Development of a milk transport security system

C. Thompson[1], F.A. Payne[2], B. Luck[2], J.R. Moore[3] & N. Tabayehnejad[2]

[1]Regulatory Services, University of Kentucky, Lexington, KY, USA
[2]Department of Biosystems and Agricultural Engineering, University of Kentucky, Lexington, KY, USA
[3]Applied Physics Institute, Western Kentucky University, Bowling Green, KY, USA

Summary

The United States Department of Homeland Security (DHS) has targeted bulk food contamination as a focus for attention because it poses a high consequence health threat to our society. The current manual methods used for monitoring milk during transport are cumbersome, paper intensive and prone to errors. The bulk milk transportation sector necessitates a security enhancement that will reduce recording errors and enable normal transport activities to occur while providing security against unauthorized access. A robust security system coupled with improved recordkeeping would provide the opportunity for security breaches to be investigated more quickly and more thoroughly. The goal of this research was to develop a milk transport security system to meet these demands, demonstrate it and transfer the technology to the public.

A milk transport security system was designed and consists of a security monitoring system (SMS) located on the milk transport tank, a handheld device (computer), and a remote data server. The SMS controls access to the milk during transport, automatically collects security data and transmits it to the handheld device. The handheld device is used by the milk hauler/sampler to collect the milk data. Both the milk data and security data are transmitted by the handheld device using cell phone communication to a data server where access is provided to data users.

The SMS was mounted on a milk transport tank and used to pick up milk during four days of operation with delivery to a dairy processor. The results to date indicate that the SMS was effective for securing the milk transport tank and recording the security data and the handheld device was effective for collecting the milk data and transmitting both the milk data and security data to a data server.

***Key words**: Recording, Monitoring, Physically store, System design, Security Monitoring System,*

Introduction

The Bioterrorism Act of 2002 (Food and Drug Administration 2002) addresses threat assessments, technologies and procedures for securing food processing and manufacturing facilities and modes of transportation. The development of security systems to prevent potential adulteration of foods, while still enabling routine food production and transportation activities to occur, is stated as essential. Key elements of the Bioterrorism Act focus on protection against adulteration of food and maintenance and inspection of records for foods.

In the US, food safety and defense of Grade A milk is under the purview of the Food and Drug Administration (FDA). Manufacturing grade (Grade B) dairy production is regulated by the United States Department of Agriculture (USDA). FDA has identified milk as a heightened food security concern and a priority in terms of national security (Food and Drug Administration 2004). Bulk milk's large batch size, high degree of accessibility, thorough mixing during processing, rapid turnaround at retail and rapid consumption after purchase by consumers are consistent features of a high-risk food. Together, the FDA and USDA comprehensively monitor dairy food safety.

The bulk milk transportation industry lacks a uniform, formal security policy. Loaded and unloaded trucks and/or tankers are regularly left unattended and may be parked overnight in unsecure and unsupervised areas. Many of these unattended, unsecure locations are secluded and may include dairy farms, remote transfer points, hauling company property and hauler residences.

Bulk milk transporters currently use voluntary seal programs to secure milk during transport. The seal programs generally utilize plastic, numbered seals on tanker openings. Not all seals are tamper evident. Seal number identifiers are recorded as they are applied to openings. As seals are broken during routine transportation activities, seal numbers are accumulated. Some companies require that broken seals be maintained. These sealing systems are problematic in that they are prone to record keeping errors and maintaining broken seals are burdensome (it is not uncommon to have numerous broken seals for a single load of milk).

Additionally, current bulk milk records are primarily handwritten. The level of detail associated with records maintained on bulk milk manifests, bills of lading, etc. for each load of milk is inconsistent and prone to inaccuracies (Department of Transportation, 2004). The maintenance of records is critical to provide for adequate trace-back of food and agricultural products when potential adulteration occurs. Most farms have a handwritten record in the milk house known as a "barn card". Furthermore, haulers typically maintain bulk milk manifests or load tickets. Pertinent information relating to each dairy farm is maintained within these records. Similar to the seal information, these records are error prone and legibility is often a concern. Recording mistakes, mathematical errors and misplaced tickets are commonplace (Department of Transportation, 2004).

