electro-optical digital flame detector (Fig. 5). The specifications for this flame detector state that a 1 ft^2 fire can be detected at a distance of 15 ft within 5 seconds.

The flame detector outputs a fault circuit and a fire circuit. Each of these circuits operates in a binary mode and the voltage output by each circuit can be read using a multimeter or by other means. The fault circuit is tripped after the flame detector performs a self-check and finds a problem with its internal operation. The fire circuit is tripped when the unit detects the presence of a fire. To reduce the number of false detections, the unit was programmed to trip the fire circuit only when two of the three wavelength spectra independently identified a positive condition. The output combined with internal redundancy made integration of this sensing system relatively easy while also being very reliable.

Fiber Optic Sensors

The BEC has used FOS in numerous other projects to monitor changes in mechanical strain in structural bridge components (instead of traditional electrical resistance strain gauges). However, these sensors had not previously been used for measuring ambient temperature at a series of points throughout a structure.

Figure 5. Flame detector.

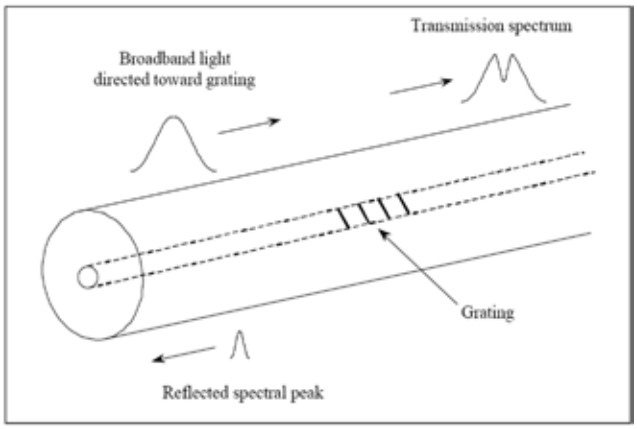


Figure 6. Fiber Bragg grating operation.

A FBG sensor, a specific type of FOS, consists of a series of etched perturbations in the index of refraction along a short length of glass fiber (Figs. 6 and 7). This grating reflects a spectral peak and permits the remainder of the light to be transmitted along the fiber. The reflected spectral peak is based on the grating spacing and, therefore, changes in the length of the fiber (strain) will change the grating spacing and thus the wavelength of light that is reflected back to the source.

The center wavelength of each sensor in a series is spaced such that no signal overlaps between adjacent sensors. The leading end of the chain is connected to a device known as an interrogator, which transmits a pulse of very pure light

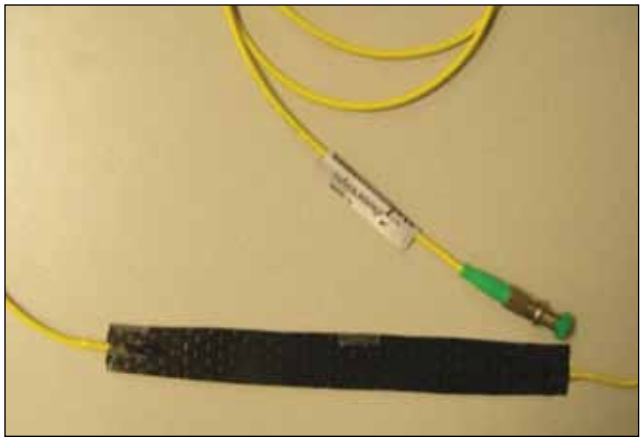


Figure 7. Fiber optic fiber Bragg grating sensor.

along the glass fiber to each sensor. The reflected center wavelength of light from each sensor is recorded and compared with the initial center wavelength, and any change in wavelength is proportional to a change at the sensor location. Based on the change in wavelength, either a mechanical strain or temperature change can be calculated depending upon the application.

Prior to purchase of a fiber optic sensor system for the Cedar Bridge, a number of laboratory evaluations were made using an interrogator and sensors on loan from the manufacturer. These evaluations will be presented in the System Evaluation section and were used to determine how many sensors would be required to adequately monitor the bridge deck of the Cedar Bridge.

Security System Integration

The complete remote security system was developed using an onsite computer to collect data from the three sensing systems to determine whether a fire or intruder event had occurred and notify interested parties. The development of integrated software and hardware communications to perform this are presented in the following paragraphs.

Hardware Communication

An onsite wireless Local Area Network (LAN) was created using network interfaces supporting both Ethernet and wireless communication technologies. The onsite network consists of four devices:

- Flame detector
- Infrared camera
- Optical sensing interrogator
- Onsite desktop personal computer

The onsite computer was used to run the custom software developed to control the monitoring system. The computer system had a 700 MHz processor, 256 MB RAM, 20GB hard drive, Microsoft Windows XP Professional

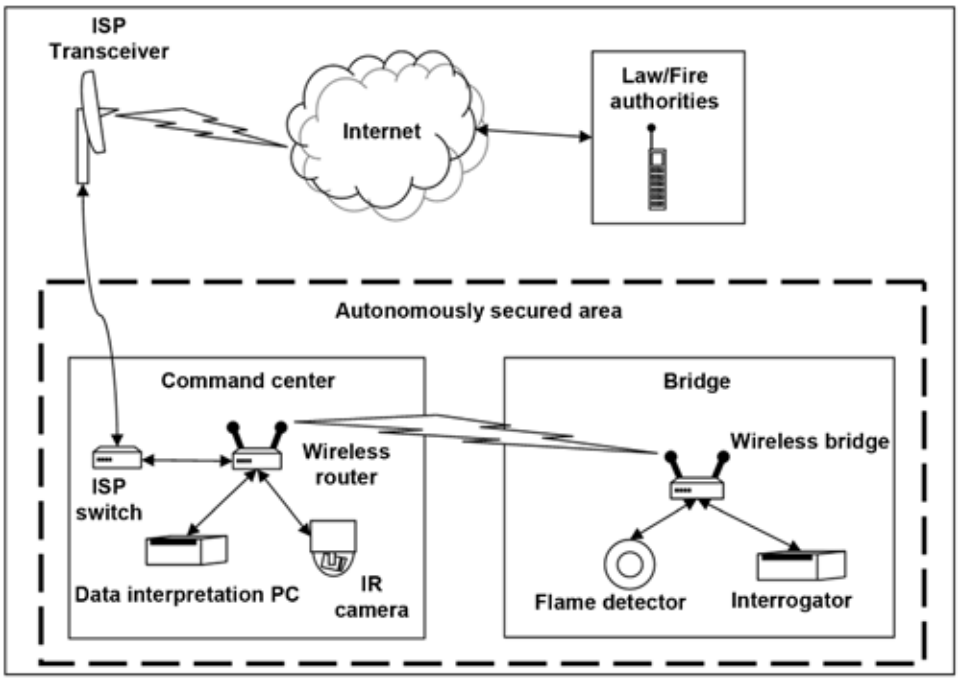


Figure 8. Schematic view of security system layout.

operating system (Microsoft Corporation, Redmond, WA), and a 10/100 BT Ethernet card.

The camera and the PC were connected to a wireless router, and the flame detector and interrogator were connected to a wireless bridge. The wireless router and the wireless bridge were purchased at a total cost of approximately $150.

The flame detector required additional equipment to establish an ethernet connection to the system. A pair of signal conditioners connected to the fire and fault relay wiring of the flame detector was added to convert an output voltage from the device to a numeric output which could be read by a microserver attached to the wireless bridge through an ethernet connection. A 5-volt power supply was connected across the two flame detector relays, which were then connected to the signal conditioners. In this way, a zero-voltage reading indicates no fire or fault and a 5-volt reading indicates a fire or fault has been detected. The total cost of these components was approximately $750.

A schematic view of the onsite monitoring components is presented in Figure 8.

