A SYSTEMATIC FRAMEWORK FOR RADIO FREQUENCY IDENTIFICATION (RFID) HAZARD MITIGATION IN THE BLOOD TRANSFUSION SUPPLY CHAIN FROM DONATION TO DISTRIBUTION

By

Natalie Rahming

A Dissertation Submitted in

Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy

in Biomedical and Health Informatics

at

The University of Wisconsin-Milwaukee

December 2012

ABSTRACT
A SYSTEMATIC FRAMEWORK FOR RADIO FREQUENCY IDENTIFICATION (RFID) HAZARD MITIGATION IN THE BLOOD TRANSFUSION SUPPLY CHAIN FROM DONATION TO DISTRIBUTION

by

Natalie Rahming

The University of Wisconsin-Milwaukee, 2012
Under the Supervision of Professor Timothy Patrick, Ph.D.

The RFID Consortium is developing what will be the first FDA-approved use of radio frequency identification (RFID) technology to identify, track, manage, and monitor blood throughout the entire blood transfusion supply chain. The iTrace™ is an innovative technological system designed to optimize the procedures currently employed when tracing blood from the donor to the recipient. With all novel technologies it is essential to consider not only the advantages, but also the potential harms that may come about from using the system. The deployment of the iTrace™ consists of two phases: 1) Phase One – application of the iTrace™ from the donor to blood center distribution, and 2) Phase Two – application of the iTrace™ from blood center distribution to transfusion. This dissertation seeks to identify the possible hazards that may occur when utilizing the iTrace™ during Phase One, and to assess the mitigation and correction processes to combat these hazards. A thorough examination of verification and validation tests, as

well as of the system design, requirements, and standard operating procedures was performed to qualify and quantify each hazard into specific categories of severity and likelihood. A traceability matrix was also established to link each hazard with its associated tests and/or features. Furthermore, a series of analyses were conducted to determine whether the benefits of implementing the iTrace^{TM} outweighed the risks and whether the mitigation and correction strategies of the hazards were effective. Ultimately, this dissertation serves as a usable, generalizable framework for the management of RFID-related hazards in the blood transfusion supply chain from donor to blood center distribution.

DEDICATION

I dedicate my dissertation work to my mother, my family, and my friends whose support has been extraordinary, unwavering, and invaluable.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

I would first like to thank my committee members who graciously and generously shared their time and expertise. Special thanks to my major advisor Dr. Timothy Patrick, as well as Dr. Mark Mone, Dr. Amy Coenen, and Dr. Rashmi Prasad for serving on my committee and providing critical feedback. I would like to extend a great deal of gratitude to Dr. Mary Shimoyama for her tremendous amount of guidance, encouragement, and advice, and to Mary Anne Wawrzyn for her support, recommendations, and assistance from the time of my onboarding onto this project all the way through to its completion.

I would like to thank the BloodCenter of Wisconsin and the RFID Blood Transfusion Consortium for welcoming me to the team, for trusting me to conduct imperative analyses, and for their willingness to provide enthusiastic and continuous support. Special thanks to Rodeina Davis for her direction, leadership, and backing throughout the entire project. A large amount of thanks also to Petra Yurchich and Jerry Holcombe for reliably affording me all of the help, materials, and documents I needed to conduct my analyses. A great deal of thanks to Clive Hohberger and Alfonso Gutierrez for reviewing my work and offering highly valuable suggestions and revisions. I would also like to thank the UW RFID Lab and Steve Ostrowski for enabling me to play a role in important system testing.

Finally, I would like to acknowledge and thank all of my teachers and mentors within and outside of UW-Milwaukee for allowing me to pursue this degree and conduct my research,

and for providing assistance and support when needed. I am truly grateful for this enjoyable experience.

CHAPTER 1: INTRODUCTION

The elimination of tragic, yet avoidable, medical errors is not an impractical illusion but, rather, a purposeful objective to pursue. Working towards this goal will improve healthcare delivery, reduce healthcare costs, and most importantly, expunge the human cost of such preventable tragedies. Medical errors occur frequently and, while many impose little potential for harm, those that do result in injury can lead to severe consequences (1). It has been estimated that as many as 44,000 to 98,000 Americans die from medical errors each year (1-6). As such, this vast magnitude of errors in medicine underlines the need for improved safeguards during healthcare delivery. Despite the common practice of identifying and penalizing the persons committing the errors, it has become increasingly evident that it is more effective to focus on the healthcare systems themselves (1, 7). The systems can utilize technology to both mitigate and correct errors. A systems analysis of medication errors found that the top eight of the 16 major types of system failures discovered could have been averted with better medical information systems (1, 7). Hence, using technology to enhance the access, availability, and dissemination of healthcare information, and thereby restructuring current methods, is worthwhile. In order to embark on the path towards an idealized medical system absent

of avoidable missteps, a deliberate approach involving the addition of innovative technologies and the optimization of current processes is valuable.

One area of healthcare where the elimination of medical errors is vital is the blood transfusion medicine supply chain. According to a 2005 US Department of Health and Human Services Report (8), in 2004 approximately 1,322 national medical treatment centers reported a total of 32,128 transfusion-related adverse events. These include various issues involving sample documentation, labeling, storage, and lab handling throughout the entire supply chain process (9). Ultimately, these seemingly trivial errors can lead to the most critical transfusion hazard: mis-transfusion (2, 10-16).

Mis-transfusion occurs when the wrong blood is given to the wrong person. All humans possess a type within the ABO blood group (Table 1). The four key types are A, B, AB, and O. There are two antigens (i.e. A, B) and two antibodies (i.e. Anti-A, Anti-B). An individual's blood type is determined by whether or not an individual's red blood cells carry the A antigen (i.e. Blood Type A), the B antigen (i.e. Blood Type B), both the A and B antigens (i.e. Blood Type AB), or neither antigen (i.e. Blood Type O). Healthy individuals produce red blood cell antibodies against A or B antigens that are not expressed on their own cells. For example, an individual carrying the A antigen, who therefore has Type A blood, will make anti-B antibodies. These anti-B antibodies will

attack and destroy the red blood cells carrying the corresponding antigen. Thus, if a Type A individual receives Type B or Type AB blood, red cell hemolysis or agglutination may take place (Table 2). At best, mis-transfusion necessitates therapeutic and diagnostic interventions and, at worst, it may result in death. In order to evaluate the best means of eliminating medical errors such as mis-transfusion from the blood transfusion supply chain, it is necessary to describe this process end-to-end.

Table 1: ABO Blood Types

ABO Blood Type	Antigen A	Antigen B	Antibody Anti-A	Antibody Anti-B
A	Yes	No	No	Yes
B	No	Yes	Yes	No
AB	Yes	Yes	No	No
O	No	No	Yes	Yes

Table 2: Blood Compatibility

Patient Type	Compatible Red Cell Blood Types
A	A, O
B	B, O
AB	AB, A, B, O
O	O

The blood transfusion supply chain begins with the collection of blood from the donor. At this time, essential data elements such as blood type, donor identification number, and other patient information details are gathered and stored. The next step in the chain

involves physically packing blood products into their appropriate containers. Containers have associated temperature properties and capacity constraints which dictates the type and quantity of items that can be included. After that, the containers are loaded onto transport trucks and released for pick-up. The containers then go through the check-in stage, where station operators inspect the containers for missing or excess items. The products are labeled with information taken at the time of collection and moved to inventory. Finally the product and its associated information are verified and distributed. At any point during this process, there exists the potential for misplacement of items, inaccurate transfer of data, or imprecise monitoring of products and information. As such, it is clear that improving the identification, tracking, monitoring, labeling, and storing of blood products during the entire supply chain process would reduce the incidence of mis-transfusion.

Many blood centers and hospitals have examined the utilization of radio frequency identification (RFID) as a means of enhancing the tracking, monitoring, labeling, and storing in the blood transfusion supply chain, and have found it to be very promising (17-27). RFID is the interaction and exchange of electromagnetic radio waves between tags and readers, enabling automatic identification and data capture (AIDC) and real-time information of marked objects (28-30). RFID is a technology that is composed of transponder tags, readers, and a hardware system to which information is written. Also,

RFID systems operate at a range of frequencies. The antennas of RFID readers exchange electromagnetic radiation waves with the tags. The readers then send information to servers via wireless networks or docking stations. Readers may be handheld or located in gates and tunnels where they can read multiple items simultaneously, as opposed to the current system of using barcodes which require line-of-sight individual readings.

Given the capacities for speedy information transmission and batch reading of multiple items, RFID is capable of supporting the need for rapid and effortless access to process data generated in the blood supply chain including collection, manufacturing, testing, labeling, inventory, and distribution (30). Furthermore, RFID is a reputable technology in logistics for identifying and tracking items, aiding in the monitoring and optimizing of logistical processes (17, 31, 32). For example, RFID technology is common in the automotive industry and is gaining widespread acceptance in supply chain processes such as retail applications (17). Additionally, the benefits of RFID have already been demonstrated in medical asset management. By tracking medical devices using RFID, both the amount of time spent searching for a device and the cost of replacing lost items can be significantly reduced (32, 33). Moreover, several other logistical areas have examined RFID as a potential solution including: access control and time registration; protection of expensive equipment; localization of equipment, staff, and patients in

healthcare facilities; organization of logistic processes for beds, containers, and apparel; safe identification of products and patients; and, protection against imitation drugs .

In response to the potential of RFID for automatic identification and data capture (AIDC) and monitoring of blood and blood products across the whole transfusion medicine supply chain, a consortium of blood centers (BloodCenter of Wisconsin, Milwaukee, WI, Carter Blood Care, Dallas, TX, and Mississippi Blood Services, Jackson, MS), hospitals (Baptist Health Systems, Jackson, MS, and University of Iowa Hospital and Clinics, Iowa City, IA), the University of Wisconsin-Madison RFID lab, and several technology partners (SysLogic, Inc., TAGSYS, Zebra Technologies, Psion TekLogix, Mediware Information Systems) are developing and evaluating the first comprehensive RFID system to document and track blood from donor to recipient (19). This system is designed to identify, manage, track, and monitor the condition of blood products from the beginning to the end of the blood supply chain. RFID technology is capable of both preventing medical accidents in the health industry as well as initiating an effective, rapid, and corrective response in the case of an emergency (34). For instance, in cases where it is possible for incorrect administration of medication to occur, RFID has been shown to enable accurate medical data transmission by offering a control for the identification and facilitating the administration of the correct quantity and type of drugs (34).

The system being deployed by the consortium will be the first FDA-approved use of RFID technology throughout all phases of the blood supply chain. This system, iTrace™, utilizes passive RFID technology that is superior to simple barcode-based AIDC methodologies in several ways (19, 35-38). Unlike barcode-based AIDC technologies, RFID technology does not require line-of-sight. This means that the tag and reader are not required to be within visual range of one another in order for data transmission to occur. Also, while barcodes must be read one at a time, RFID allows for batch – or concurrent – reading of multiple items simultaneously without disrupting the processing of the data or its accuracy. In addition, RFID possesses a broader field of readability, is more durable and capable of enduring harsh environments, and is able to store more editable information on its chips than barcodes. This is important as it demonstrates the ability of RFID to more efficiently track and monitor products and information by working at longer ranges, withstanding damage, and holding more relevant information on its chips. Additionally, whereas barcodes are generally used once and discarded, RFID technology enables the data to be completely erased and the tag to be reused if necessary. Moreover, RFID tags may be integrated with sensors to assist with time and temperature tracking, reducing waste and diminishing patient danger due to spoiled products.

RFID technology is generally applied when there is a need to read tagged items outside of the short visual range of a bar code (39). In addition, processes like the transfusion

medicine supply chain may involve environmental conditions such as temperature, dirt, or contamination that make optically scanning barcodes ineffective (40). Also, RFID technology allows for better tracking and reconciliation of products. Additionally, it augments the precision of product locations by utilizing its tag memory qualities of data encoding and storage, as well as its broader field of readability and batch reading capabilities (30). Furthermore, RFID may boost the accuracy of tracking time and temperature, reducing product waste and increasing the quality and availability of blood products due to its integration of temperature sensors to assist with time and temperature tracking (30). Hence, RFID is the preferred solution for the blood transfusion medicine supply chain. While the employment of barcodes alone has been somewhat effective at reducing medical errors, the systems are not fully efficient as individual scanning of each item and searching for relevant data does little to reduce staff workloads (41-46).

The iTrace™ system incorporates RFID technology as a complement to the traditional procedures. It will initially serve as a supplement to, not a replacement of, the barcode so that it will work with current processes, not against them (37). The integration of barcodes and RFID tags has the potential to improve complex systems and support, and align all components to produce optimal outcomes (6). This is significant as it will reduce tragic errors such as mis-transfusion, eliminate the human cost of these errors, and enable better delivery of healthcare.

Bar codes will still be utilized as a backup in case of unforeseen RFID troubles or system failures during the implementation and testing period. Barcodes will be applied as a secondary identification source for ensuring that the products are properly labeled. The iTrace^{TM} was created for a more intelligent blood supply chain where every element works together cohesively (47).