The objective of this project was to develop a milk transport security system (MTSS) that will provide assurance that the milk, milk samples, milk data and security data are securely transported between the dairy farm and dairy processor, demonstrate the security system at two milk plants and multiple dairy farms, and deliver the technology to the national community through collaborations, technical conferences, publications and standards.

Materials and methods

System design

An analysis of the system was conducted and a set of critical functional design requirements were established for the milk transport security system which were to:

1. Provide "secure transport" of milk.
2. Operate within the current milk transport infrastructure.
3. Physically store the milk and security data with the milk transport tank.
4. Provide redundant storage of milk and security data to meet the operational and security needs of the dairy industry.

The design of the milk transport security system incorporated all of the critical design requirements to assure the secure transport of bulk milk, milk samples, milk data and security data between locations and specifically between dairy farms, transfer stations, receiving stations and dairy processors. It includes three processor subsystems: a security monitoring system (SMS) installed on the milk transport tank, a handheld device, and a data server. Figure 1 shows the components of the SMS and their location on a typical milk transport tank. Figure 2 graphically illustrates the three processor subsystems used to collect the milk and security data and transmit it to the data server. These three subsystems were designed to work together to meet the functional design requirements for the milk transport security system.

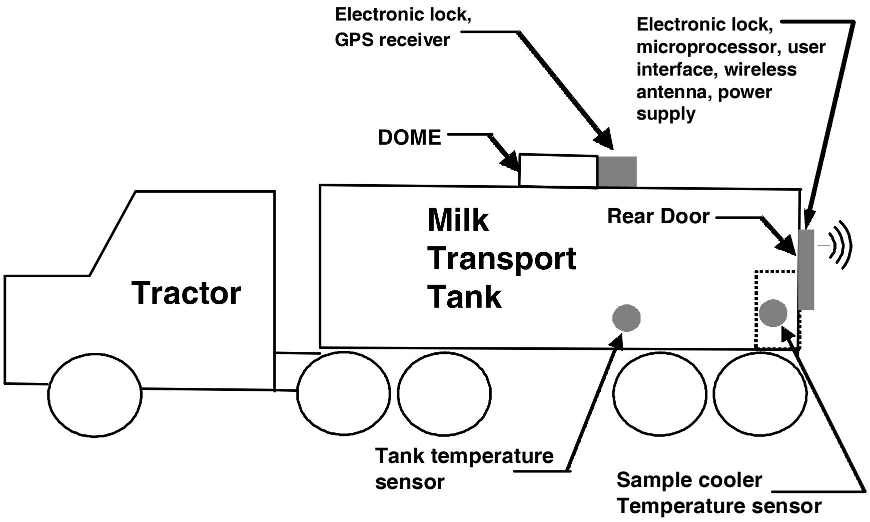

Figure 1. The Security Monitoring System (SMS).

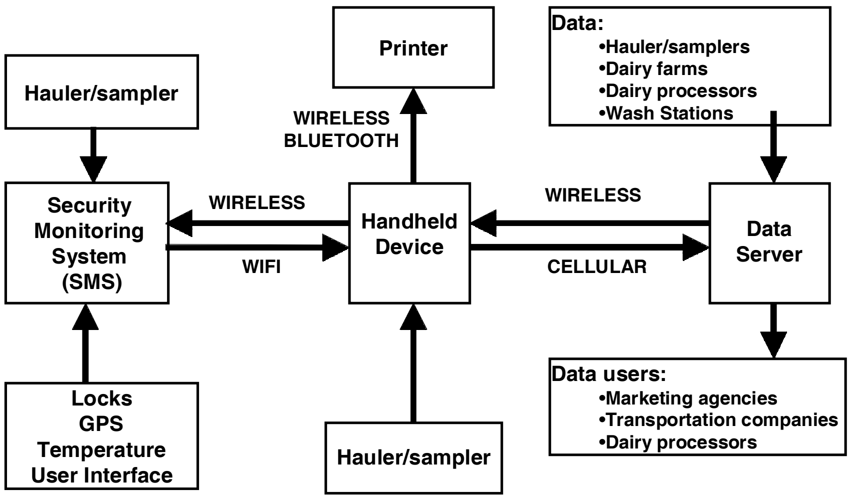

Figure 2. Milk transport security system design and communication diagram.