Software Communication

The software that monitors and controls all the sensing systems was developed using object-oriented ActiveX dynamic-link libraries (DLL) language modules. The DLLs contain reusable functions and data, and ActiveX technology, based on a Microsoft standard that defines how software components interact with each other. In total, researchers at Iowa State University developed four DLL modules—three to control each of the three major sensing systems and a fourth to control and integrate the other three modules.

The modules for each sensing system were written separately to decrease system maintenance time. In this way, when an update is required for one module, the entire program does not need to be recompiled—only the module needing to be updated. The main module, which controls the three component modules, is used to enable or disable the components that control any of the sensing systems.

Three possible events (fire, person, or fault) can be detected by the sensing system at the Cedar Bridge. Of these, the most significant is related to a fire, which may be detected at any hour of the day, or a person, who may be detected during late night hours. Each of the three sensing system modules was developed to send a true/false status report to the main module. Depending on the module, this status report represents either a “fire–no fire” or “person detected–no person detected” or a “fault–no fault” report.

The function of the four DLL modules is as follows:

- Main module—manages the inputs and outputs from the other modules. The main module only takes action when a fire, fault, or person event status is reported by one or more of the sensing systems.
- Flame detector module—sends two types of status reports to the main module: fire or no fire, and fault or no fault.
- Interrogator module—sends only one type of event status report to the main module: fire or no fire.
- Infrared module—sends two types of event status reports to the main module: fire or no fire, and person or no person.

Figure 9. Sample image taken from onsite infrared camera following a person event.

If a fire event report is received by the main module from any of the sensor modules, the following events occur:

- The main module sends this event status to the other two sensing modules for confirmation.
- An e-mail message is dispatched to a predetermined list of recipients, informing them that a fire has been detected on the bridge. The list of recipients can be easily changed to add or delete recipients.
- Each of the three sensing-system modules is given instructions to store buffer data and record live data for a specified amount of time (typically 5 minutes).
- Once the specified buffer period time has elapsed, all three sensing-system modules are instructed to save both the data from the buffer and the live recording to a specified location on the onsite computer.

In the event that the infrared camera detects a person onsite at the bridge during late night or early morning hours, the infrared module sends a person event status report to the main module. At this point, the following events occur:

- The IR module then instructs the camera to record an infrared picture at specified intervals (10 seconds) for a specified period of time (1 min) (Fig. 9). These pictures are then saved to a specified location on the onsite computer.
- An e-mail message is dispatched to a predetermined list of recipients at the BEC, informing the BEC that a person has been detected at the bridge. The list of recipients can easily be changed to add or delete recipients.

In the event that a fault status report is received by the main component, an e-mail is sent to a predetermined list of recipients at the BEC, informing them that a fault has been detected within the flame detector. The flame detector can be powered off and restarted remotely.

Sensing Module Programming

Each of the sensing modules can be configured and adjusted to fine-tune the sensitivity of their respective event triggers and reduce the number of false alarms. The logic used to develop the programming for each sensing module is presented in the following paragraphs.

The flame detector module has a number of configurable parameters that relate to detection of a fire or a fault. A positive voltage reading must be received for the flame detector module to send a fire or fault event report to the main module. The administrator sets the minimum voltage value before a positive value is recorded for either a fire or fault. A minimum number of consecutive positives—typically five—must occur before the event report is transmitted to the main module. The flame detector is polled on a set time interval (typically once per second) by the flame detector component to determine the voltage readings.

The interrogator module can be adjusted to control the threshold temperature that must be recorded prior to issuing a fire event report to the main module. A specified number of consecutive readings above the threshold temperature (typically 5) must be recorded before the fire event is reported to the main module. The interrogator module includes a data buffer that stores the temperatures recorded by each FOS for a preceding set amount of time. It is these data that are saved after a fire occurs. An initial temperature and corresponding center wavelength for each FOS was recorded at the time of installation. The recorded center wavelength values are converted to temperature readings as specified by the manufacturer and compared with the initial values. The rate of temperature change at a particular sensor must exceed a specified threshold value prior to a fire event report being transmitted to the main module.

The final sensing-system component is the IR camera. The first parameter set in the camera component is how often the camera will send data to the camera component. The data that are sent by the camera can be either a picture or temperatures associated with a configurable box or spot in the camera's field of view. The administrator can create up to four boxes and four spots of interest in the camera's field of view. The temperature data corresponding to these boxes are the average, minimum, and maximum detected, and the data corresponding to the spots are the detected temperature. The camera component has a data buffer that stores the data from the camera for a predetermined set amount of time. In order for the camera component to issue a fire alarm, the maximum temperature in a box of interest must exceed a set threshold temperature, and this condition must be met for a specified number of consecutive readings. The camera component also needs to detect the presence of humans during restricted times. Thus, the restricted times need to be set to

prevent false alarms from occurring during regular visiting hours. If a person is detected during the restricted times or a fire event is issued, the camera component will take pictures at a set time interval for a set time period.

The camera module uses two independent tests to detect a person (note that people can be distinguished from animals through the heat signatures associated with their hands and head) within the field of view:

- **Using a threshold temperature as an indicator.** When the camera module records a maximum temperature reading exceeding the threshold a set number of consecutive times, a person event status report will be sent to the main module.
- **Using a temperature differential as an indicator.** In this test, two rectangular regions are defined within the field of view. A temperature-control box is defined somewhere in the camera's field of view where people are highly unlikely to be present. A temperature test box is defined and contains the regions most likely to contain a human. The surface temperature from the control box or spot is compared with the temperature in the test box. If the difference between the two temperatures exceeds a specified value, a person event report is sent to the main module.

In most cases, the temperature differential method appears to give more reliable results and reduces the potential number of false alarms. Onsite test results will be presented in the System Evaluation section. Examples of events recorded by the onsite monitoring system are in the Appendix.

Remote Monitoring

A local internet service provider (ISP) in Madison County was hired to enable the BEC to remotely monitor the system installed at the bridge. The research team was able to take advantage of the fact that the local businessman who owned the ISP was the same individual who has received a grant to install Web-based security cameras at all covered bridge sites in Madison County. Since the Web-based cameras were connected to the internet via a wireless access point (WAP) near the bridge, it was very convenient to use this same connection for data transmission from the onsite monitoring system. In fact, the utility pole where the infrared camera was to be installed is the same location where the Web-based camera and the WAP were installed. An IP address was assigned by the local ISP to the onsite computer. From the WAP, a signal is transmitted to the nearest wireless transceiver within the local ISP network to the ISP's main computer server, which is connected to the internet through telephone lines.

The monitoring system was designed such that it can be remotely accessed via a desktop connection to connect to the IP address assigned to the onsite computer. This remote access allows the user to see and control the onsite computer from anywhere in the world.

Figure 10. Cabinet installed near utility pole.

Onsite Installation of Components

The selected sensors and computer equipment were installed at the Cedar Bridge site during the summer and fall of 2005. The following briefly summarizes the installation and connection of these components.

Weather-Tight Cabinets

Two weather-tight, steel, locking cabinets, formerly used to house traffic signal equipment, were installed at the bridge site to protect the instrumentation and monitoring equipment. These cabinets, and the equipment they contained, are as follows:

- Located beneath the south approach span of the bridge—containing the FOS interrogator, wireless bridge, and the 5-volt power supply and signal conditioners for the flame detector.
- Located near the base of the utility pole—containing the onsite computer and wireless router (Fig. 10).

The cabinets were supported on small, cast-in-place concrete pads and supplied with electrical power through an agreement between Madison County and the Winterset Municipal Utility. The Madison County engineer supplied equipment and labor to excavate a small trench to permit shared electrical power between the cabinets. Unfortunately, the distance between the cabinets prevented the direct connection of computer equipment and components using the same trench. Both enclosures were equipped with a heater and a fan to help control the temperatures within the cabinets. The two enclosures were purchased for approximately $800 each and were installed in summer 2005.