The impact of integrating these technologies into a useful system triggers an evaluation of the value proposition. In other words, in order for the tool to be implemented, it must be apparent that the return on investment is sufficient (1), and that the deviation from inexpensive barcode-alone processes would be worth the venture of implementing this new system. The consortium conducted an impact analysis to quantitatively model and estimate the effects of RFID on the business metrics of the blood center (38). The analysis consisted of two primary components: organizational impact and cost/benefit analysis. In terms of the business metrics, it was concluded that the key gains would be in productivity and quality due to automated processes, reduction of discarded products, and enhanced inventory management. For the cost/benefit model, the chief outputs measured were total expected costs, total expected benefits, expected payback period, and net present value. The consortium projected that there would be a $83,560 (11.2%) return on investment (ROI) over 5 years resulting in an approximate 4 year payback period. For larger organizations, the recovery may be less than three years (approximately 30

months), but for smaller institutions the payback period may be as much as 6.9 years (2). Ultimately, the researchers of the consortium estimated that, by improving quality control and identification procedures through RFID, the blood banking industry would save more than $9 million per year and result in 40,000-45,000 fewer units of discarded blood products (9). Thus, it may be justifiable operationally and economically, particularly for larger organizations, to employ RFID technology in the blood supply chain.

Moreover, since iTrace™ software introduces a new technology to the Transfusion Medicine field, a pre-market approval from the Food and Drug Administration (FDA) is essential before employment of the new software is permitted. All technological devices in their infant stages trigger an array of questions concerning the effects of their use. Although the benefits of using the tool may appear tangible, the uncertainty of the actual advantages or consequences of using the technology remains until confirmation is attained through research and testing. Thus, it is very important to identify and understand not only the gains, but also the hazards of employing new technologies.

The potential hazards of using new technologies can be seen in the story of the Therac-25 (48). This notoriously defective system would malfunction up to 40 times per day as a result of its software. In a 20-month period, the software defects led to massive radiation overdoses for six cancer patients, leading to the deaths of three. In dealing with medical

devices and, hence, the lives of others, the existence of potential harms may outweigh the likely advantages.

Several types of hazards – technological, implementation, functional – may occur. Technological hazards are potential sources of harm originating from technology or system conditions, or from the interaction of human activity with these conditions. Implementation hazards are potential harms related to technology usage in an everyday setting. Functional hazards are the potential harms which may disrupt the ability of the system to perform its intended duties appropriately and accurately. Full awareness of the hazards, as well as system specifications and strategies for mitigation and correction are essential. Since the iTrace™ is the first tool to account for complete blood supply chain management from the donor to the recipient, the risks of utilizing RFID in blood supply operations has not previously been assessed.

There are two phases for the implementation of the iTrace™. "Phase One" encompasses all of the activities at the blood center starting with blood donation, manufacturing, testing, inventory management, shipping, and distribution of blood products to the hospital. "Phase Two" comprises all activities of transfusion services at the hospital starting with receiving blood products and ending with cross-matching and transfusing patients. The consortium has completed development and a pilot for both phases and is

currently finalizing all documentation and deliverables necessary to submit for Medical Device Class II clearance from the FDA for iTrace™ Phase One. The submission will be done in accordance with Section 510(k) of the Food, Drug and Cosmetic Act, which requires device manufacturers to register and notify the FDA of their intent to market a medical device. This is known as Premarket Notification - also called PMN or 510(k).

In this instance, the RFID Blood Transfusion Consortium becomes a medical device manufacturer that is required to submit a premarket notification because of the intent to introduce a device into commercial distribution for the first time or reintroduce a device that will be significantly changed or modified to the extent that its safety or effectiveness could be affected. In the case of the iTrace™, the substantial change is the addition of RFID to the current blood supply chain processes. Building a comprehensive analysis of its technological, implementation, and functional hazards is a key component of receiving approval before releasing to the commercial market. Since the project is still in its early phases and the types of hazards that would be encountered vary extensively between the two Phases, the analysis presented here will focus solely on Phase One.

A major function of any new project or development is a thorough risk analysis. It includes rigorous, fact-based methodologies with predefined criteria for assessing the risks associated with all elements of the offering. It also consists of structured reviews of

each potential hazard to assess the status, severity, problems, issues, and dependencies. Additionally, mitigation strategies are developed to define the preventive actions required to minimize the risk, and correction strategies are designed to address the hazard in the instance of occurrence. SysLogic's Quality System Manual and FDA guidance documents provided preliminary direction for these analyses.

Although the Consortium used these applicable standards and pre-identified hazards for the implementation and functional portions of the project, assistance was needed on the technology portion. Using RFID in this environment is an entirely new practice, and help from someone with biomedical and health informatics training was essential in uncovering the issues that could potentially occur. In response to this need, I was tasked with discovering what these technological hazards could be. The consortium also wanted help in producing a thorough analysis – including the categorizing, qualitative and quantitative ranking, and mitigation/correction strategy evaluation – of all of the hazards that could take place throughout Phase One. As this assessment was a requirement for FDA 510K approval and critical for the system evaluation overall, I was responsible for completing this initiative as well. My role was a key component in revealing potential harms, assessing the system's value, and answering questions regarding the system's usability.

Therefore, the purpose of this project was to conduct a hazard analysis of this new medical device to deduce answers to the following inquiries: 1) how the benefits of the tool outweigh the existence of the potential hazards, 2) how sufficient are the applied mitigation and correction strategies, and 3) how may the methods employed to qualify and quantify the hazards into specific categories be transferred to other new medical devices.

There were several objectives to this study. The first was to identify all of the possible hazards that may occur when using the iTrace™ from donation at the blood center to blood product distribution at the hospital, and rate the severity of each. The consortium had already begun to identify hazards based on the SysLogic Quality Document and FDA guidance documents which detailed what hazards are commonly encountered with medical devices, as well as which steps to take during the verification and validation milestones of product development. I managed the identification and assessment of the technological hazards associated with RFID use in the blood supply chain. Next, an analysis of the severity and likelihood for all hazard types was performed. The strategies taken to eliminate, mitigate, prevent, or respond to those hazards were then documented. Third, the effectiveness and success of these methodologies were assessed. Fourth, an evaluation of whether the application benefits of the iTrace™ were worth the risks was completed. Lastly, the ultimate goal of the project – to construct a comprehensive hazard

analysis and traceability matrix, establishing the foundation of a systematic framework for managing RFID-related hazards in the blood transfusion medicine supply chain from donation to distribution for generalized use with other technologies – was completed.

RESEARCH QUESTIONS

RQ 1: How do the benefits of using the iTrace™ outweigh the potential RFID-related hazards?

RQ 2: How sufficient are the mitigation and correction strategies for managing RFID-related hazards in the blood transfusion medicine supply chain from the donation to blood center distribution?

RQ3: How can the methods utilized in this paper effectively qualify and quantify the associated hazards into standard categories which may be transferable to other newly deployed RFID-based healthcare technologies?

CHAPTER 2: BACKGROUND

This chapter will provide insight into the primary design features of the iTrace™. It will also give details on the particular "pain points" or situations in which there is the highest demand for RFID use, as well as on the "touch points" or areas within the blood transfusion supply chain where RFID-enabled processes are the most advantageous. In addition, the types of hazards that may be encountered during Phase One will be described. Lastly, background information on the RFID consortium itself will be supplied.

iTRACE™ DESIGN

The iTrace™ design consists of specific RFID technologies, various RFID touch points, and a particular architecture formulated for best use practices from donation to blood center distribution.

RFID Technology

Radio Frequency Identification (RFID) is a technology which identifies items by using electromagnetic radio waves (wireless air interface) to interact and exchange data between transponder tags and readers (30) (Figure 1). It is generally composed of transponder tags, readers, and a hardware system to which information is written, and it

operates at a range of frequencies. Tags may be active, passive, or semi-active/passive. Active tags are battery-powered and able to emit signals without activation by a reader. Passive tags “awaken” when in the field of the reader. The power from the reader prompts them to communicate. Semi-active/passive tags use a thin battery, which can be used to increase the read range of the tag, to power the chip. The iTrace™ solution uses the passive tag, which is the most widely accepted for healthcare supply chain solutions (40, 41, 49).

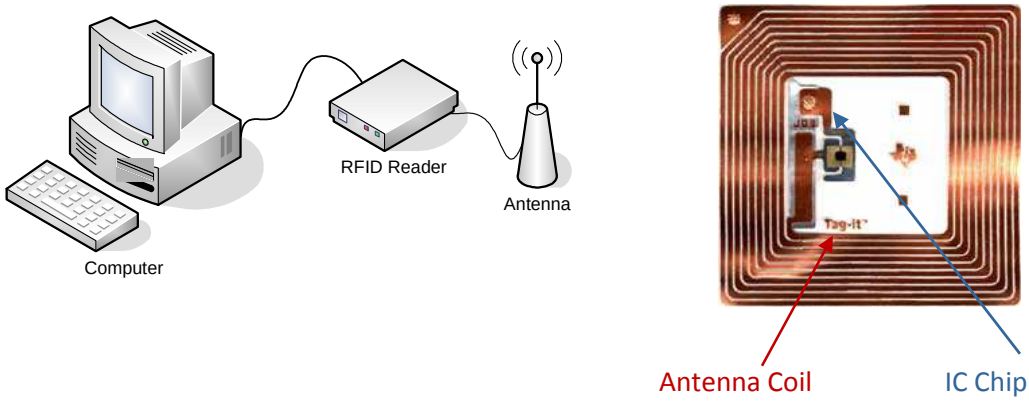

Figure 1: RFID Technology Structure

The readers of RFID systems have antennas that exchange electromagnetic radiation waves with the tags. The information that is read by the reader is sent to servers via wireless networks or docking stations. Readers may be handheld or located in gates and tunnels where they can read multiple items within a single container at once.

There are three different kinds of frequencies on which RFID can work that determine the range at which the tags can be read. The first is low frequency. Low frequency (LF) bands typically work at frequencies of 125-134 KHz. High Frequency (HF) bands operate at 13.56 MHz. This is the global ISO-standardized frequency, and is widely accepted for use in the healthcare industry. Ultra High Frequency (UHF) works at 850-900 MHz. These are the most expensive tags, possessing the best ranges and transferring data the fastest. However, UHF licenses vary in allowance due to health and safety issues. UHF is capable of exciting water molecules in blood products to the extent that they would likely raise the temperature of the blood beyond acceptable levels. The iTrace™ employs the international standard 13.56MHz, which is the recommended standard for blood transfusion medicine (30, 38, 40, 50).

Furthermore, RFID tags are capable of storing information and carrying all major data about the product. The minimum suggested memory capacity of 2 Kbits enables the use of International Society of Blood Transfusions (ISBT) 128 data structure and messaging (30). The data on the tag may be locked to protect sensitive information, or it may be unlocked to allow for reuse of tags. Data carrier-independent ISBT 128 compliant figures which use 7-bit ISO 646 (ASCII) characters are used for the tag memory (35). Tag user memory is distributed in 4-byte physical memory blocks which are individually addressable and locatable (35).

iTrace™ Architecture

The iTrace™ is made up of a set of devices installed and used at the central blood center, remote fixed donation sites, and remote mobile donation sites as described in the iTrace™ Technical Specifications documents.

The components of the central blood center facility include a server on which the software and application are installed, a network of fixed and handheld RFID/barcode readers and antennae that are connected to a server via the blood center's local area network (LAN), one or more servers on which the blood center's Blood Establishment Computer System (BECS) is installed, one or more client workstations used to access the iTrace™, and a network connection through which a server connects to and interoperates with devices at remote donation sites.

Remote fixed and mobile donation sites both contain hardware components such as a server software installed on a PC connected to the internet and a Wi-Fi LAN at the donation site, one or more handheld RFID/barcode readers that are connected to the donation site Wi-Fi LAN and interact with the server, and printers and supplies used to print shipping manifests, blood donation record forms, and labels. Additionally, for fixed remote sites, an electronic interface between the electronic blood donation record and the server software which reduces manual entry for each collection may be employed. Similarly, a USB thumb drive may also be used to store donation record information.

For all site types, there is a set of design features and underlying assumptions on which all of the applications that comprise the iTrace™ depend. These include the physical items tracked, the use of RFID tag identification numbers (TINs) and user memory, containers, locations, notes and tracks, and hardware devices supported at each touch point. Moreover, the physical location and movement of the following items are all tracked with the iTrace™: blood donation records (BDRs), test tube sets, blood bags, and containers. Each item is distinguished and identified by the RFID system using a combination of RFID tags and bar code labels using ISBT128 format. While blood bags and containers have RFID tags attached, test tube sets and BDRs are identified by bar codes. Collection bags use 14 x 31mmRFID tags placed under the standard ISBT 128 DIN label (35). The items are tracked both individually and as a set. All of the applications that comprise the iTrace™ are designed to work with either bar code only or RFID-enabled blood bags and containers, allowing the RFID application to have a back-up in case the tag becomes unreadable.