Provide "secure transport" of milk

Security of the milk transport tank is assured by

1. Identification of authorized personnel who may access the vessel to load, unload, sample milk, wash/sanitize or adjust/inspect equipment.
2. Locking access ports and monitoring their status.
3. Recording the reason for access.
4. Monitoring the geographic location of the milk transport tank and e) recording all data for traceability.

The system was designed to meet the following functional requirements:

1. Only authorized persons are given pass codes to the handheld device.
2. The combination of physical locks and electronic monitoring of the locks provide a constant assurance of the security of the milk transport tank even when not observed by a qualified employee. Securing the vessel means locking it so that access cannot be obtained without "breaking the lock". Locking the milk transport tank provides the level of security sought for transport of milk and is similar to security levels implemented in milk processing plants.
3. The data is collected throughout a security session which typically encompasses the time from initiation of washing/sanitizing the milk transport tank to the end of unloading of the milk at the plant and the security data is stored.
4. A "reason code" is used for tank access.
5. A GPS (Global Positioning System) unit is installed on the milk transport tank.
6. The milk and security data are stored on a server for future traceability.

Operate within the current milk transport infrastructure

The system must operate within the existing bulk milk transport infrastructure, operate with electronically instrumented and non-instrumented dairy farms, operate for dairy farms that direct-load a milk transport tank, operate for multiple dairy record keeping systems, provide versatility to allow the bulk milk hauler/sampler to perform routine activities if any part of the milk transport security system malfunctions, maintain security in the event of a system failure (power loss, mechanical, electrical, software malfunction) and accommodate the potential future requirement that herd data be collected.

The system was designed to meet the following functional requirements:

1. Bar codes are used to identify the farms thus no farm power is required for non-instrumented dairy farms.
2. A digital entry key pad is included in the design for unloading events when a handheld device is not available or if it malfunctions.
3. Wireless WiFi communication was included as part of the system for collection of herd data from farm based PC.
4. A database structure was developed to accommodate flexibility for the entire system.

Physically store the milk and security data with the milk transport tank

Loaded tankers are regularly connected to and moved by multiple tractors. This practice emphasizes the importance of a system that provides tanker-based data collection/storage. For example: a hauler/sampler may perform the farm pickups using one handheld device. The hauler/sampler may drop the full tanker trailer of milk at a location. Another driver may connect to the tanker with another tractor to pull the milk across country. Additionally, this driver may or may not have a handheld device. The tanker of milk may be pulled by multiple drivers across country. Maintaining the physical association of milk and the data is a basic premise for a successful system.

Meeting this function requires that the data collection be tank-based and contain sufficient auxiliary power for up to 100 hours. Milk tankers are required to be washed and sanitized prior to each use. The sanitization cycle is valid from the time of sanitization for up to 96 hours until the first milk is loaded onto the tanker. Additionally, tankers are regularly separated from tractors (the power source) and stored without use for varied amounts of time. For these reasons, the tanker based portion of the system must maintain sufficient auxiliary power for up to 100 hours. If a tanker is stored dormant for an extended period, this auxiliary power will allow continual monitoring of the tanker security. The 100 hour time period will be sufficient because tankers remaining dormant past this period will need to be connected to a tractor (a power source) and moved to a facility for a new wash and sanitization cycle (due to the 96 hour requirement). This movement will subsequently result in a new "security session".