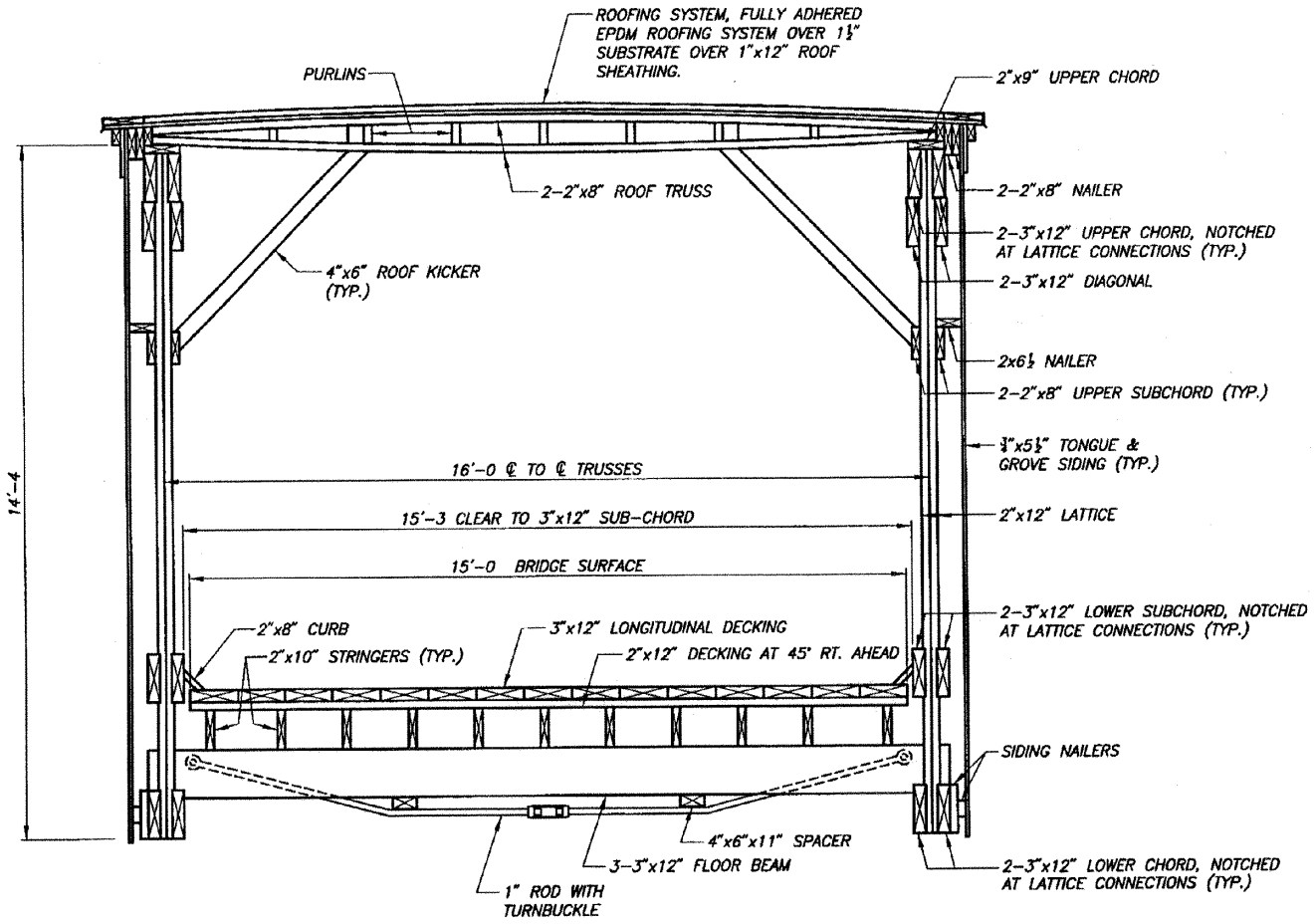


Figure 11. Section view of bridge showing original and revised location of flame detector.

Flame Detector

The initial location selected for the flame detector was within the roof truss members directly above the south portal of the bridge. This location provided a very uniform monitoring coverage of the south half of the bridge deck, but unfortunately, the view from this point was largely obstructed by framing members of the bridge roof system (Figs. 11 and 12).

The flame detector was subsequently relocated to a location near the southwest corner of the roof of the covered portion of the bridge (Fig. 13). All the wiring was concealed between the truss framing and outer sheathing of the bridge. The flame detector was covered with a small wooden box to help preserve the aesthetic appearance of the bridge. Note that even in the alternate location, the flame detector view was still slightly compromised by obstructions from roof kicker members, and multiple flame detectors would be required for true 100% coverage (Fig. 13).

Fiber Optic Sensors

A total of 12 fiber optic sensors were installed in two series of six and were located along the outer edge of the roadway at the south end of the bridge (Fig. 14). The sensors were attached to the back side of the truss framing and hidden from view to the greatest extent possible (Fig. 15).

Insulated staples were hand-hammered to attach the connecting patch cords to the truss framing. The staples were selected to provide a loose fit around the fiber to ensure that the sensors were not rigidly attached to the framing and thus were able to measure thermal changes and not mechanical strains. Fiber optic patch cords were run from the two closest FOS along the underside of the bridge, into the enclosure and connected to the interrogator.

Although precautions were taken to conceal the wires during installation, one series of six sensors (along the east truss) were disabled by an unknown person during the early months of 2006 (Figs. 16 and 17). The glass fiber within each patch cord is protected by a thin layer of Kevlar within the outer jacket, so it takes considerable effort to cut one of these fibers, which makes it unlikely that this damage was caused by any accidental event. Loss of the fiber was reported as an "event."

Infrared Camera

The camera enclosure was installed approximately 25 ft above the ground on the previously mentioned utility pole (Fig. 18). The infrared camera was aligned to view the entire bridge site including the approach roadway on both ends of the bridge. Unfortunately from this vantage point, a single mature tree created a significant viewing obstruction during

Figure 12. Original location for flame detector above south portal.

Figure 13. Flame detector installed near southwest portal of bridge.

the growing season. A request was made of the county parks department to selectively prune some of the branches.

Numerous pieces of hardware were used in the installation of the system on the bridge. These pieces of hardware were used for connections, camouflage, and protection of wiring. The total cost for the miscellaneous pieces of hardware was approximately $2,000.

System Evaluation

Each of the sensor components was evaluated individually for effectiveness and reliability in the laboratory located on the ISU campus as well as following installation in the field. The results of these evaluations are presented here.

The recognized industry standard used for fire detection equipment uses a gasoline fire covering an area of 1 ft^2 (Factory Mutual 1994). A gasoline fire was considered too

Figure 14. View of flame detector slightly obscured by roof kicker members.

volatile for use on an historic covered bridge; therefore, denatured ethyl alcohol was used for both the laboratory and field evaluations in place of gasoline. A galvanized metal pan measuring 12 in. diameter (0.79 ft^2) was used to contain the alcohol during each test.

Laboratory Evaluation

The individual sensor components were tested for sensitivity and reliability prior to their assembly into a complete system. The tests performed for this current study used three sources of heat and flame including

- Butane lighter (tested at 3-in. increments from sensor)
- Disposable propane torch (tested at 6-in. increments from sensor)
- Alcohol pan fire as described above (tested at 1-ft increments from sensor)

In each test, the heat source was positioned near the sensor and data collected until a steady-state was reached. The heat source was then moved to the next incremental distance from the sensor and the process repeated. The goal with this testing was to determine the distance and associated rate of detection at which a fire could be detected by each sensing system.