Every item within a collection, as well as the set itself, shares the same donation identification number (DIN). However, each item is further identified by its type (BDR, test tube, or blood bag), content type name (RBC-1, RBC-2), and globally unique tag identification number (TIN). The TIN is fixed at the time of manufacturing, can never be changed, and is guaranteed to be unique even across different tag manufacturers.

Each RFID tag has a small amount of random access user memory that can be used to store information about the item to which it is attached. The tags record the following information: Product Code, ABO/Rh, Donation Identification Number, and Product Expiration Date. The Procedure Code is also collected to assist in the manufacturing process. The user memory can be read and written multiple times. Areas of the tag may be hidden to inhibit modification. Furthermore, the tags are capable of responding to a one-time "kill" signal, which triggers the self-destruction of the tag such that neither the TIN nor the user data memory can ever be read or written again.

There are four readers that are used in the iTrace™: Tagsys L400, PA600, Tracient Paddle, and traditional barcode scanners. They can be directed to read tag TINs or read and write tag user memory. During the writing of information to the tag's user memory, the software first directs the reader to write the desired data to the tag's user memory and then read the data back from the tag. The software confirms that the data was successfully written to the tag. Data written to the blood bag tag is never read or used by the system software. Only the TIN is read at each of the RFID-enabled touch points to associate, retrieve, and process blood bag information from the database. Figure 2 depicts the RFID reader display.

Figure 2: iTrace™ Reader Display

PAIN POINTS

The dynamic nature of the blood transfusion supply chain results in considerable difficulties in information acquisition, processing, and management (51). As the volume of information increases, so does the potential for human error. Consequently, blood

centers are turning to information technology resources to improve the productivity and efficiency of blood banking processes (17-27).

Blood banks are looking to RFID technologies for identification, authentication, tracking, traceability, management, labeling, inventory, security, sensing, and regulatory purposes (32, 52). The auto identification and data capture capabilities of RFID enable the elimination of mistakes and the optimization of processes. RFID technology in healthcare has also been shown to be cost effective for healthcare operations (53). The combination of these benefits helps facilitate the construction of transparency and trust for the healthcare system through the use of a total quality systems approach.

The goal of the iTrace™ is to enhance the delivery of transfusion medicine by supporting the operational process at critical points. Process owners from blood banks participating in the consortium identified "pain points" in the current transfusion supply chain processes. "Pain points" denote areas throughout the supply chain where inefficiencies or errors often occur (38). Each pain point was ordered according to the frequency of the incidence and the magnitude of the consequence.

In Phase 1 – from donation to blood center distribution – there were four primary pain points (35, 38) (Figure 3). The first involved reconciling data with physical reality. This means it was necessary to ensure that the data record detailing the expected amount and

type of products matched the amount and type of products that were actually delivered. With the current barcode process, each blood product must be tracked and accounted for individually. The RFID-enabled iTrace™ solution was designed to construct unit/container relationships, allowing for better tracking and faster container reconciliation of products.

The second pain point dealt with physically locating products. Like the first pain point, this was reflective of single product tracking constraints. The solution was to use RFID to capture details and log data/update a database with the most recent location of all products encountered during searches to enable better traceability.

Similarly, the third pain point was the difficulty in scanning multiple items. Unlike the barcode-based processes currently in place, the RFID processes enabled by the iTrace™ will support the preferred capacity to read multiple units simultaneously and without the necessity of line-of-sight reading. This will facilitate rapid donation check-in and shipment verification at the blood center. The iTrace™ is capable of reading all of the units in a closed container at the same time, considerably increasing efficiency.

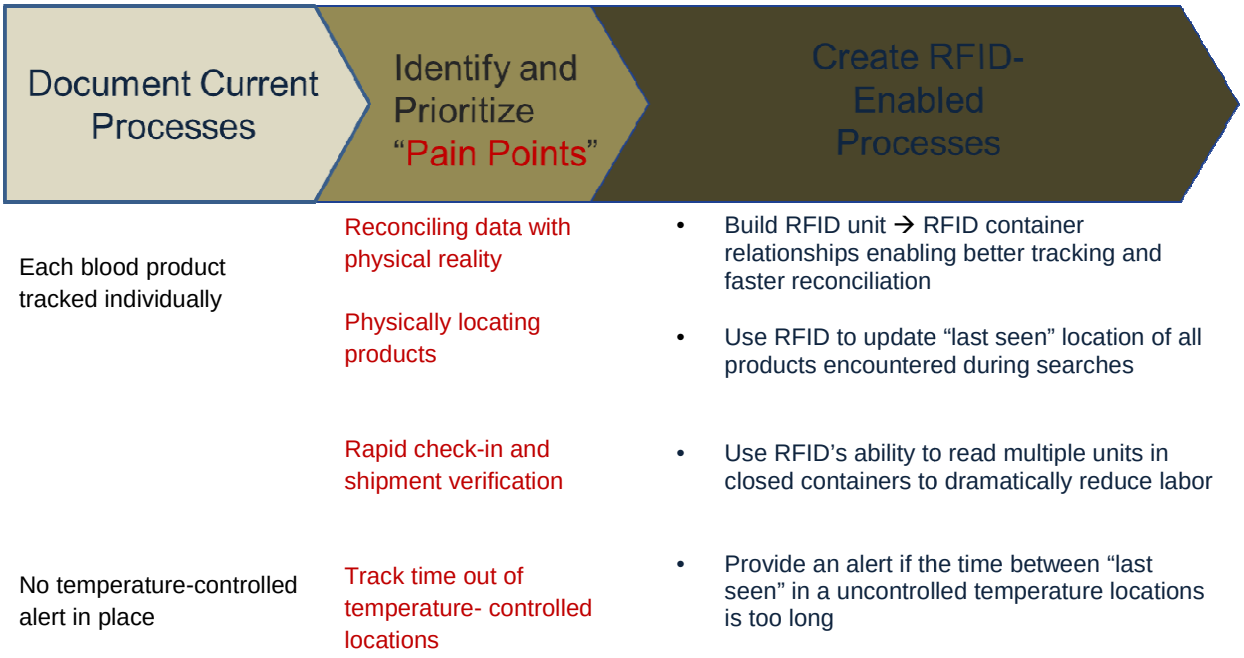

Figure 3: Pain Points

The final pain point identified during Phase One was difficulty in tracking time and temperature. Existing barcode-only procedures do not utilize temperature-controlled alerts. The iTrace™ solution remedied this pain point by providing alerts if and when the time between scans/reads in uncontrolled or incorrect temperature locations exceeded expectations. As such, it appears evident that RFID is capable of solving many of the challenges facing traditional blood banking operations. The analysis of the current processes and pain points served as the groundwork for designing the iTrace™, and enabling its application across various process touch points.

iTRACE™ TOUCH POINTS

The touch points are the areas of the blood supply chain in which the iTrace™ complements the current processes (Figure 4). According to the Functional Specifications Document of the consortium, they include the following actions throughout the supply chain: collection, pack container, load and release pickup, check-in container, label product, check-in inventory, verify container, check-in returns, check-in imports, and inventory management functions.

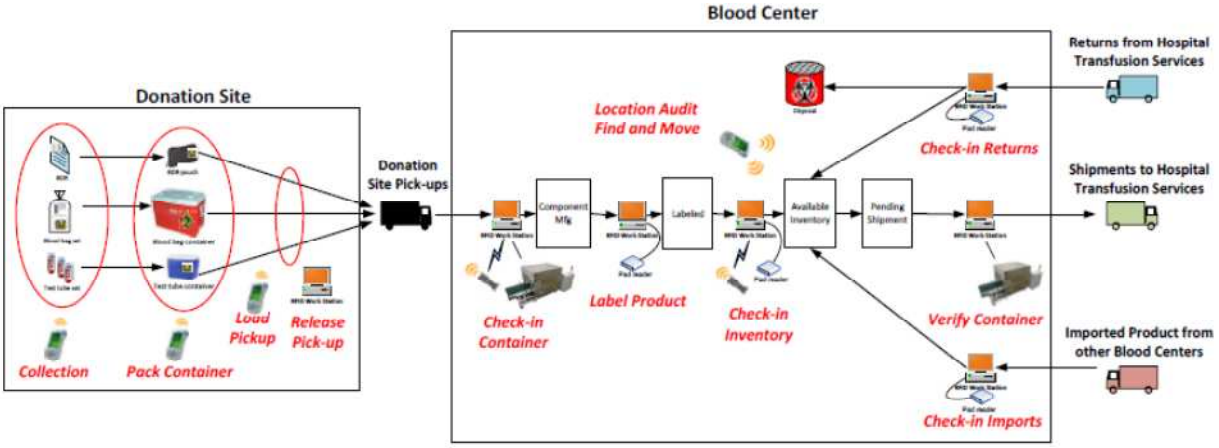

Figure 4: iTrace™ Touch Points

Collection

During donation collection, RFID technology is used to uniquely identify and track physical components that make up the collection such as BDRs, test tube sets, and blood

bags. It is also used to gather key data elements for collection. The selected information about the collection is encoded and stored in the RFID tag memory associated with the blood bags included in the collection.

Pack Container

When packing the container, RFID associates items with their containers by their DIN as they are physically packed into the containers. This facilitates fine-grained tracking of each item's location, as well as the formulation of pick-up documentation to be used in reconciliation activities. Each container has an associated type, capacity, and temperature property, which is used to determine the maximum quantity and kinds of items that can be packed in the container. The container types and capacity constraints are verified as each item is packed.

Load and Release Pickup

RFID technology enables the association of containers with a pick-up as they are loaded onto transport trucks, allowing the detailed tracking of the container's location. The technology also permits automatic creation of pick-up documentation for use in reconciliation. This establishes a chain of custody transfer from the donation site to the

pick-up transport service as well as visibility for products in transit from remote donation sites to blood centers to assist in advanced production planning.

Check-In Container

During the check-in stage, the RFID technology reconciles the content of each container individually and as a whole, giving the check-in station operator the ability to view and classify containers, as well as found, missing, and excess items within each container. Items are “batch read,” meaning they are read simultaneously. The information that is read is sent electronically to the Blood Establishment Computer System (BECS) to check-in the items.

Label Product

Product labeling information from the BECS for the blood bag being returned to the blood center is received. Additionally, the RFID encodes, updates, and verifies the information (DIN, product code, expiration date, ABO/Rh, etc.) on the bag’s RFID tag memory.

Check-in Inventory

The RFID provides chain of custody details when newly-labeled products move from the labeling area into inventory, updating both the back-end BECS as appropriate as well as the product's inventory storage location information that is maintained in the RFID system.

Verify Container

RFID, again, allows for batch reading of an outbound shipping container's contents and performs a final verification of a packed shipping container's content before the container leaves the blood center.

Check-in Returns

When the blood bag is returned to the blood center, product labeling information from the BECS is received. Simultaneously, encoding, updating, and verifying of the information on the bag's tag memory occurs. Any patient information that is located on the tag is removed.

Check-in Imports

During check-in imports, product labeling information from the BECS is received, and the information on the bag's RFID memory is encoded, updated, and verified. The product's inventory storage location is also updated.

Inventory Management Functions

The RFID technology helps the user find blood bag products in inventory and move them to new locations in single batch operations. Additionally, it helps the user update the inventory of items currently stored in a specified location as a single batch operation. The BECS is updated appropriately.

The impact of RFID appears to be substantial. Yet, until the risks of utilizing the technology are examined, the full impact of its application cannot be measured. The hazards of using RFID technology in the first half of the blood transfusion supply chain must be assessed and the appropriate responses disclosed so that a functional, valuable framework may be established.

POTENTIAL iTRACE™ HAZARDS

The three primary types of hazards that are encountered are during Phase 1 of the BSC are technological, implementation, and functional. My role was to serve as the project

lead for the technology hazard group, identifying, testing, and analyzing technological hazards that may occur with the introduction of RFID technology into the blood supply chain processes. The implementation and functional hazards listed were derived from the SysLogic Quality Plan document which details hazards commonly met with the adoption of new medical devices. The Project Manager and various members of the consortium identified them as potential hazards that may impact the use of the iTrace™ tool.

Technology Hazards

Technological hazards involve the read/write efficiency of the RFID system and the effects of the high frequency (HF) radio frequency magnetic waves on other medical devices and the blood products themselves. They also include tag and system capabilities and survivability under harsh conditions. There are safety and critical functionality requirements that must be fulfilled in order for the successful mitigation of the hazards associated with the iTrace™. The safety and critical design requirements for the potential technology hazards of the iTrace™ include the following:

- Preventing Read/Write Errors or Failure.
- Ensuring No Adverse Effects of RFID Technology on Blood Products.
- Ensuring Performance Capability of RFID Tags During the Most Common Blood Supply Chain Processes.

- Ensuring RFID Tag Survivability After Experiencing the Most Demanding Conditions in the Blood Supply Chain.
- Ensuring No Interference of RFID High Frequency (HF) and Electromagnetic Interference (EMI) with Other Systems.