The system was designed to meet the following functional requirements:

1. The Security Monitoring System (SMS) will contain auxiliary power sufficient to power the system for 100 hours. The design of the power system has not been specified.
2. The SMS collects security data and stores it in a data file on the SMS.
3. The handheld device combines the security and milk data and stores this in a data file on the SMS.

Provide redundant storage of milk and security data to meet the operational and security needs of the dairy industry

The loss of data will result in the loss of a load of milk, disrupting the marketing of farm milk and detrimentally impacting dairy producers. The dairy industry will not implement any data system which has potential to loose the data collected.

Data redundancy is critical because multiple hauler/samplers may be involved in farm pickup processes and because multiple drivers may be involved in the transport of a tanker. Additionally, data redundancy provides backup in the event of a handheld device failure during the milk pickup or transport process or if the handheld device does not accompany the load from one driver to the next.

The system was designed to meet the following functional requirements:

1. SMS data is stored in a "log" and "security data" file on the SMS and maintained for 60 days.
2. Security data is transmitted to the handheld device and stored for up to 60 days.
3. Milk data is stored on the handheld device.
4. Milk data and security data are combined into a "Security Session" data file and stored on the SMS for up to 60 days, on the handheld device for up to 60 days, and on the server for an undetermined period of time.

Results and discussio

System design

The SMS electronics included electronic locks for the hatch and back door, a temperature sensor on the milk transport tank wall and another in the milk sample cooler, a GPS receiver, Wi-Fi antenna, digital user interface keypad, Liquid Crystal Display (LCD) screen, and a data storage unit. Figure 3 shows the rear access of the milk transportation tank along with the keypad, Wi-Fi antenna, LCD screen and electronic lock. Figure 4 shows the top dome access to the milk transport tank and the GPS receiver, dome electronic lock and also specifies other critical components of the modified dome assembly. Three on-board electronics nodes were linked with a Controller Area Network (CAN bus). The CAN bus has the ruggedness and bandwidth to work well in this application. The SMS processor monitors and stores the status of the locks, GPS, and temperature sensors on one minute intervals or upon an event i.e. when a lock is opened or when other events as defined occur. The temperature sensors monitor the milk in the transport tank and the sample cooler. The tank temperature has the potential to record the tank temperature during the wash cycle thus verifying a proper wash.

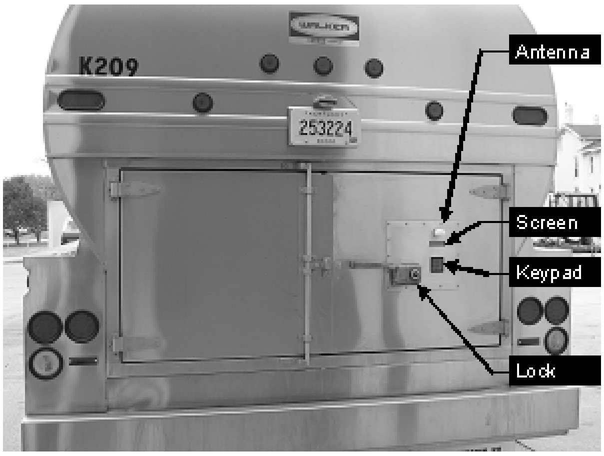

Figure 3. Rear access port of the Security Monitoring System (SMS).

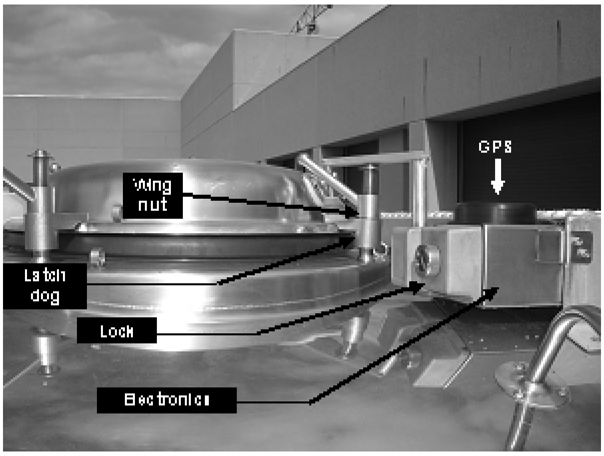

Figure 4. Top dome of the Security Monitoring System (SMS).