Fiber Optic Sensors

A series of tests was performed to determine the response of the FOS to the heat generated by each source. The sensor was positioned at a range of distances up to 6 ft from the heat sources. The results from these tests are shown in Figures 19 and 20.

From these test results, it is evident that the fiber optic sensor was not able to record any significant temperature changes from the pan fire beyond approximately 2 ft. However, since the installation location on the actual bridge will

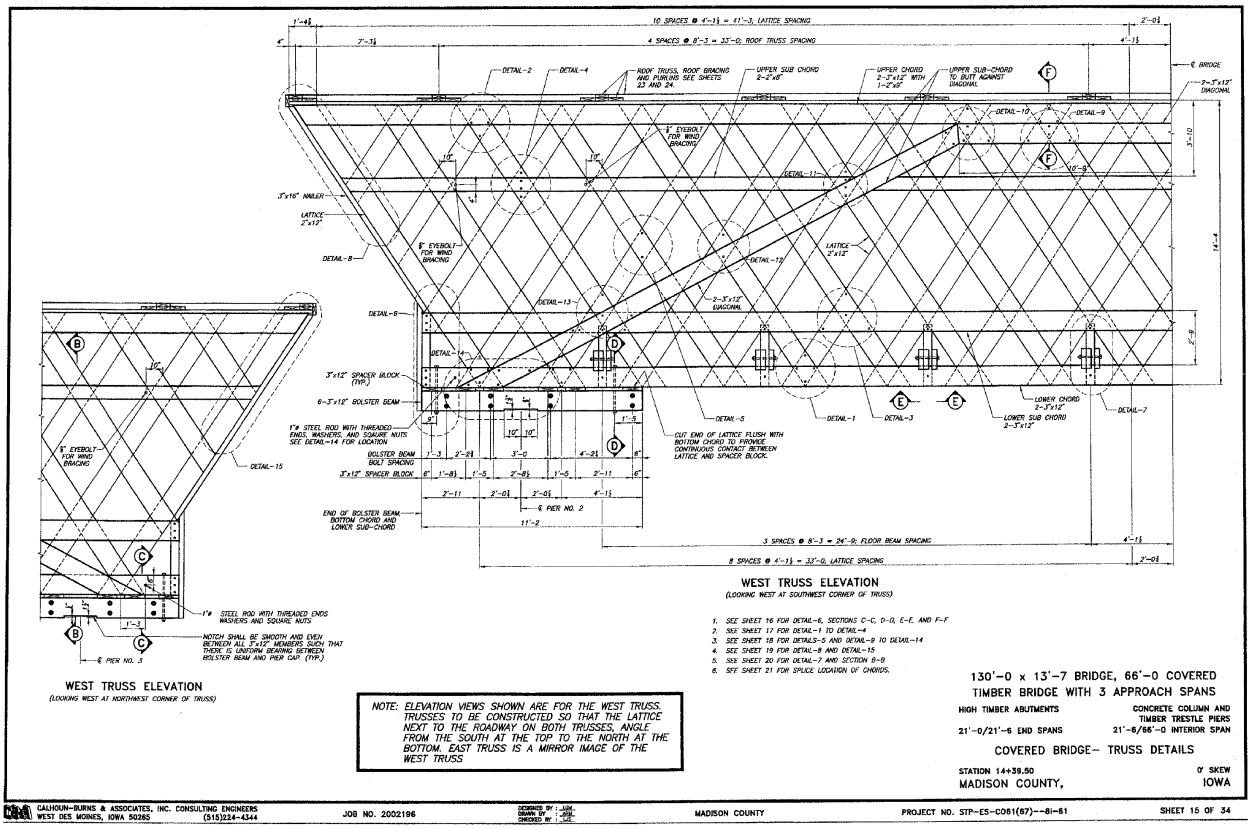


Figure 15. Truss elevation showing fiber optic sensor locations.

Figure 16. Installation of fiber optic sensors behind truss members.

Figure 17. Fiber optic sensor series damaged by possible vandalism.

Figure 18. Infrared camera (bottom camera) and web-based video camera (top camera) attached to utility pole.

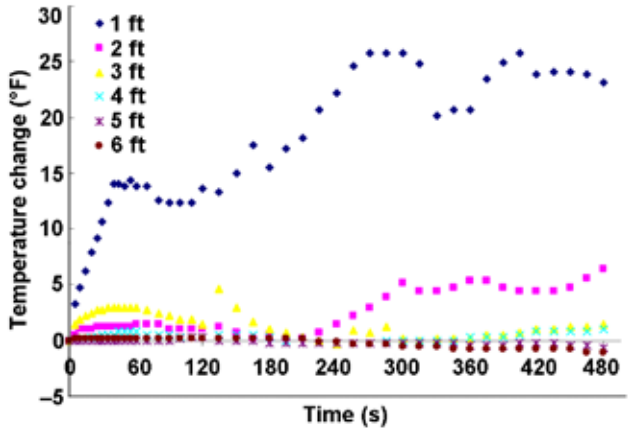


Figure 19. Fiber optic sensor sensitivity to pan fire.

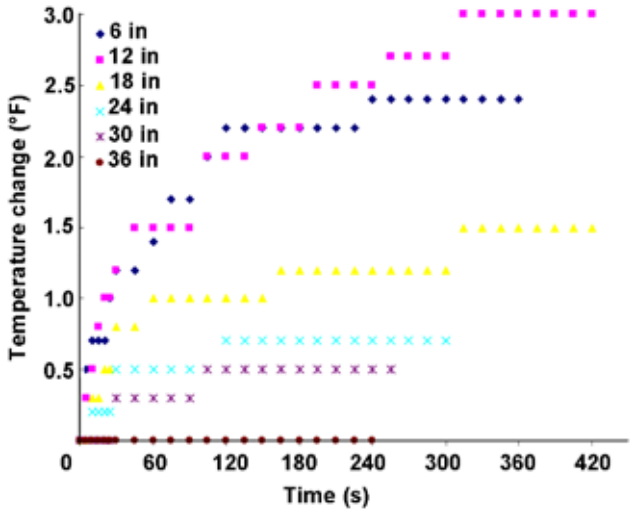


Figure 20. Fiber optic sensor sensitivity to propane torch.

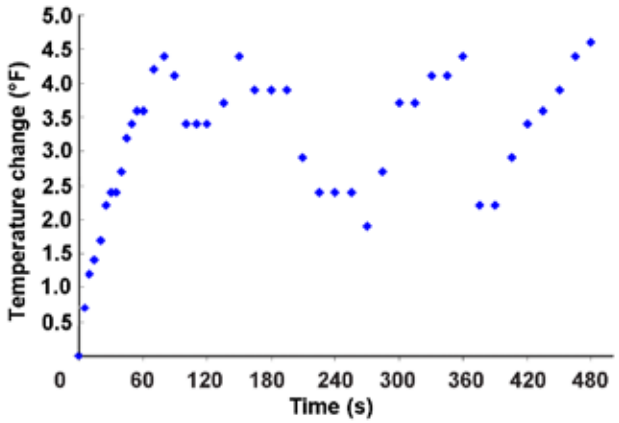


Figure 21. Fiber optic sensor sensitivity to pan fire with wood shielding.

be near the deck level and hidden behind the truss, a fire very likely could be started in this area (and within a few feet of a sensor).

In the case of the propane torch, the maximum temperature change recorded was approximately 3 degrees. We thought that perhaps 5 degrees is the minimum threshold of localized temperature change that could be reliably used to trigger a fire alarm, and thus no further testing was performed using smaller heat sources, for instance, the butane lighter.

To test the ability of a FOS to detect temperature changes when separated from the heat source by a layer of wood, a similar test was performed using a nominal 1- in.-thick layer of cedar wood as a screen. For this test, the fire was located 1 ft from the sensor. The results from this test are shown in Figure 21. The maximum recorded temperature change was approximately 4.5 degrees, indicating that a FOS would not be able to reliably detect a fire on the opposite side of a timber member or exterior sheathing.