The specific hazards that were pinpointed and assessed will be discussed in Chapter 4.

Implementation Hazards

SysLogic, Inc. maintains a list of recognized or foreseeable hazards associated with medical devices under both normal and abnormal conditions. Previously identified hazards are also taken into account. Possible implementation hazards encompass a broad range of issues related to the realization or execution of the device specifications. They include matters involving the database, interface, data processing, data corruption or loss, and audit trail items. The safety and critical design requirements for the implementation of the iTraceTM consist of the following:

- Preventing Sequencing or Timing Errors
- Preventing Data Loss / Corruption
- Preventing External Interface Errors

Functional Hazards

The functional hazards identified and tested are also components of SysLogic, Inc.'s known and foreseeable list of risks associated with medical devices. Functional hazards

consist of any potential risks to the performance of the system/device in a daily operational setting. They are comprised of concerns related to the ability of the system to record read/written information appropriately and accurately. They also include other software design and capability issues such as security, access, traceability, notification alerts, monitoring, tracking, and labeling. The safety and critical design requirements associated with the functionality of the iTrace™ include:

- Preventing Unauthorized Entry or Override of System Data
- Preventing Loss of Traceability
- Preventing Packing in Improper Containers at Collection Sites
- Ensuring Reconciliation of Materials from Collection Site
- Ensuring Blood Product Labeling Information is Properly Captured from BECS
- Preventing Unsuitable Products from Being Released to Distribution

CONSORTIUM ROLES AND RESPONSIBILITIES

Due to the existence of several valuable players in the RFID Blood Center Consortium, it is important to identify the roles and responsibilities of each. This will enable a better understanding of the project's organization. The consortium consists of personnel from the multiple aforementioned organizations working under the guidance of the Program Director, Rodeina Davis. Members of the consortium make up various components of the organizational structure including the Steering Committee, Project Management Team, Product Manager, Project Manager, Project Coordinator, Grant Administration Team,

Activity Team Leads, Activity Teams, and Grant Administration Team members (Figure 5).

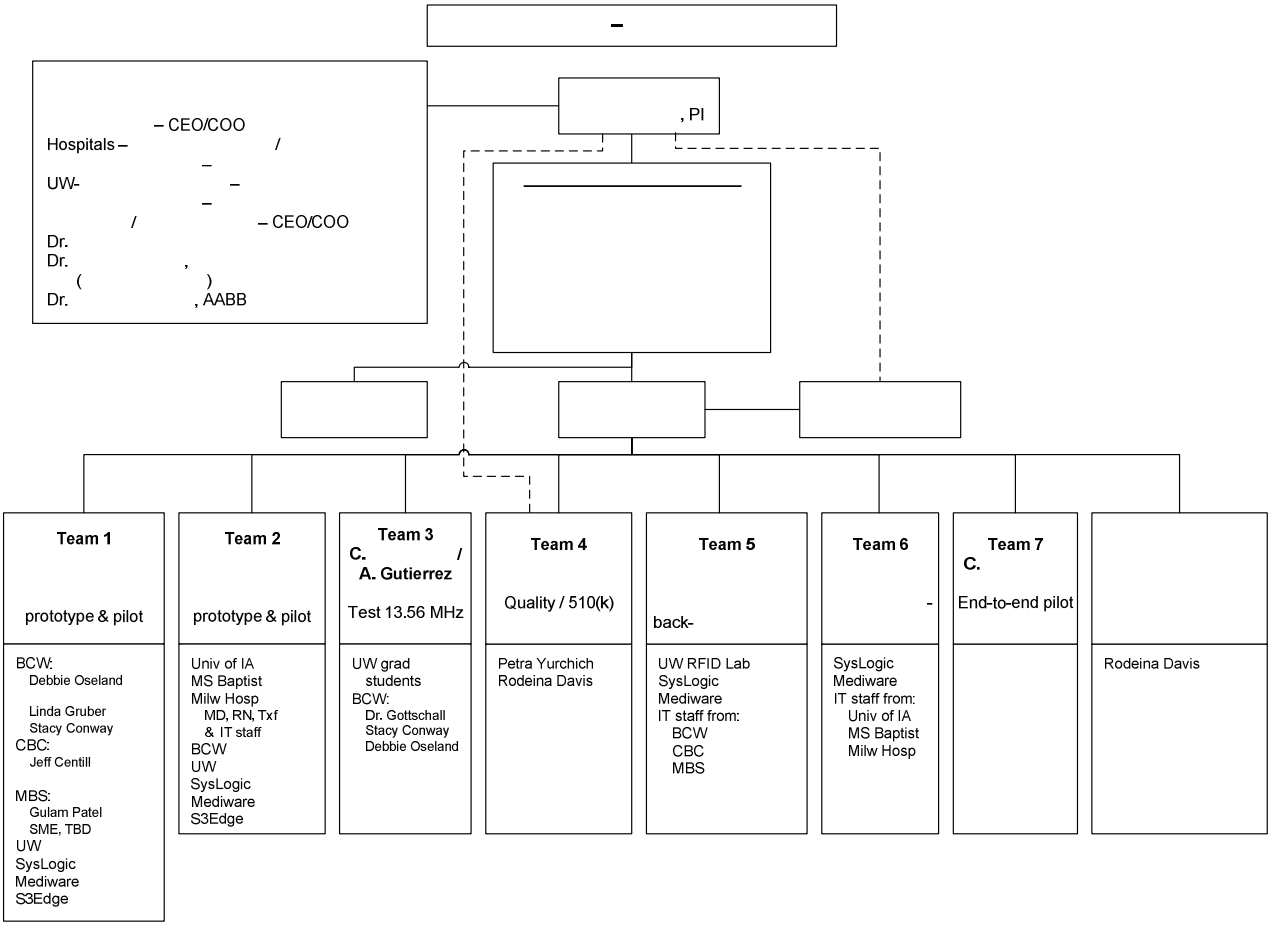

Figure 5: RFID Consortium Organizational Chart

My role in the consortium fell under Team 4 for Quality/ 510(k). I served as the project lead for technology hazard analysis. I identified, documented, and analyzed the hazards

associated with the technology itself. Additionally, I participated in the analysis of the implementation and functional hazards. Furthermore, I assisted Alfonso Gutierrez and the UW RFID team in performing and analyzing the Wireless Communication Protocols study. Finally, I constructed the traceability matrix, linking all of the hazards and mitigation strategies with verification and validation procedures.

CHAPTER 3: METHODS

The hazard analysis for Phase One consisted of four primary steps: the identification, definition, crosschecking, and ranking of hazards based on the impact the hazard has on the system, patient, or safety of the blood product when the system fails or a design flaw is uncovered. Verification and validation of the mitigation strategies, as well as corrective actions, were examined through extensive use of protocol testing, unit testing, and system testing. This was done to ensure that the functionality of the system remained continuous and effective. A traceability matrix was also constructed to illustrate the sources, methods, and results of the tests of each hazard mitigation strategy. Upon complete analysis of the results of each test, complete operational understanding of the new iTrace^{TM} throughout the entire supply chain was achieved. Then, a subjective evaluation was completed to determine the resultant risk and appropriate steps to be taken. There is

no consistent or standard method for estimating this, but the severity and likelihood matrix which will follow generally derives acceptable results for low- to medium-risk devices.

HAZARD IDENTIFICATION

The process undertaken for identifying the hazards began with a thorough analysis of the use of the iTrace™ in the entire blood transfusion supply chain. It entailed detailed consideration of the system's intended use, features, and functions throughout each stage. The first step involved the review and gathering of potential relevant harms from a list of known and foreseeable hazards. These hazards were found in the SysLogic Quality Document standard. They tended to consist of implementation and functional hazards such as those involving security, access, alerts, and notifications.

The next step consisted of the analysis of distinguishable iTrace™ characteristics using the system design and requirements documents. Hazards identified for this group comprised those which had an impact on the basic functionality of the system. General system attributes and properties such as read/write failures, bad tag data, and altered tag data were found by reviewing the possible vulnerabilities or threats associated with each

feature or requirement. In other words, harms were diagnosed by accounting for any inadvertent instances of system failure or deviation from intended use.

After that, additional hazards were discovered by analyzing factors presented in the protocol studies. The Limit Testing protocol revealed hazards dealing with the effects of 13.56 MHz radio frequency (RF) magnetic field radiation on the temperature elevation and toxicity of cellular protein structures of red blood cells (RBC), aged red blood cells (aRBCs; near expiration of the 42 day shelf life), whole blood derived platelet products (WBDP), plasma, and plasma coagulation factors under extreme RF exposure conditions. This study was concerned with the potential consequence of 13.56 MHz on blood products, and its possibility of leading to: 1) a rise in the temperature of blood products (red cells, pooled platelets, and plasma) due to dielectric heating generated by extended exposure to the intense RF field, or 2) cellular or protein degradation from extended exposure to the intense RF field. Therefore, hazards were uncovered by noting the adverse thermal or biological effects on the transfusion safety or efficacy of blood cellular products and coagulation factors that may arise from exposure to intense RF radiation from 13.56 MHz RFID readers.

Additionally, the Performance Testing protocol sought to determine the commercial applicability of the RFID system solution in the blood transfusion medicine industry. As

many aspects of the performance capability of RFID tags as possible during the most common blood supply chain processes were evaluated. The study combined the four different types of readers: (1) TagSys HF RFID Tunnel, (2) TagSys HF RFID Flatbed, (3) Unitech handheld, and (4) Tracient PadL with all of the traditional containers used for blood products – Coleman cooler, tray, two generic Styrofoam boxes and platelet boxes – in varying groupings to determine the efficacy. The different combinations were applied at each of the RFID-enabled checkpoints in the blood supply chain process to thoroughly assess where and what types of hazards may occur, as well as how to combat them. Hazards were revealed by probing the scenarios which could occur if the system did not perform as expected with any of the above-mentioned combinations of commercial application.

Furthermore, analysis of the RFID Tag Survivability Protocol helped to identify hazards by investigating functional tag performance changes that could arise from exposure to centrifugation, blast freezing, and gamma irradiation. The studies simulated operational conditions equivalent to those a blood product would traditionally undergo. These methods can lead to degradation in tag functionality or, ultimately, failure. As a result, hazards were discovered by understanding the worst case effects that these processes could have on the system and users.

The HF RFID Application in Blood Centers Wireless Considerations Protocols investigated the potential effects of electromagnetic interference (EMI) on existing medical equipment and systems, as well as among High Frequency (HF) RFID entities. Such consequences included instances in which there was an interruption or failure in wireless, waveform data, or communication transmissions. Hazards were identified by assessing unfavorable outcomes related to EMI effects and erroneous and/or incomplete system communications. The culmination of all these aforesaid processes has led to the comprehensive group of hazards identified, described, and rated in this study.

In analyzing the hazards and the procedures that may be taken to mitigate them, the following verification and validation methods were employed.

VERIFICATION STRATEGY

For each, the team analyzed the risk of implementing the technology to avoid potential hazards. Testing protocols were created to ensure that each technology hazard was mitigated. It was verified that the technology used met safety and critical functionality requirements, via the following:

a. **Limit Testing Protocol** – Ensured RF radiation had no adverse effects on blood products. Limit testing in phase 1 of the RFID project indicated 13.56 MHz RF

energy had insignificant temperature and biological effects on RBC products that were < 11 days old and whole blood-derived platelets even at very high magnetic field levels of 5 amperes/meter and extended exposure durations. Results of initial limit testing were reported to the FDA on January 21, 2008, which confirmed the safety of 13.56 MHz RF with RBC and platelets and led to the agency's consent to proceed with prototype testing and pilot use of the system with those products. Aged red cells (nearing expiration of the 42 day shelf) and thawed plasma products were also tested.

This protocol was initiated to examine the effects of 13.56 MHz radiofrequency energy under the most extreme conditions possible in order to demonstrate the slight likelihood that the identified potential hazards could arise. It was utilized to evaluate the effects of RF frequency because, if the conditions established for the study far exceeded any to which a blood product would customarily be subjected, then the probability of the hazard occurring would be minimal. Thus, this test of extreme conditions was highly valuable for ranking the hazards associated with it by demonstrating the ways in which the hazard could be reduced.

All of the blood products were tested in the same manner. The only variation was in the bag volumes and normal storage and testing temperature requirements for

each type of product. Therefore, all of the normal processes that blood products would experience were considered, yet with the unique requirements essential for each.

b. **Tag Survivability Protocol** – This protocol was used to confirm the safety, reliability, and performance of the 13.56 MHz RFID technology as follows: RFID tag survivability and resiliency under centrifugation, irradiation, extreme cold (blast freezing and thawing), as well as RFID tag security and integrity, electromagnetic interference effects and temperature and biological effects of 13.56 MHz RF energy on plasma and aging red blood cells.

   The Survivability studies were designed to either simulate operational conditions equivalent to those a regular blood product would normally undergo or subject the blood product to extreme exposure when encountering centrifugation, blast freezing, and gamma irradiation. Since the solution will be commercialized in the transfusion medicine industry, it was critical to uncover the impact of both. The survivability tests were intended to serve as a complement to the standard systems software test.