The handheld device (CN3, Intermec, Everette, WA) utilized three modes of communication (Bluetooth, Wi-Fi, and Cellular) and possessed an alphanumeric keypad, barcode reader and touch screen. The device is constructed in a rugged, water-proof case and is suitable for this application. Bluetooth was used to communicate with the label printer, which was always within close proximity. WiFi (802.11 standard) had a range of 100 m and was used to communicate to the SMS.

The data server contained the information attributes of the dairy farms, milk transportation companies and their transportation tanks and tractors, receiving stations at dairy processors and wash stations. This information was stored as tables with associations as required. A database structure for storage and retrieval was developed as part of this system. The system was developed to permit only authorized personnel to access any of the access ports. If any of the access ports are accessed, the SMS will record the reason for access, monitor the geographic location using GPS, and record all security data.

System tests

A prototype was first demonstrated on a commercial milk truck in September 2007. System testing began in October 2007 with the pickup of milk on a regular route for delivery to a processor. The objective of the system tests was to confirm the function of the SMS, handheld unit and data server as well as the associated hardware and programming. The focus of the initial tests were to unlock the locks using wireless communication, collect the milk data using barcodes for farm identification, print milk sample labels and print a milk ticket from data transmitted to the data server.

The results were positive with the milk being successfully picked up on all days. The wireless technology proved to functionally work throughout testing. The handheld device initially communicated milk data to the server. The milk data was uploaded to the server after each farm pick-up through cellular communication and the system secured milk during transport. There were a multitude of interrelating issues regarding the data structure, sequence of events, data storage on the SMS and general programming that have required a continuous effort to improve robustness. The focus on robustness continued through February when a robustness test showed that the complete system functioned flawlessly on six consecutive simulated pickups.

System testing resumed during February 2008 with the goal of demonstrating the system robustness, printing milk tickets at the dairy processor from data in the data server, and quantifying the amount of data being transmitted over the cell phones. Quantification of the hardware design for a commercial phase will also be an objective of the testing in 2008.

The system validation and a gradual development and verification of software enhancements and web based software input and output programs are expected to continue through 2008 including the development of traceability programs. Continued prototype field testing will include collecting milk on multiple routes with deliveries to multiple processors.

Conclusions

1. A system analysis of milk transport security requirements was conducted.
2. A set of critical functional requirements were developed.
3. A prototype system was designed and developed to implement the critical design requirements.

4. The system tested in the fall of 2007 and demonstrated the functional performance of the system.
5. Development work will continue during 2008 to further develop and implement enhancements including web base data input and output programming.

Acknowledgments

This research was supported by a grant "A Wireless Electronic Monitoring System for Securing Milk between the Dairy and Milk Plant" from the Department of Homeland Security through the National Institute for Hometown Security. Close collaboration with Alan Wilson Trucking, Bluegrass Tank and Equipment, Dairy Farmers of America-Mideast Council, Kentucky Milk Safety Branch, Slayback Milk Transport, Southern Belle Dairy, Starr Stainless, and Winchester Farms Dairy has ensured that anomalies associated with any one particular segment was addressed.

List of references

Department of Transportation. 2004. "Security of Milk Transport in the United States Project", U. S. Department of Transportation Report Number DOT-VNTSC-TSWG-04-01, May 2004.

Food and Drug Administration. 2004. "Security Surveillance Assignment for Periods of Increased Risk, Executive Summary". Internal report dated 9/08/04 v2.

Food and Drug Administration. 2002. "The Bioterrorism Act of 2002". <*www.fda.gov/oc/bioterrorism/Bioact.html*>.