Infrared Camera

Two series of laboratory tests were performed using the infrared camera using different fire sources and at varying distances from the sensor. Independent measurement of fire temperature was made using a handheld infrared thermometer. In each test, five infrared images of the flame were captured at 15–20 second intervals. The following heat sources were used to evaluate the infrared camera sensing system:

- A butane lighter located at 1-ft increments up to 20 ft from the camera
- Pan fire located at 10-ft increments up to 250 ft from the camera

Subsequent analysis of the infrared images from both the lighter tests and the pan fire tests indicate that the IR camera is able to detect temperatures very close to the actual fire temperatures almost immediately. A sample of the IR camera images recorded is presented in Figures 22 and 23.

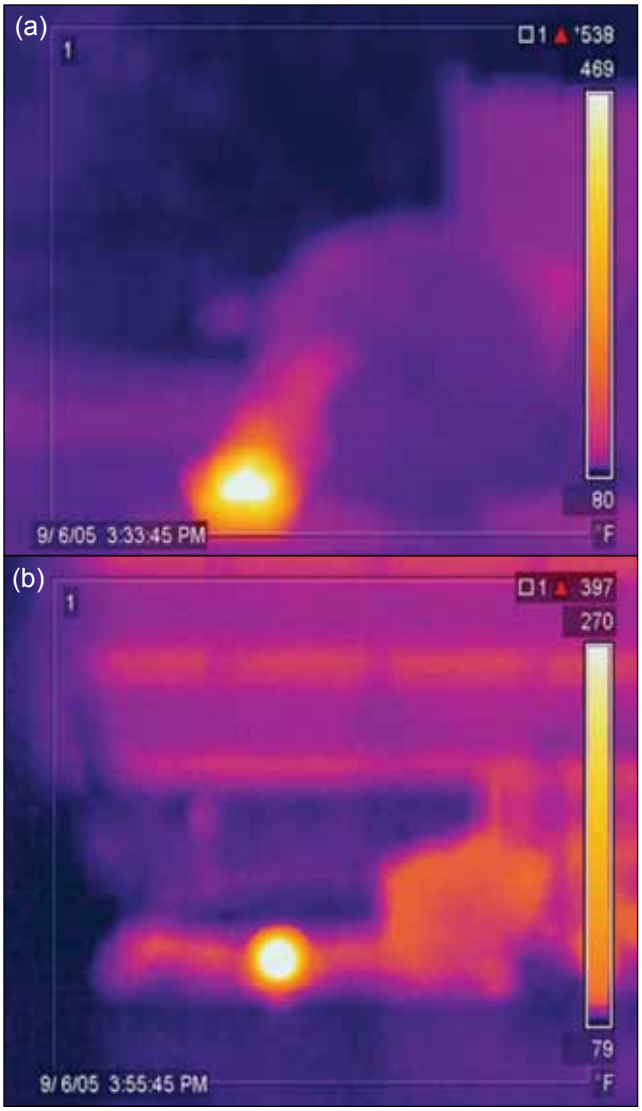


Figure 22. Infrared photo—pan fire with a) fire located 30 ft from camera and b) fire located 100 ft from camera.

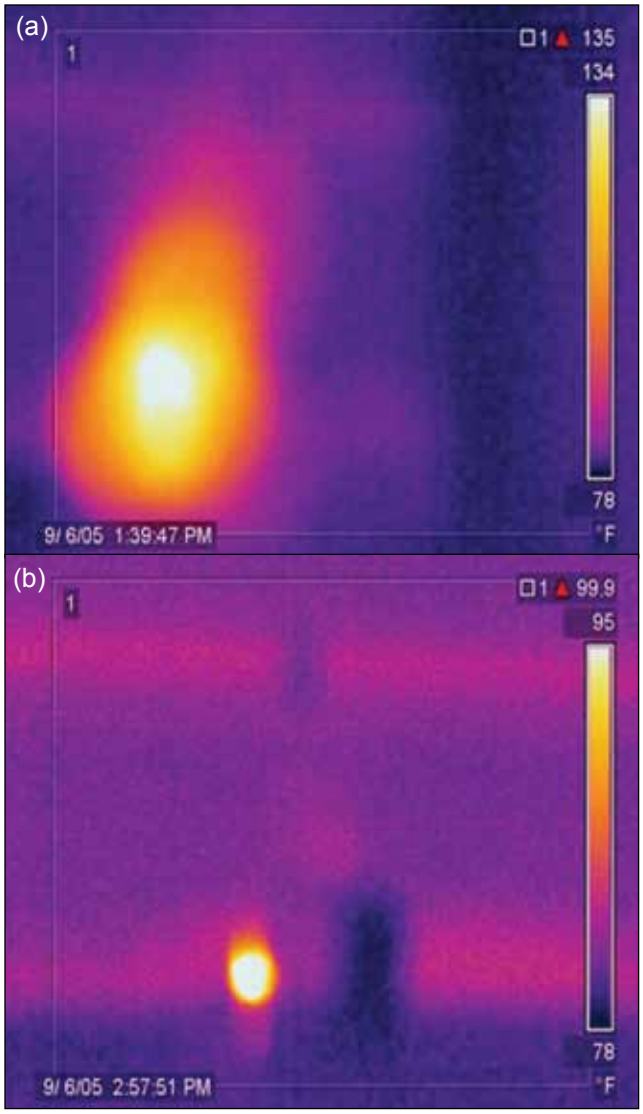


Figure 23. Infrared photo—butane lighter with a) fire located 2 ft from camera and b) fire located 20 ft from camera.

Flame Detector

A series of laboratory tests was performed to determine how quickly the flame detector could reliably detect a fire of various sizes at a range of distances. An initial series of tests were performed using the 12-in. pan fire, located at a distances of 10–80 ft from the source. The laboratory setup for this test is shown in Figure 24.

The manufacturer claims that the sensor can reliably detect a 1 ft^2 pan fire at a distance of 15 ft in 5 seconds. Note that although the test results indicate detection occurs at approximately 7 seconds, the pan fire used for this test covers approximately 22% less area than the reference fire used by the manufacturer. The results of these tests are presented in Figure 25.

An additional series of tests was performed using a butane lighter as the flame source. In this test, the flame detector was located at distances from 3–24 in. from the source. Beyond this distance, the sensor could no longer detect the flame within 5 min. The results of these tests are shown in Figure 26.

Onsite Evaluation

A series of onsite tests was performed to evaluate the individual component's effectiveness in detecting fire events. In each of these fire tests, a 12-in. diameter metal pan was used to contain the fire and a small four-wheeled cart was used to allow the fire to be easily moved on the bridge deck without the need to extinguish the fire prior to each test.

All fire tests were performed with the knowledge and consent of the local fire and law enforcement authorities. In addition to extreme caution used by the research team when

Figure 24. Laboratory setup for flame detector tests.

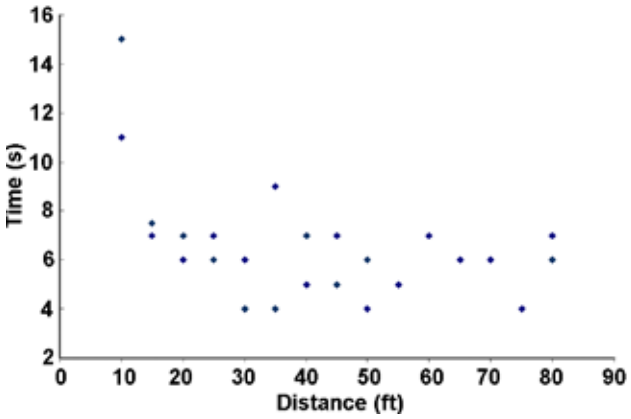


Figure 25. Flame detector sensitivity to pan fire.