   The protocol was selected because of its ability to account for different processes and show the functionality of the tag in a general commercial environment. All of

the different types of tests were run in the same manner, and the potential hazards that arose from each process – centrifugation, blast freezing, gamma irradiation – were identical as they could lead to similar functionality deviations and failures.

c. **Performance Testing Protocol –** Evaluated RFID tag read/write performance during the most common blood supply chain processes using a defined set of performance measure indicators. Tag performance refers to whether the coupled system tag/reader performs satisfactorily (reading/encoding tag content) in simulated scenarios including different bag containers, packaging materials, and different types of readers.

   This protocol was significant as it tested varying combinations of system functionalities. It was selected to mimic traditional processes. As it was based on the performance of the system, it was important to have protocols which would imitate scenarios that would occur in common settings. Likewise, it was valuable to evaluate all possible reader/container relationships to investigate all potential situations that could take place.

d. **EMI Testing Protocol** – Determined whether there is potential electromagnetic interference (EMI) from high frequency (HF)-based RFID systems on existing medical equipment, as well as the potential EMI of HF RFID equipment on

existing wireless devices and systems found in donation and processing centers. The protocol also identified any potential for erroneous and/or incomplete communication between HF RFID entities (e.g., between tag and reader or between reader and server) due to EMI from other devices. Where applicable, proactive measures to minimize or eliminate EMI effects were also suggested. This protocol was essential as it demonstrated the effectiveness of the system when placed in proximity to other similar technologies. It showed the ability of the system to still function without impeding the capabilities of the other systems. It also demonstrated the ability of the iTrace™ to work as intended without leading to the harm of patients as a result of disrupting wireless, waveform, and communication transmissions.

The capabilities of the system were tested by placing the iTrace™ at varying proximities to a range of other medical devices. This methodology was selected in order to determine its effects within and between technologies at different distances. It was a worthwhile procedure as it showed the impact of the technology on an array of different systems and from a range of distances.

VALIDATION STRATEGY

Validation tests were used to determine whether the technological design, implementation, and functional capabilities of the system operated as expected. The instances in which the system was unsuccessful at achieving anticipated results served as demonstrations of potential weaknesses, risks, and hazards to system use. The tests consisted not only of desired outcomes, but also of unfavorable circumstances that could potentially cause malfunctioning of the system or the reading/writing of inaccurate data. The thoroughness of the testing was essential to the discovery of both the benefits and hazards of employing the system.

a. **System Testing** – Final end-to-end test of the RFID solution conducted by the RFID Consortium. All system functionalities of the iTrace™ were evaluated. The system tests were conducted in accordance with the Consortium's software development life cycle. Successful completion of system testing was required prior to release for user acceptance testing. During system testing, the proper interdependency between hardware, software and interfaces was validated. Each system capability throughout each stage of the blood transfusion supply chain from donor to blood center distribution was evaluated.

   A total of 29 system tests were run on the iTrace™. The common operational

functions and systematic procedures of the iTrace™ are all referenced in one or multiple system tests. System testing was selected as it took into account all of the possible system functionalities and capabilities, as well as potential hazards and hazard mitigation/correction procedures that could be applied from the beginning to the end of Phase One.

During testing, team members validated that the functionality included in the system operated accurately and reliably as a whole and met performance criteria prior to user acceptance testing. Testers validated the system by:

- Following the System Test Plan (developed using the Consortium's System Development Life Cycle)
- Checking that the interface is properly designed
- Proceeding "top down" or "bottom up" as required

Nonconformance was documented on the system testing results documentation and summary documentation. Correction and retesting occurred as required.

b. Unit Testing – Extensive unit testing was conducted on the iTrace™. The principal objective of unit testing was to take individual components of testable software and processes of the application, isolate them from the

remaining elements, and analyze their behavior. Units were tested independently prior to incorporating them with other processes. In other words, each stage within the blood transfusion supply chain was tested separately. Several hazards anticipated as a result of the implementation or functionality of the iTrace™, as well as some based on the technology of the system, may be linked to one or many unit tests.

The unit tests were performed to verify that the iTrace™ and its middleware software piece would accurately capture data relating to the Blood Transfusion Supply Chain collection, tracking, monitoring, and processing of products and materials. The aim of the system is not only to enable greater traceability, but also to enhance the efficiency of key supply chain operations.

There was a total of 21 Unit Tests carried out to effectively test the functioning of the system throughout all stages of the supply chain from donor to blood center distribution. Various conditions that could occur within these stages, as well as expected results, actual results, and discrepancies were documented for each test. The test was deemed successful if the operation concluded as anticipated. The test was considered a failure if the incident which actually ensued was a deviation from the intended design or

functionality of the system. These steps were taken to comprehensively evaluate all aspects of the system from end-to-end.

c. **Performance Qualification** – Formal validation completed by a user/customer in a regulated environment. The purpose is to validate use of the system tested solution within the context of specific operations using Standard Operating Procedures (SOPs) or Quality System Designs (QSDs) and training documentation. It further ensured that key functions perform at acceptable speeds. Key functions are identified (e.g., remote and on-site user access screens, system processing and data retrieval, network interfaces and external system interfaces) and an acceptable performance standard is achieved. This validation ensured that the system, training of users, and SOPs/QSDs work together, as expected. Successful completion of Performance Qualification (also referred to as user acceptance testing or beta testing) was a precursor to allowing use of the system in the pilot phase. This test was done to demonstrate the usefulness of the system in a real, commercial environment.

   Prior to testing, the test team received training for conducting testing. During testing, users thoroughly tested and accepted the RFID application before it

could be authorized for pilot use. They tested the system in the QA instance by:

- Following the Performance Qualification Test Plan (developed using BCW's QSDs relating to Performance Qualification)
- Testing their own SOPs or QSDs
- Validating the training received to use the system
- Validating the user guide

Nonconformance was documented according to performance qualification QSDs in place at BCW. Correction, retest, and validation occurred as required before placing the system into the pilot phase. Following a successful pilot, the system was released for production use. After the Performance Qualification Test was executed, a summary was prepared and approved.

Thus, the methods described illustrate the foundation of a comprehensive strategy for identifying hazards and assessing the strategies for reducing or mitigating them. There was a detailed, thorough process for identifying the hazards, as well as an all-inclusive approach for testing them with simulated, extreme, regulated, actual, and end-to-end methodologies. All tactics were valuable for the overall formulation of a practical

procedural framework for hazard identification and testing.

SEVERITY AND LIKELIHOOD ANALYSES

The hazard class was determined by the impact of the hazardous effects on the system, other systems, or individuals. The level of injury was rated by the damage done or degree of harm. For example, if the hazard had the potential to simply interrupt current processes, then it was given a severity level of one. On the other hand, if the hazard led to the complete destruction of the system, failure of the tag, or mis-transfusion to the patient, then the severity rating was the highest at five – critical.

Severity Estimate

The severity estimate has been determined in keeping with definitions, criteria, and guidance as defined in SysLogic's Quality Plan. It is defined as the qualitative rating of the possible consequences of a hazard. There are four (4) levels of severity ratings as seen in the Guidance on Severity Levels table (Table 3):

1- **Negligible** (no injury; irritation and/or discomfort only)
2- **Mino**r (recoverable minor injury; no loss of function)
3- **Moderate** (moderate injury or recoverable, non-life-threatening injury)
4- **Critical** (major/life-threatening injury, or death)

Table 3: Guidance on Severity Levels

Severity	**Level**	**Description**
Negligible	1	No injury; irritation and/or discomfort only
Minor	2	Recoverable minor injury; no loss of function
Moderate	3	Moderate injury or recoverable, non-life-threatening injury
Critical	4	Major/life-threatening injury, or death

Likelihood Estimate

Consideration was also given as to the likelihood that each identified hazard might occur. As the iTraceTM is a new technology, the probability of occurrence was deemed by assessing the number of times the hazard actually occurred during system testing and/or by taking the opinions of consortium experts into account. The final estimate was the weighted average of all responses. The number of outcomes that were possible were also specified and discussed. The number of times the event may occur over a particular period of time in relation to the number of possible outcomes is the means by which the likelihood estimate was established.

SysLogic's Quality System uses five (5) likelihood ratings as seen on the Guidance on Likelihood table (Table 4):

1- **Improbable** (so unlikely that it is assumed it will never occur)

2- **Remote** (unlikely but may occur over the range of users)
3- **Occasional** (once per device over its intended life, or once in 6 months)
4- **Probable** (less than once per week but greater than once per month)
5- **Frequent** (greater than once per week)

Table 4: Guidance on Likelihood Levels

Likelihood	**Level**	**Description**
Improbable	1	So unlikely that it is assumed it will never occur
Remote	2	Unlikely but may occur over the range of users
Occasional	3	Once per device over its intended life (6 months)
Probable	4	Less than once per week but greater than once per month
Frequent	5	Greater than once per week

Risk Acceptability Rating:

By weighing the severity of a risk against its likelihood of occurrence, an overall risk acceptability rating was obtained. SysLogic's Quality System uses the legend and matrix below (Table 5) to assign a risk acceptability rating. The way to compute the Risk Acceptability is shown in Table 6.

Table 5: Legend for Determining Resultant Severity Risk of the Device

Risk/Hazard Class	**Severity**	**Probability**	**Risk Level**
No damage; inconvenience only	1-Negligible	1-Improbable	A-Acceptable
		2-Remote	A-Acceptable
		3-Occasional	B-Tolerable
		4-Probable	C-Intolerable
		5-Frequent	C-Intolerable
Minor damage, no loss of tag/system function, or recoverable minor damage	2-Minor	1-Improbable	A-Acceptable
		2-Remote	B-Tolerable
		3-Occasional	B-Tolerable
		4-Probable	C-Intolerable
		5-Frequent	C-Intolerable
Moderate damage or recoverable non-permanent impairment/loss of function	3-Moderate	1-Improbable	B-Tolerable
		2-Remote	B-Tolerable
		3-Occasional	C-Intolerable
		4-Probable	C-Intolerable
		5-Frequent	C-Intolerable
Major damage (permanent impairment or total loss of function)	4-Critical	1-Improbable	B-Tolerable
		2-Remote	C-Intolerable
		3-Occasional	C-Intolerable
		4-Probable	C-Intolerable
		5-Frequent	C-Intolerable

Table 6: Risk Acceptability Computation Table

		Severity			
		Negligible	Minor	Moderate	Critical
Likelihood		1	2	3	4
Improbable	1	A	A	B	B
Remote	2	A	B	B	C
Occasional	3	B	B	C	C
Probable	4	C	C	C	C
Frequent	5	C	C	C	C

SysLogic's Quality System defines the risk acceptability ratings as follows (Table 7):

Table 7: Definitions of Risk Acceptability Ratings

A	**Acceptable Risk:** The risk comes within the broadly acceptable (green) region, i.e., either the severity of the harm or the likelihood of occurrence of an event is so slight that the risk can be neglected compared to the risks of other hazards. There is not necessarily a need to reduce this risk.
B	**Tolerable Risk:** The risk comes within the ALARP (As Low As Reasonably Practicable) region (yellow), between the broadly acceptable and unacceptable region; i.e., the risk is reduced to the lowest reasonably practicable level. Risks in this area must be carefully weighed with regard to the efficiency of the device and the workload/expenditure for reduction of the risk. A risk ranging near the unacceptable region will normally be reduced even though this may involve high cost expenditure.
C	**Intolerable Risk:** The risk comes within the (red) unacceptable/ intolerable region, i.e., the risk of the hazard is so severe that a system/ device involving such hazards would be intolerable. A risk within this region has to be reduced by reducing the likelihood of occurrence of that hazard.

Risk Assessment Process and Inter-rater Reliability

The risk assessment process involved determining the extent of the consequence as well as the frequency with which it was expected to occur. The severity was determined by measuring the impact to the system, staff, or patients. For example, the wireless communication hazardous event in which unauthorized access occurs during the communication between the transmitter and receiver was given a level three severity. This is because the unauthorized access could lead to enough problems that it would generate a fair amount of concern, yet not enough to cause irreparable damage to the system or harm to the patient.

Additionally, this hazard was assigned a level one likelihood. This is primarily due to the rigor applied to reduce it. There were several techniques performed including adhering to provisions in air protocols and standards which make it difficult to inappropriately access data during communication, limiting the communication range between the tag and reader, designing the tag to ensure data integrity, neglecting to include transmission of confidential medical data, and incorporating data encryption security on the wireless network. The combination of these approaches minimized the potential of occurrence to the point that it was improbable. Furthermore, the number of times the hazard was experienced during any of the verification or validation procedures was also taken into account. Ultimately, this hazard received a Pre-Mitigation Risk level score of B.

Nevertheless, since this assessment took place prior to completely implementing the device, the evaluation was obviously highly subjective. As such, inter-rater reliability was essential. My assessment and scoring assignments were reviewed, discussed, and approved by the teams of consortium members. The consortium met and agreed on the risk assessment assignments for each hazard.

SUPPLEMENTAL SEVERITY ASSESSMENT

As a supplement to assessing the risk using the accepted SysLogic, Inc. technique, I included an additional measure. Since the severity of the hazard is partially calculated by the success of the method of control, the following scale was included to further illustrate its impact.

I. **Prevents/Mitigates the Hazard from Occurring**: This measurement reflects the ability of the method of control to deter the risk from happening. It is the most highly desired effect of the controls. The risk legend would extend to, for example, AI.

II. **Corrects/Remedies the Situation Following the Occurrence of the Hazard**: This measurement reflects the ability of the method of control to respond to the hazard post-occurrence. It includes resolution strategies and back-up plans to account for hazards. It is not as appealing as the prevention

methodologies, but it does provide an effective solution to dilemmas that may unfold. The risk legend could potentially extend to AII or BII for example.

III. **No Effect on Hazard Mitigation or Correction**: This measurement reflects the total inability of the strategy to proactively inhibit or counter the risks associated with iTrace™ use. It consists of the most undesired methodologies due to the lack of efficiency in negating or amending processes in the face of hazards. The risk legend could apply as CIII for example.

CHAPTER 4: TECHNOLOGY HAZARD ANALYSIS

It is evident that it is necessary to analyze the risks of implementing HF RFID (13.56 MHz) technology and system tools to avoid potential hazards. The impact a hazard would have on the efficacy of blood products and, perhaps ultimately, on patient safety in the event a failure occurs or a design flaw is discovered should be assessed. The technology hazards are the potential harms that may occur from technology or system conditions, or from human interactions with these conditions. These hazards were identified using the methods described above. The following safety and critical design requirements will be discussed in this chapter:

- Preventing Read/Write Errors or Failure.
- Ensuring No Adverse Effects of RFID Technology on Blood Products.
- Ensuring Performance Capability of RFID Tags During the Most Common Blood Supply Chain Processes.
- Ensuring RFID Tag Survivability After Experiencing the Most Demanding Conditions in the Blood Supply Chain.
- Ensuring No Interference of RFID High Frequency (HF) and Electromagnetic Interference (EMI) with Other Systems.

TECHNOLOGY – SAFETY CRITICAL DESIGN REQUIREMENT: PREVENT DATA READ/ WRITE FALIURE

There are six potential system hazards which could potentially affect the ability of the iTrace™ to effectively read/write essential data. The first is a general read/write failure due to any malfunction of the handheld or pad RFID reader. The consortium team rated this as a one on the severity level and three on the likelihood level. This indicates that, while the hazard may occur occasionally, it will not cause any significant harm to the patient, blood products, or system. The mitigation applied to this is a simple, yet helpful solution that is reflective of the inherent functionality of the middleware used in the application. Each time a tag is read/written by a handheld or pad reader, an audible sound

is heard. This notifies the user that the tag was successfully read/written. Additionally, the handheld and/or work station display is also updated with the newly read/written information in the instance of successful completion of the activity. If an error is, in fact, detected, the application prevents the user from continuing the process until the current problem is resolved. Moreover, should the RFID reader fail, the user may revert to the standard barcode reader to read/write the same information.

The pre-mitigation risk for this hazard was rated a **B**. Level B signifies a tolerable risk. It falls within the As Low as Reasonably Practicable (ALARP) region. The hazards which fall into this category must be measured in comparison to the advantages of utilizing the device and the methods taken to reduce the risk. In other words, the cost of minimizing the risk must be lower than the value of using the device. The results of the analysis on cost vs. benefit of employing the iTrace^{TM} with regards to each hazard described will take place in the Discussion Chapter.

Likewise, the second hazard is again an overall read/write failure, this time due to any breakdown in the process associated with the RFID tunnel reader. The RFID tunnel reader reconciles blood product containers and their contents as they are checked into the Blood Center and shipped to/from the Blood Center. Reconciling refers to the system's role in verifying that the expected container and its contents correctly match what is

actually presented. As with the first hazard, the consortium rated this hazard a one on the severity scale and a three on the likelihood scale, showing that it has the potential to happen intermittently, but will not lead to any harm when it does.

The mitigation strategy used here was the application of yet another inherent functionality of the middleware: the software driver for the tunnel reader. The software driver can determine whether items are missing or excess items are present in containers. If a RFID tag is detected for a product that is not anticipated to be included in a container during the tunnel read check-in process, the product is flagged as an “excess” item. The operator is then required to manually inspect the container and its contents to correct the issue.

Similarly, if the RFID tag for an expected product is not identified during the tunnel read check-in operation, the application notifies the operator of the potentially “missing” item. Again, the operator is instructed to manually inspect the container to determine if the product is, in fact, missing, if the RFID tag failed, or if the tag was blocked by other container contents. For this hazard, the operator is always charged with manually examining the container to resolve any discrepancies. In addition, in the event of an RFID reader failure, the user maintains the option to use the standard barcode reader to read the same data which is barcoded on the label.

The pre-mitigation risk for this hazard is also a Level **B**. The risk is tolerable, yet there is a need to diminish it. We must assess whether the benefits of employing the device outweigh the cost of mitigating this hazard.

The third hazard that must be lessened to meet the safety critical design requirement of preventing data read/write errors/failures is the risk of bad data on the tag. This RFID hazard is caused by corrupted data existing on the tag. This hazard was given a level three severity and level one likelihood. The ratings indicate that the risk is of moderate severity, leading to relative, though recoverable and non-permanent, damage, injury, or loss of function; however, it is improbable, assuming it will likely never occur. This presents the highest severity, yet least likelihood, thus far.

Bad data on the tag could hypothetically be the result of harsh conditions experienced by the tag such as centrifugation, blast freezing, and gamma irradiation; but, formal protocol testing was conducted on tag survivability, examining the effects of these techniques under extreme and excessive circumstances. The study, which will be explained in more detail subsequently, demonstrated that these methods would not significantly affect the performance or survivability of the tag.

Furthermore, a new ISBT128 data structure was developed to enable more advanced detection of tag memory corruption. An ISBT-128 local data identifier is used to facilitate

the parsing of this field from other ISBT-128 data structures. Also, the ISBT-128-compatible memory checksum data structure is used. The system is designed to recalculate and rewrite the data every time the tag data changes. When the full tag data structure is read, the reader calculates and compares its result with the data values already stored in the memory block. If even one bit of the tag memory is corrupted, the recalculated and stored data identifier will disagree, indicating that memory corruption has occurred.

The pre-mitigation risk for this hazard is a Level **B**. As such, the hazard is determined to be tolerable. Despite the moderate risk presented with this hazard, it is still acceptable due to the unlikely possibility that it will occur.

The next RFID system hazard that falls into the read/write error category involves the subsequent alteration of the donation identification number (DIN) written on the tag at collection. This hazard may be due to the lack of enforcement of the DIN field locking on the tag. It was rated a two on both the severity and likelihood scales, indicating a minor severity with no loss of tag/system functionality and a remote possibility of occurrence.

The method of control involves the configurable design of the application, which allows the organization to use the DIN locking feature at the point of collection or at labeling. The locking process unfolds as follows:

1. The DIN labels for the entire blood collection set are placed on individual bags prior to collection. This includes placing an RFID tag on the RBC bag. All bags receive both an RFID tag and DIN label during apheresis collection.
2. The handheld reads the DIN bar code label and writes the ISBT-128 DIN data structure contained in the bar code directly into the tag without any data transformation.
3. Every ISO 18000-3 mode 1 RFID produced has a Tag ID Number (TIN). The TIN is a unique factory-programmed 64-bit serial number, which includes the manufacturer ID and tag model number. Both the TIN and the DIN are recorded in the RFID database.
4. The DIN data structure is read back into the RFID reader to verity that it was written precisely.
5. The four 32-bit data blocks containing the DIN on the tag are then permanently locked by the RFID reader, inhibiting the threat of the data ever being modified or overwritten.
6. The lock bits can be read back by the reader to confirm that locking did actually take place.

In the rare instance in which the tag failed to physically lock the DIN memory blocks, and the DIN was altered, the DIN and TIN are associated in the RFID database.

Therefore, if the DIN on the tag changes, the next time the tag is read, an error will be displayed to alert the operator that the DIN and TIN do not match.

The pre-mitigation risk for this hazard was rated a Level **B** by the consortium. Here, the risk is highly tolerable because it is both minor and rare. Nevertheless, as with all tolerable risks, the value in relation to the reduction of the risk must be assessed.

The next hazard to be evaluated was the potential for the DIN created at final labeling to be altered. As with the last hazard, this hazard may be the result of the DIN field locking not being enforced. Additionally, this hazard also receives a severity and likelihood rating of two and two.

The method of control executed to mitigate this was as follows. If there was no RFID tag present at final labeling, a blank RFID tag was affixed to the product bag. The process of printing, applying, and verifying the barcoded final label occurred as normal. The labeling operator then began the process of programing the ISBT 128 label data structure by placing the product on an RFID pad reader which is connected to the RFID server. The server had an application titled “Label Product,” which the operator launched. The operator then scanned the DIN and Product Code barcodes from the blood bag, and selected the “Label” button. The data was then uploaded to the RFID server, which gathered all other required information from the BECS. The pad RFID reader wrote all

the required ISBT-128 data structures including the ISBT-128 DIN Data Structure into assigned memory blocks. All memory fields on the tag were then read again to confirm that the data was successfully written to the RFID tag's memory, and coincided with data received from the BECS' master file. The tag's TIN was read by the RFID server and permanently associated with the DIN and product code in the database. Finally, the two 32-bit blocks containing the ISBT-128 ABO data structure and the four 32-bit blocks containing the ISBT-128 DIN data structure were locked, rendering them unalterable.

Here, again, the Pre-Mitigation Risk was a Level **B**. It fell in the middle of the tolerable risk category, putting it at the exact midway point between the acceptable and intolerable region. Consequently, it was likely that it could be reduced without a great deal of cost expenditure.

The final risk falling into the category of read/write RFID system errors was the potential hazard of the ABO being rewritten on the tag. The severity and likelihood ratings of this hazard were three and one respectively. This indicates a moderate severity with an improbable chance of occurrence. The method of control applied here dealt with the placement of the ABO label for the blood bag on the individual bags during final labeling. It included placing an RFID tag on products that did not already carry one. The process of printing, applying, and verifying the barcodes on the final label remained

unchanged. As with the hazard of the alteration of the DIN at final labeling, this procedure for programing data structures was applied, ultimately rendering the ABO data structure unchangeable. The Pre-Mitigation Risk was a **B** for this hazard. The risk remained tolerable, yet needed to be mitigated or decreased.

TECHNOLOGY – SAFETY CRITICAL DESIGN REQUIREMENT: ENSURE NO ADVERSE EFFECTS OF RFID TECHNOLOGY ON BLOOD PRODUCTS

The five hazards that could impact the safety and critical design requirements necessary to ensure no adverse effects of RFID technology on blood products were examined through the use of a formal protocol and testing procedures. The Limit Test Protocol for Radio Frequency Exposure Testing was performed. The background for the protocol testing was as follows. 13.56 MHz is the global standard frequency recommended for blood transfusion medicine by the International Society for Blood Transfusion (ISBT) working party. There were several criteria for selection of this operating frequency, including: 1) 13.56 MHz is a global standard frequency for RFID usage, supporting the ISBT's global mandate, and 2) at this frequency, the RF signal contains only a magnetic field component and the electric field is suppressed, thereby minimizing the possibility of biological interaction.

In order to prevent adverse occurrences resulting from the use of RFID in the transfusion medicine supply chain, the objective was to outline test protocols and success criteria for evaluating the worst-case effects of 13.56 MHz RF magnetic field radiation on the temperature elevation and toxicity of cellular protein structures of red blood cell (RBC), whole blood derived platelet products (WBDP), plasma and plasma coagulation factors under extreme RF exposure conditions.

The RFID Consortium, under the guidance of the FDA, developed and undertook this protocol testing regimen to ensure that the proper methods of control for mitigating the potential hazards were established. The RBCs, WBDPs and plasma products followed identical RF testing protocols. The only difference was in the bag volumes and normal storage and testing temperature requirements for each type of product.

The testing methodology for these protocols included three iterations of identical exposure conditions to CONTROL and TEST bags appropriate to the product being tested under exposure guidelines provided by Center for Devices and Radiological Health (CDRH). The testing was designed to focus results in two primary areas of interest to CDRH and Center for Biologics Evaluation and Research (CBER) respectively:

- Any rise in temperature of blood products (red cells, pooled platelets, and plasma) due to dielectric heating generated by extended exposure to the intense RF field, and
- Cellular or protein degradation from extended exposure to the intense RF field.