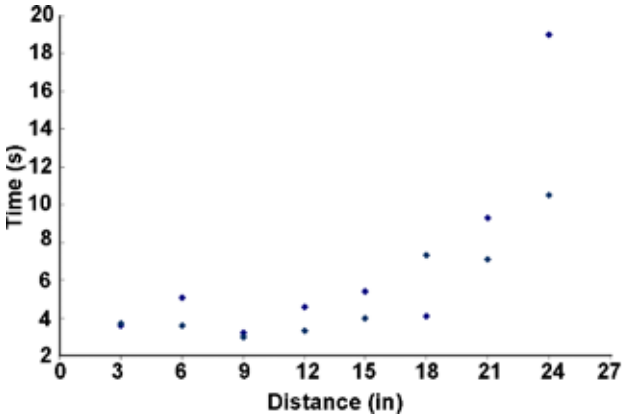


Figure 26. Flame detector sensitivity to butane lighter.

Figure 27. Pan fire test on south bridge approach span.

using flammable materials near the bridge, a fully-charged fire extinguisher was available at all times during these tests.

In addition to fire testing, the infrared camera was tested for its ability to detect a person moving about at the bridge site during selected hours of the day.

Fiber Optic Sensors

The FOS were evaluated for their ability to detect a standard pan fire during both daylight and darkness. The pan fire was located as near to the bridge sheathing as deemed safe without risking the possibility of unintentional damage to the bridge. The results of these tests indicate that a pan fire could be detected within 5–8 seconds when the flame source was located within a few feet of a sensor.

Infrared Camera

The infrared camera was subjected to fire tests during both daytime and nighttime hours. These tests were performed with the standard pan fire positioned at several locations on the south approach span of the bridge (Fig. 27). In all cases, the fire was detected within less than 10 seconds in all tests and in less than 5 seconds in over 75% of the tests.

In addition to the fire tests, a series of intruder tests was performed that consisted of a person moving about on the bridge site during the hours of darkness.

A series of photos (Fig. 28) presents the infrared images captured during both fire and intruder tests. The image of a person is clearly visible in a), which indicates that the IR camera is fully capable of this type of detection.

Flame Detector

A series of pan fire tests were performed to determine the area of the bridge which could be reliably monitored by the flame detector. A rectangular grid, measuring 4 ft by 4 ft,

Figure 28. Infrared photos—onsite system evaluation of a) person only, b) person and initial fire, c) person and fire after 2 min.

was used to locate the pan fire prior to each test. These tests were performed during both daylight and dark hours.

In fact, the detection of a fire was not limited by the distance from the flame source to the sensor. Instead, the primary impediment to reliable detection using the flame detector was line-of-sight interference from bridge roof framing members. In all cases where interference was not present, the flame detector was able to detect a fire within 5–7 seconds.

Conclusions and Recommendations

The instrumentation and monitoring of the Madison County Cedar Bridge presented in this report has provided an excellent first step in the development of security and fire protection monitoring of important historic resources.

A total of three sensing systems were installed and tested both in the laboratory as well as at the actual bridge site. These systems included the following:

- Infrared camera mounted on utility pole to monitor the bridge and approach roadways
- Industrial flame detector mounted near the bridge portal to monitor the bridge interior
- Fiber optic sensors mounted near the timber bridge deck to monitor ambient temperature changes

The three sensor systems were connected via a wired and wireless network to a computer running custom-designed software which collects data from each of the sensors, determines whether a fire or intruder event has taken place, and notifies interested parties.

The three systems were evaluated on the basis of cost and effectiveness. Based on the ease of installation, reliability, and relatively low cost of the industrial flame detector used on this project, these units appear to offer the greatest potential benefit to bridge owners at detecting fires in similar installations. The primary impediment to the reliable use of similar flame detector units is line-of-sight interference from bridge framing members. Future installations should carefully consider the placement of these sensors or provide a number of sensors with differing viewpoints to eliminate these interferences. The infrared camera proved to perform well at detecting the presence of persons at the bridge site. This sensing system, when properly placed, can provide an early warning to authorities of persons at a location where they should not be.

The research work performed during this project generated a considerable amount of media attention in the local, regional, and national press. This increased visibility may in some small way have improved the public recognition of the critical need to protect vital historical resources.

Future developments that could be made to improve security monitoring of covered bridges:

- Application of solar power systems which can provide sufficient power for monitoring without overly affecting the aesthetic appearance of historic bridge sites

- Development and installation of a wide area monitoring network, which would permit an owner-agency to continuously monitor all of the covered bridges under their jurisdiction.

References

Cho, A. 2005. Cameras and sensors will patrol New York rail, bridges. Engineering News-Record. September 5; 16.

Crossett, J.; Rhodes, B. 2005. Protecting America's roads, bridges, and tunnels: the role of state DOTs in homeland security. Report RP–PAR–1. Washington, DC: American Association of State Highway and Transportation Officials.

Factory Mutual. 1994. Flame radiation detectors for automatic fire alarm signaling. FM 3260. Norwood, MA: Factory Mutual.

Roberts, J.E.; Kulicki, J.M.; Beranek, D.A.; Englot, J.M.; Fisher, J.W.; Hungerbeeler, H.; Isenberg, J.; Seible, F.; Stinson, K.; Tang, M.C.; Witt, K. 2003. Recommendations for bridge and tunnel security. Washington, DC: American Association of State Highway and Transportation Officials, Transportation Security Task Force.

Stevens, M.A. 2005. Security essentials. Buildings. 99(8): 42–46.

Williamson, E.B.; Winget, D.G. 2005. Risk management and design of critical bridges for terrorist attacks. Journal of Bridge Engineering. 10(1): 96–106.

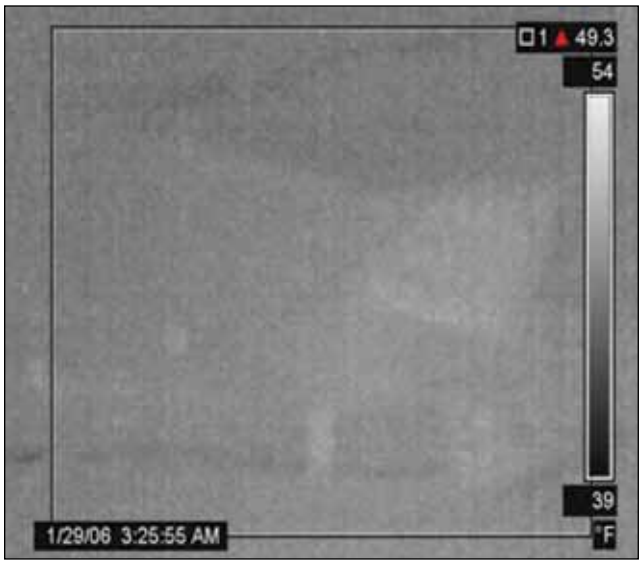
Wolff, T.O. 2003. Proposed TMC response protocol to suspicious activity at highway bridges. Advanced surface transportation systems class. College Station, TX: Texas A&M University: 56–75.

Appendix A—Events Recorded by Onsite Monitoring System

Nine events were recorded by the system in place at Cedar Bridge (Table A-1, Figs. A-1–A9).

Table A–1. Summary of recorded events

Event number	Date	Time	Type	True/ False
1	01/29/2006	2:29:46 a.m.	Intruder	True
2	03/03/2006	10:07:33 p.m.	Intruder	True
3	03/07/2006	10:40:13 p.m.	Intruder	True
4	03/11/2006	9:04:21 p.m.	Intruder	True
5	04/19/2006	2:57:57 p.m.	Fire	False
6	04/27/2006	9:10:14 a.m.	Fire	False
7	05/04/2006	10:27:45 a.m.	Fire	False
8	05/24/2006	7:41:38 a.m.	Fire	False
9	06/16/2006	4:10:32 a.m.	Intruder	False

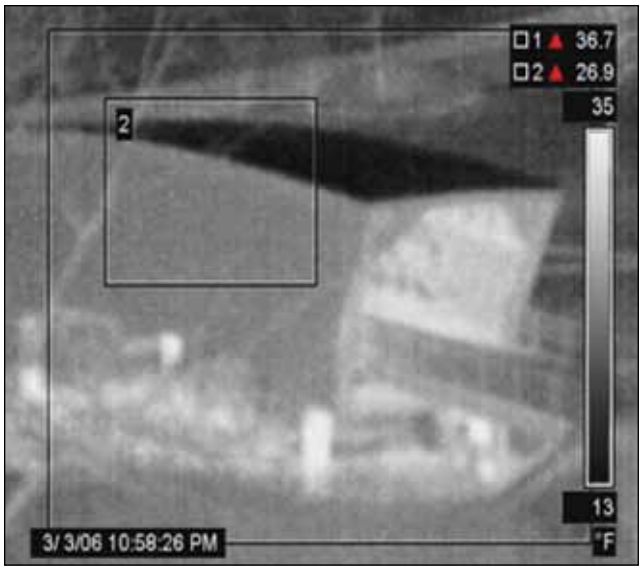


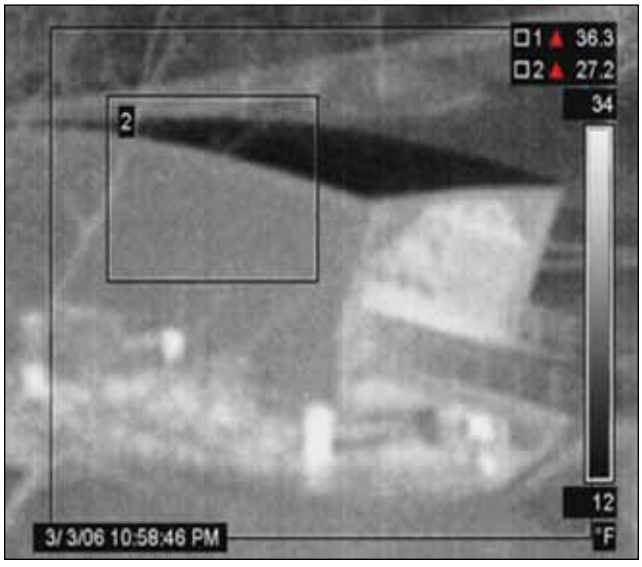
Date: Sun, 29 Jan 2006 02:29:49 -0600
From: bird@iastate.edu
Subject: Person Detected at Cedar Bridge
To: bird@iastate.edu,
jmsmvs@iastate.edu,
mlaviol@iastate.edu,
bphares@iastate.edu

System: FLIR A20M IR Camera
Date/Time: 1/29/2006 2:29:46 AM

A PERSON has been detected at the Cedar Bridge.

Figure A–1. Event 1—Person detected at Cedar Bridge (1/29/06, 2:29 a.m.) a. Image 1, b. Image 2, c. Image 3, d. Image 4, e. Image 5, f. E-mail notification.





Date: Fri, 3 Mar 2006 22:07:45 -0600
From: bird@iastate.edu
Subject: Person Detected at Cedar Bridge
To: bird@iastate.edu,
jmsmvs@iastate.edu,
mlaviol@iastate.edu,
bphares@iastate.edu

System: FLIR A20M IR Camera
Date/Time: 3/3/2006 10:07:33 PM

A PERSON has been detected at the Cedar Bridge.

Figure A–2. Event 2—Person detected at Cedar Bridge (3/3/06, 10:07 p.m.) a. Image 1, b. Image 2, c. Image 3, d. Image 4, e. Image 5, f. E-mail notification.

Date: Tue, 7 Mar 2006 22:40:17 -0600
From: bird@iastate.edu
Subject: Person Detected at Cedar Bridge
To: bird@iastate.edu,
jmsmvs@iastate.edu,
mlaviol@iastate.edu,
bphares@iastate.edu

System: FLIR A20M IR Camera
Date/Time: 3/7/2006 10:40:13 PM

A PERSON has been detected at the Cedar Bridge.

Figure A–3. Event 3—Person detected at Cedar Bridge (3/7/06, 10:40 p.m.) a. Image 1, b. Image 2, c. Image 3, d. Image 4, e. Image 5, f. E-mail notification.

Date: Sat, 11 Mar 2006 21:04:31 -0600
From: bird@iastate.edu
Subject: Person Detected at Cedar Bridge
To: bird@iastate.edu,
jmsmvs@iastate.edu,
mlaviol@iastate.edu,
bphares@iastate.edu

System: FLIR A20M IR Camera
Date/Time: 3/11/2006 9:04:21 PM

A PERSON has been detected at the Cedar Bridge.

Figure A–4. Event 4 – Person detected at Cedar Bridge (3/11/06, 9:04 p.m.) a. Image 1, b. Image 2, c. Image 3, d. E-mail notification.

Date: Wed, 19 Apr 2006 15:06:56 -0500
From: bird@iastate.edu
Subject: Fire Detected at Cedar Bridge
To: bird@iastate.edu,
jmsmvs@iastate.edu,
mlaviol@iastate.edu,
bphares@iastate.edu

System: FLIR A20M IR Camera
Date/Time: 4/19/2006 3:06:47 PM

A FIRE has been detected at the Cedar Bridge.

Figure A–5. Event 5—Fire detected at Cedar Bridge (4/19/06, 2:57 p.m.) a. Image 1, b. Image 2, c. Image 3, d. Image 4, e. Image 5, f. E-mail notification.

Date: Thu, 27 Apr 2006 09:10:33 -0500
From: bird@iastate.edu
Subject: Fire Detected at Cedar Bridge
To: bird@iastate.edu,
jmsmvs@iastate.edu,
mlaviol@iastate.edu,
bphares@iastate.edu

System: FLIR A20M IR Camera
Date/Time: 4/27/2006 9:10:14 AM

A FIRE has been detected at the Cedar Bridge.

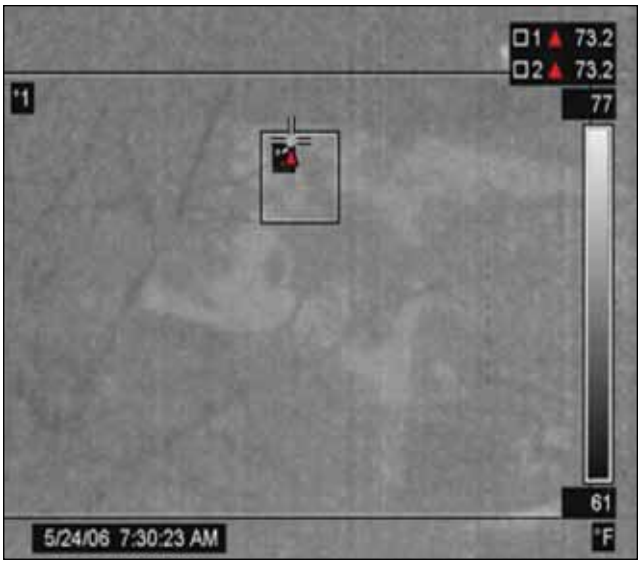
Figure A–6. Event 6—Fire detected at Cedar Bridge (4/27/06, 9:10 a.m.) a. Image 1, b. Image 2, c. Image 3, d. Image 4, e. Image 5, f. E-mail notification.