The potential hazards included:

1. High Frequency RF radiation could increase the temperature of RBCs and platelets beyond acceptable level of 1.5 °C due to Joule heating.
2. High Frequency RF radiation could lead to increased degradation of RBC cellular and protein structures beyond acceptable level of hemolysis of ≤1%.
3. High Frequency RF radiation could lead to increased degradation of WBDP cellular and protein structures, such that the pH decreases beyond acceptable level of ≥6.2.
4. High Frequency RF radiation could increase the temperature of plasma types (FFP, FP24, and TP) beyond acceptable level of 4 °C due to Joule heating.
5. High frequency RF could degrade the activity of the coagulation factors (PT, aPTT, Antithrombin Activity, Factor V, Factor VIII, Factor XI, Protein C, Protein

S, VWF: RCo) levels of three types (FFP, FP24, and TP) of thawed plasma products beyond an acceptable level of 20%.

The joint mitigation strategy for all of these hazards was associated with this protocol. The RFID Consortium study team chose to enlist the involvement of the FDA CBER at an early stage to determine its level of interest or uncover any concerns related to the use of RFID in transfusion medicine. The FDA emphasized the necessity of identifying and assessing the total impact, if any, that radio frequency energy may have on the safety and efficacy of blood products. The FDA also prohibited the use and transfusion of blood products in an RFID-enabled pilot study until they had reviewed the *in vitro* test results of an accepted protocol.

As a result of the testing conducted at the CDRH (54, 55), the FDA CBER and CDRH proposed the execution of a more specific and exhaustive protocol consisting of a limit test that would simulate worst-case scenarios. These organizations, along with the consortium, collaborated to develop the Limit Test Protocol, including the parameters to be studied, the length of time the products would be exposed to RF energy, the RF magnetic field strength, the type and number of products to be studied, and the acceptance criteria. A single RF Limit Test Protocol would be performed for all products.

The intent of the Limit Test was to expose blood components to extraordinarily higher RF power levels and for longer durations than would ever be seen in practice, and compare those results with an unexposed control group. The Limit Test in question would test for both thermal (Joule Heating) effects on the blood products, as well as assay changes in cellular and chemical parameters.

The consortium estimated that the average exposure of a blood bag over its entire useful life would be at a RF magnetic field strength of 1 Ampere/meter for a discontinuous period of less than 21 minutes. The Limit Test simulated a 13.56 MHz RF magnetic field strength of 5 Amperes/meter for a continuous exposure period of 23-25 hours (56). In other words, the blood products were tested at hundreds of times the exposure they were anticipated to experience during normal use.

Because there was no known apparatus that was of the size and capability to hold a blood bag in a uniform, intense 13.56 MHz RF magnetic field of 5 Amperes/meter field strength, Hohberger and Tsirline of Zebra Technologies designed and constructed a segmented 86cm Helmholtz coil with 90 Watts RF input (56). This simulated a constant repeating RFID reader interrogation. Zebra Technologies donated the entire apparatus to the University of Wisconsin RFID Lab.

Each test used identical test and control bags, with only the test bags experiencing the full RF exposure. The control bags were placed outside of the RF field. Product samples were collected from each bag prior to the start of the test, after 7 hours, and at the end of the test period of 24 hours. *In vitro* chemical, morphological, and biological assays on both control and test bags were performed. The temperature at each bag's surface and core were measured every minute. The detailed testing and results have been documented and published (19, 57).

There were two rounds of Limit Tests. The first round included tests performed on young red blood cells (RBCs) and whole blood-derived platelets (WBDPs) at the BloodCenter of Wisconsin. Personnel from the University of Wisconsin RFID Lab, under the direction of Alfonso Gutierrez, and from the BloodCenter of Wisconsin under the direction of Graminske, conducted the Limit Testing on both AS-1 packed RBC products at 4◦C that were six to nine days old and fresh WBDP at 22-24◦C. These Limit tests were performed at RF magnetic field levels of 5A/m and extended exposure durations for 24 hours. Three pairs of bags were tested, with each pair consisting of a control bag (placed 2m outside of the coil center) and a test bag (placed at the center of the Helmholtz coil). Due to the extension of the magnetic field beyond the Helmholtz coil, the control unit was exposed to only 0.64% of the RF magnetic field strength generated at the location of the test product (56). This exposure was deemed acceptable and negligible in the protocol review.

The study results demonstrated that RBC and WBDP products had no increased cellular/protein degradation after extended exposure to RF. Joule heating by the RF field had acceptable effects on the temperature rise of RBC and WBDP (35). More specifically, the findings were as follows (19):

- Hemolysis of young (6-9 days old) RBCs after 23-25 hours of RF energy exposure was <0.2% for all TEST and CONTROL RBC units, well within the ≤ 1% limit of the FDA-approved acceptance criterion.

- While there was minimal RBC TEST versus CONTROL bag center temperature rise due to Joule heating, the average 0.14 ± 0.35 °C relative temperature increase measured at the end of the test between TEST and CONTROL units never exceeded the 1.5 ºC acceptance criterion.

- No clinically significant changes were observed in RBC, Hb, Hct, MBC, RBC morphology and potassium in the RBC TEST versus CONTROL group.

- For WBDP, the mean pH of the measured TEST group pH was 7.27; CONTROL group pH was 7.19, exceeding the minimum pH criterion ≥ 6.2.

- The maximum temperature increase of the WBDP TEST unit relative to the CONTROL was 0.30 ± 0.27°C, not exceeding the 1.5° C criterion.

For the second round of testing, the FDA expressed concern that aged red blood cells (aRBCs) – those near expiration of the 42-day shelf life) might be more susceptible to the effects of radio frequency than young RBCs and should be tested. This study utilized the same testing protocol as the first, and allowed measurement of peak transient temperatures in the aRBC and plasma bags prior to their achieving thermal equilibrium (57).

Pairs of aRBC control and test bags of the same age and blood type from no later than day 41 of storage were used so that testing was completed by the 42-day product expiration. For the plasma tests, the objective was to show that long-term RF exposure did not impact the coagulation factor levels of thawed plasma products. All plasma products were donated by females of blood group O. The Applied Research Lab at BloodCenter of Wisconsin (BCW) thawed the frozen plasmas at 30-37◦C. Nine pairs of aged frozen plasma products, three each of three types, were randomly selected by the BCW's Component Department. Nine pairs of aged frozen plasma products, three each of three types, were randomly selected by the BloodCenter of Wisconsin's Component Department. The three types of plasma units selected for testing were:

1) FFP (*plasma frozen within 8 hours from collection*) was freshly thawed and stored at 1°C - 6°C for up to 24 hours. Testing started on the day of thaw.

2) FP24 (*plasma frozen within 24 hours of collection*) was freshly thawed and stored at 1°C - 6°C for up to 24 hours. Testing started on the day of thaw.

3) Thawed plasma (TP) (*plasma frozen within 8 hours from collection*) was thawed 4 days prior to testing and stored at 1°C - 6°C for up to 5 days. Testing started on day 4 of thawed storage.

Plasma testing always began on the day prior to shelf life expiration so that the end of the testing was on the same day the product expired. Prior to any Limit Testing, the thawed plasma pairs were each aseptically pooled together, mixed and then equally divided into test and control bags.

The RF exposure protocol for all plasma pairs was identical to that used in the aged RBC trials. All plasma products were assayed at zero, seven, and 23-25 hours for Prothrombin Time (PT), activated Partial Thromboplastin (aPTT), Antithrombin III, Factor V, Factor VIII, Factor XI, Protein C, Protein S, and von Willebrand factor ristocetin cofactor (VWF:RCo) activities.

The results for the second round of testing for aRBCs were consistent with earlier tests on young RBCs (19). The results were as follows:

- Hemolysis after 23-25 hours of RF energy exposure was < 0.3% for all TEST and CONTROL aRBC units and well within the ≤ 1% acceptance criterion.

- No notable changes were observed in red blood cell count, hemoglobin, hematocrit, mean cell volume (MCV), RBC morphology score, free hemoglobin, and potassium or percent hemolysis in the TEST versus CONTROL group.
- The maximum transient relative center temperature increase between TEST and CONTROL units of 0.77 ± 0.17 °C due to Joule heating. The highest peak recorded of 1.00 °C never exceeded the 1.5 °C criterion.
- Biological test results were within acceptance criteria and consistent with earlier tests on 6-9 day RBCs.
- There was no detectable acceleration in cellular degradation of aRBCs over young RBCs.

Similarly, the 3x3 sets of thawed FFP, FP24 and TP paired plasma units had comparable results between test and control bags, demonstrating that long-term RF exposure does not impact the coagulation factor levels of thawed plasma products (57). The results of the plasma testing were as follows:

- All three groups of plasma products (FFP, FP24, TP) with one exception met the FDA limit test acceptance criterion of<20% difference between TEST and CONTROL parameters assayed before and after RF exposure for Antithrombin

activity, Factors VIII and IX; PT and aPTT; Proteins C and S; Fibrinogen and VWF:RCo. (*There was a single exception in TP pair #1. For that pair, the CONTROL product VWF:RCo inexplicably dropped much lower than the TEST product. Since, however, the CONTROL sample had negligible RF exposure, the anomalous result is not likely due to any RF exposure process*).

- While Joule heating was present in the TEST bag, the average relative temperature increase between TEST and CONTROL units' centers was 1.36 ± 0.68 °C. The highest peak temperature recorded of 2.30 °C never exceeded the 4 °C criterion for plasma.

Overall, the results demonstrated that 13.56 MHz-based RFID technology is unlikely to have any significant temperature or biological effects on RBC and WBDP units under normal RFID operating conditions. More specifically:

- Both young RBCs and aRBC products do not have any increased cellular/protein degradation after high levels of extended exposure to RF energy. All results on aged RBCs were consistent with the earlier tests on young RBCs (57).

- WBDP products do not have any increased cellular/protein degradation after high levels of extended exposure to RF energy (19).

- All tested plasma products (FFP, FP24, TP) with one explainable exception met the FDA limit test acceptance criterion of<20% difference between TEST and CONTROL parameters assayed before and after RF exposure for all test coagulation factors.
- The RF field emitted by the Helmholtz coil had no significant effect on the temperature of RBC and WBDP blood products, and an acceptable effect on plasma products. The relative temperature increase of the exposed blood products did not exceed at any time their acceptance criteria.

Consequently, in review of the five hazards which could affect the safety and critical design requirements of ensuring there were no adverse effects of RFID technology on blood products, the methods demonstrated in the Limit Test Protocol and Results show that this will not likely occur during application of the technology. For these five hazards, the entity at risk of the RFID radiation hazard was the product or patient. Furthermore, all were given the same severity and likelihood measurements of two and one respectively, indicating that, even in the very unlikely incidence that the hazards will occur, they will only lead to minor, recoverable injury. Moreover, the results of the aforesaid method of control described in the Limit Test protocol can be applied to all.

The first hazard involves the event in which the maximum temperature increase of the RBCs and Platelets exceeds the acceptable levels of 1.5◦C. The results demonstrated that, for RBCs, the maximum average transient temperature increase of test versus control units due to Joule heating was 0.77 ± 0.17°C. There was no transient increase of greater than 1.00°C. For platelets, the maximum average transient temperature increase of test versus control units due to Joule heating was 0.30 ± 0.27◦C.

The second hazard was the potential of the cellular and protein structures of RBCs (complete blood counts including sample weight, RBC count, Hb, Hct, MCV; potassium, aluminum; free hemoglobin; level of blood gases) being degraded or altered beyond the acceptable level of ≤1% hemolysis. Test results demonstrated that, for young RBCs, Hemolysis was < 0.2% for both test and control RBC units. Additionally, for aRBCs, hemolysis was < 0.2% for both test and control RBC units.

The third potential hazard was the possibility of the cellular and protein structures (Lactate, Aluminum, P-Selectin, and complete blood counts including sample weight, WBDP count, Plt, and MPV) of WBDPs being degraded such that the pH decreases beyond the acceptable level of ≥6.2. The results of the Limit Test Protocol showed that the average pH of the test bags was 7.27. The average pH of the control bags was 7.19.

The next hazard involves the potential for the maximum temperature increase of plasma types (FFP, FP24, and TP) to exceed the acceptable level of 4 °C. The study showed that the maximum average transient temperature of the test vs. control bag was 1.36 ± 0.68 °C. Also, there was no transient temperature increase that exceeded 2.30 °C.

Finally, the last hazard in this group deals with the potential activity of coagulation factor (PT, aPTT, Antithrombin Activity, Factor V, Factor VIII, Factor XI, Protein C, Protein S, VWF: RCo) in all types (FFP, FP24, and TP) of thawed plasma products being altered beyond an acceptable level of 20%. The protocol results revealed that all three groups of plasma products (FFP, FP24, TP) with one exception met the FDA limit test acceptance criterion of <20% difference between test and control parameters assayed before and after RF exposure for PT, aPTT, Antithrombin activity, Factors V, VIII and IX; Proteins C and S; Fibrinogen and VWF:RCo. There was a single exception in TP pair #1. For that pair, in the control product VWF:RCo inexplicably dropped much lower than the test product. Since, however, the control sample had negligible RF exposure, the anomalous result was deemed unlikely to be due to any RF exposure process.