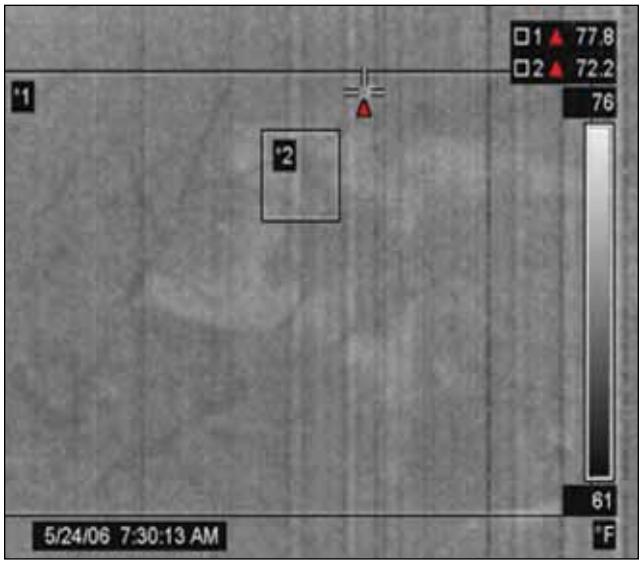
Date: Thu, 4 May 2006 10:27:53 -0500
From: bird@iastate.edu
Subject: Fire Detected at Cedar Bridge
To: bird@iastate.edu,
jmsmvs@iastate.edu,
mlaviol@iastate.edu,
bphares@iastate.edu

System: FLIR A20M IR Camera
Date/Time: 5/4/2006 10:27:45 AM

A FIRE has been detected at the Cedar Bridge.

Figure A–7. Event 7—Fire detected at Cedar Bridge (5/4/06, 10:27 a.m.) a. Image 1, b. Image 2, c. Image 3, d. Image 4, e. Image 5, f. E-mail notification.



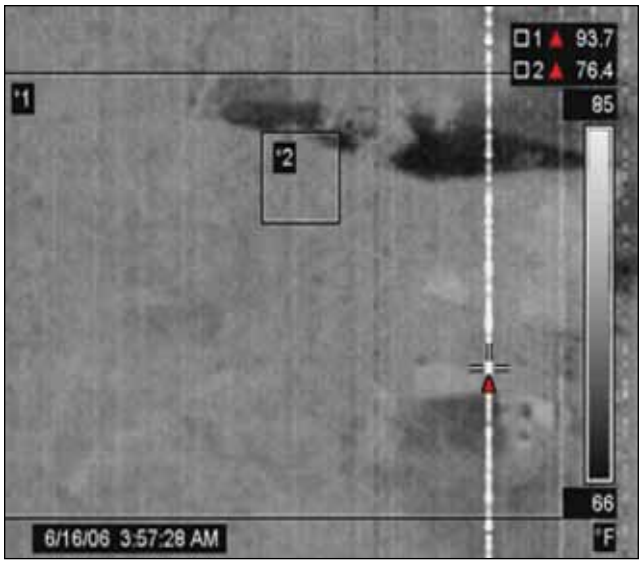


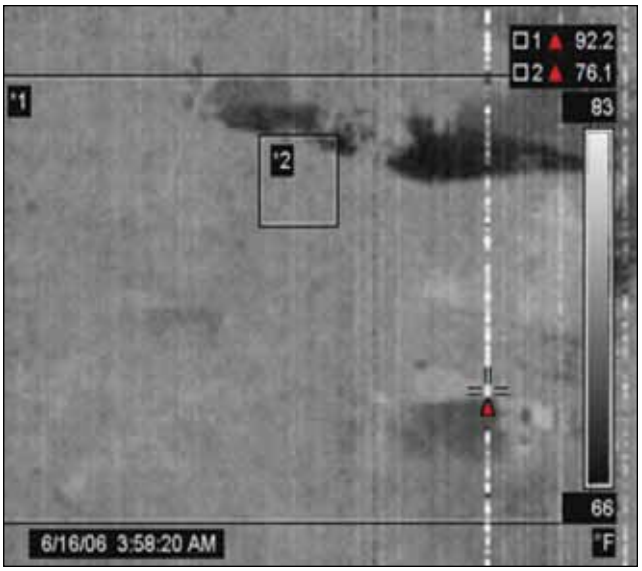
Date: Wed, 24 May 2006 07:41:40 -0500
From: bird@iastate.edu
Subject: Fire Detected at Cedar Bridge
To: bird@iastate.edu,
jmsmvs@iastate.edu,
mlaviol@iastate.edu,
bphares@iastate.edu

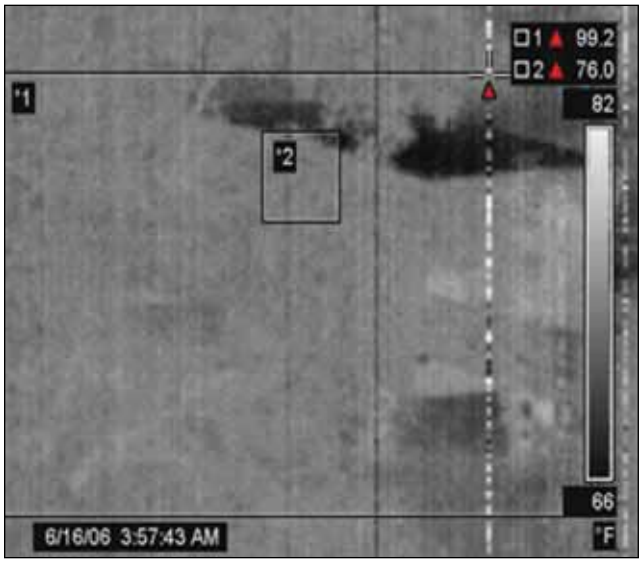
System: FLIR A20M IR Camera
Date/Time: 5/24/2006 7:41:38 AM

A FIRE has been detected at the Cedar Bridge.

Figure A–8. Event 8—Fire detected at Cedar Bridge (5/24/06, 7:41 a.m.) a. Image 1, b. Image 2, c. Image 3, d. Image 4, e. Image 5, f. E-mail notification.







Date: Fri, 16 Jun 2006 04:10:35 -0500
From: bird@iastate.edu
Subject: Person Detected at Cedar Bridge
To: bird@iastate.edu,
jmsmvs@iastate.edu,
mlaviol@iastate.edu,
bphares@iastate.edu

System: FLIR A20M IR Camera
Date/Time: 6/16/2006 4:10:32 AM

A PERSON has been detected at the Cedar Bridge.

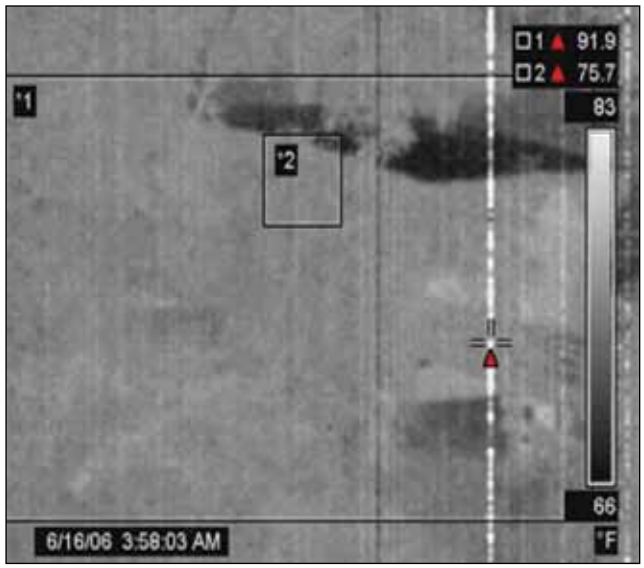


Figure A–9. Event 9—Person detected at Cedar Bridge (6/16/06, 4:10 a.m.) a. Image 1, b. Image 2, c. Image 3, d. Image 4, e. E-mail notification.