The Pre-Mitigation Risk of all five hazards in this category was determined to be at Level **A**. Level A is indicative of acceptable risk. This means that either the severity of the harm or the likelihood of occurrence of the event is so small the risk can be considered

negligible compared to the risks of other hazards. As a result, there is not a great need to reduce this risk.

TECHNOLOGY – SAFETY AND CRITICAL DESIGN REQUIREMENT: ENSURE THE PERFORMANCE CAPABILITY OF RFID TAGS DURING THE MOST COMMON BLOOD SUPPLY CHAIN PROCESSES

Similar to the hazards potentially impacting the previous safety and critical requirement of ensuring no adverse effects of RFID on blood products, the hazards which threaten this requirement of ensuring the performance capability of RFID tags during the most common blood supply chain processes were all tested under the same protocol. The Performance Test for RFID Tags in Blood Products Protocol was conducted.

In order to best understand the iTrace™ and the Performance Test for RFID Tags in Blood Products Protocol, it is important to be aware of the type of tag used, as well as the reason for why this particular tag was selected. Standard ISO/IEC 18000-3 mode 1 passive RFID tags, which are also compliant with the ISO 15693 standard, were selected for use at 13.56 MHz frequency. These tags were chosen for several reasons: 1) ISO 18000-3 is the international standard for passive RFID tags and describes the parameters, which are specifically optimized for healthcare applications, for use at 13.56 MHz, 2)

The tags are read/write capable, 3) The tags have the ability to store up to 3 kilobit of memory, some of which would be locked on the tag, and 4) The tags are unaffected by water and are able to withstand harsh environments. Avery Dennison AD-730 HF RFID tags with an operating temperature range of -40 to +85◦C were placed underneath the DIN barcode on the 0.9N saline filled blood bags. The tags operate using the 1 kilobit NXP|*Code SLI integrated circuit, consist of aluminum antenna external dimensions measuring 14x31 mm, and has an average free air resonance tuning of 14.0 MHz.

To determine the commercial applicability of the RFID system solution in the blood transfusion medicine industry, this protocol was designed to develop procedures and success criteria for evaluating the performance capability of RFID tags during the most common blood supply chain processes. The protocol used a defined set of performance measurement indicators. Tag performance was measured according to whether the tag/reader system performed satisfactorily when dealing with tag content in simulated scenarios including: different bag containers, varying types of readers, and packaging materials.

The UW RFID lab attached the RFID tags to simulated blood bags (actual blood bags filled with saline-based liquid content). The protocol considered all typical containers used for blood products at the BloodCenter of WI: Coleman cooler, tray, two generic

Styrofoam boxes, and platelet boxes. The performance of each tag was measured by reading the containers with four different RFID specified readers (tunnel reader, flatbed reader, dual barcode-HF handheld, and HF paddle reader). Acceptance thresholds were set for each test metric after analyzing the results from pre-testing and practicality considerations for real world application. Furthermore, the thresholds were established prior to fine tuning, thereby reflecting the worst case acceptable operation conditions.

The testing methodology for this protocol included 41 test scenarios and 23 separately analyzed experiments of container-reader combinations that have been documented by the BloodCenter of Wisconsin. The instances which involve reading all blocks with the handheld or the paddle were executed one blood bag at a time. The handheld devices cannot read more than one at a time since having multiple tags in the reading field creates reading problems for these readers. Therefore, the application will limit the use of these devices to reading one bag at a time.

The testing was designed to focus results in three primary areas of interest:

- Time to read (header) – Time in milliseconds to the point when the tag was seen for the first time after start of test,

- Time to read (memory blocks) – Time in milliseconds to read the predefined number of memory blocks from the tag memory, and
- Time to write (only done with single bag scenarios) – Time in milliseconds to the point when the tag acknowledges encoding completion; which includes reader header, reading the current data in the tag, erasing the tag by writing all zeros, writing a random pattern and finally verifying that the data was written correctly. All operations would be done to a predetermined number of blocks in the tag memory after start of test. If the written operation is not completed the trial is ignored and repeated.

The three potential hazards that may be experienced are as follows:

1. The time to read the headers of 20-bags-equivalent exceeds the maximum threshold established for specific container/reader combinations.
2. The time to read/write all memory blocks of 20-bags-equivalent exceeds the maximum threshold established for specific container/reader combinations.
3. The time to write all blocks exceeds the maximum threshold established for specific container/reader combinations.

The RFID Consortium is seeking to implement the RFID systems solution into commercial applications of the transfusion medicine industry. In doing so, a series of tests were planned to complement the standard software systems test. These included two phases of testing: tag survivability and tag performance testing. This portion of the document discusses the tag performance testing protocol execution and results. The survivability testing aspect will be discussed later.

The consortium developed this protocol based on the most common scenarios where RFID tags would be utilized in the blood supply chain. The goal was to evaluate as many aspects of the performance of RFID tags as possible in order to determine its full potential. The method was to combine the four different types of readers: (1) TagSys HF RFID Tunnel, (2) TagSys HF RFID Flatbed, (3) Unitech handheld, and (4) Tracient PadL with all of the traditional containers used for blood products at the BloodCenter of Wisconsin – Coleman cooler, tray, two generic Styrofoam boxes and platelet boxes – in varying groupings to determine the efficacy. The different combinations were applied at each of the RFID-enabled checkpoints in the blood supply chain process.

The UW RFID lab used a factorial design to formulate a total of 41 test scenarios. The combination of scenarios generated 23 experiments. The factors or variables that were manipulated during each experiment were the amount of data processed and the number

of units in the container. There were also two test levels for each variable: the two extreme values for the number of bags and the number of memory blocks. For the number of bags variable, the 60 bags were randomly grouped into the corresponding number of bags per container and tests were run until all 60 bags were read in each scenario.

The testing team worked closely with the software developer (S3Edge) and the tunnel manufacturer (TagSys) to ensure the tunnel configuration was appropriately attuned for the test purpose. Since tags were read individually using the handheld and paddle reader, it was found that the packaging type did not matter and the only variable that had an effect was the number of tagged units. The units were tested in groups of 2, 4, 10, 17, and 30, and the only difference was the absence of the container.

Using two level factor analysis on preliminary data collected on the variables' effect between the different levels, it was estimated that a minimum of 60 test units was required as a sample size to ensure 95% confidence of results applying two replications per run.

The acceptance thresholds were set for each test metric after analyzing results from pre-testing the most difficult scenarios of the blood supply chain. The time to read/write was taken as the average value of all data obtained for the scenario. If the average time to read

or write exceeded the threshold by a statistically significant amount at $\alpha=0.05$, the test failed.

All measurements were converted to 20-bags-equivalent and compared with its corresponding 20-bags-equivalent threshold.

The results of this protocol show that RFID tags demonstrate acceptable levels of performance in all scenarios of real world application. More specifically, the results were as follows:

- All scenarios passed the statistical t-test with a confidence level of 95% when compared to the pre-determined threshold.
- Some scenarios, such as the tray with the flatbed were dependent upon the operator because the flatbed reader only used a single antenna that had dimensions smaller than the length of the tray.
- The system can be fine-tuned to improve performance over the results obtained through this study.
- The handheld and paddle reader need to have exactly one tag in the reading field, making it difficult to read all blocks within packaged containers where there is

interference from neighboring tags – each bag must be read individually with these devices.

- When reading headers with handheld and paddle readers, the type of packaging did not significantly affect the performance.

Thus, all scenarios passed the performance thresholds that were set based on actual pre-test data and practicality considerations for real-world applications. The tunnel reader was found to perform the best with the fastest read times in its applicable scenarios. Next was the flatbed, then handheld, and the last was the paddle reader. Other tests showed that the paddle antenna had the highest Q, thereby reducing its sensitivity to RFID tags which are detuned form the 13.56 MHz reader interrogation frequency. Consequently, this increased the number of retries needed to read these tags and boosted the average reading time.

Additionally, when using the handheld and paddle readers, bags had to be read individually. As a result, the performance of the system in some of these scenarios depended on the user's ability to properly employ the device and the software user interface.

Furthermore, when comparing the time to read barcodes on individual bags with the results obtained from the RFID tags, a marked improvement in performance is shown. The improvement can be highlighted by the read time for the tunnel where one can read at a rate of less than a second per bag without having to open or unpack the container. This compares with approximately 0.5-1 minute per tag for unpacking and reading the barcodes on each bag individually, depending on the operator's skill level, as measured by the check-in process in other studies. RFID considerably improves the time it would take to read barcodes from each bag, serving as a major source of return on investment in the blood center.

Even with the poorest performing reader, the paddle reader, it is possible to read a tag every 2 seconds. Moreover, through additional fine-tuning of the tunnel reader's parameters, the possibility of greater performance improvement is feasible. This enhancement will take place in tandem with the fine-tuning of the final user application development.

As a result, the evaluation of the three hazards which could affect the safety and critical design requirement of ensuring performance capability of RFID tags during the most common blood supply chain processes could be attributed to the Performance Test Protocol and Results. For these three hazards, the entity at risk of the RFID hazard is the

system itself. In addition, the hazards are all caused by system capability. Furthermore, all were given the same severity and likelihood measurements of one and two respectively. This means that, even in the remote chance that the hazards will occur, they will only lead to negligible injury. What is more, the results of the abovementioned mitigation strategy for the Performance Testing Protocol can be applied to all three hazards for their methods of control.

The first hazard refers to the potential scenario in which the time to read headers of 20-bags-equivalent exceeds maximum threshold established for specific container/reader combinations. The results of the Performance Test Protocol demonstrated the following:

Tunnel Reader:

1. Maximum threshold = 15-25 seconds for the 20-bags-equivalent, depending on container.
2. Maximum average time to read only headers was 6.19 seconds.
3. Mean time to read the header of any one tag was 0.26 seconds.

Flatbed Reader:

1. Maximum threshold = 20-40 seconds for the 20-bags-equivalent, depending on container.
2. Maximum average time to read only headers was 23.7 seconds.
3. Mean time to read the header of any one tag was 0.87 seconds.

Handheld Reader:

1. Maximum threshold = 35-45 seconds for the 20-bags-equivalent, depending on container.
2. Maximum average time to read only headers was 37.7 seconds.
3. Mean time to read the header of any one tag was 1.27 seconds.

Paddle Reader:

1. Maximum threshold = 70, 75, & 80 seconds for the 20-bags-equivalent, depending on container.
2. Maximum average time to read only headers was 68.9 seconds.
3. Mean time to read the header of any one tag was 1.95 seconds.

The second hazard deals with the possibility in which the time to read/write all 28 memory blocks of 20-bags-equivalent exceeds maximum threshold established for specific container/reader combinations. The results of the Performance Test Protocol were as follows:

Tunnel Reader:

1. Maximum threshold = 25-40 seconds for the 20-bags-equivalent, depending on the container.
2. Maximum average time to read all blocks was 26.5 seconds.
3. Mean time to read all blocks on any one tag was 0.89 seconds.

Flatbed Reader:

1. Maximum threshold = 30, 50, & 60 seconds for the 20-bags-equivalent, depending on the container.
2. Maximum average time to read all blocks was 45.6 seconds.
3. Mean time to read all blocks on any one tag was 1.23 seconds.

Handheld Reader:

1. Maximum threshold =80 & 60 seconds for the 20-bags-equivalent, depending on the container.
2. Maximum average time to read all blocks was 25.0 seconds.
3. Mean time to read all blocks on any one tag was 1.27 seconds.

Paddle Reader:

1. Maximum threshold =130, 140, & 150 seconds for the 20-bags-equivalent, depending on the container.
2. Maximum average time to read all blocks was 102.4 seconds.
3. Mean time to read all blocks on any one tag was 4.4 seconds.

The third and final hazard of this category involves the potential situation in which the time to write all blocks exceeds the maximum threshold established for specific container/reader combinations. The protocol test results showed the following:

Flatbed Reader (Write): Tag read and written twice:

1. Maximum threshold =70 seconds.
2. Mean time to write one tag was 50.7 seconds.

Handheld Reader: Tag read and written twice:

1. Maximum threshold = 130 seconds.

2. Mean to write one tag was 120.5 seconds.

All three of the hazards described in this section received a Pre-Mitigation Risk Level of **A**. Again, a level of A indicates acceptable risk. It denotes that there is not necessarily a need to reduce the risk.

TECHNOLOGY – SAFETY AND CRITICAL DESIGN REQUIREMENT: ENSURE RFID TAG SURVIVABILITY AFTER EXPERIENCING THE MOST DEMANDING CONDITIONS IN THE BLOOD SUPPLY CHAIN

There are several hazards that could impact the safety and critical design requirement of ensuring the RFID tag survivability after experiencing the most demanding conditions in the blood supply chain. In order to investigate these hazards, a formal protocol study entitled “RFID Tag Survivability Testing Protocols: Centrifugation, Blast Freezing, and Gamma Irradiation” was conducted. As the RFID Consortium is seeking to implement the RFID systems solution into commercial applications of the transfusion medicine industry, this protocol represented the survivability portion of a series of tests that were designed to complement the standard software systems test.

The general objective of this protocol was to evaluate RFID tag survivability and changes in functional performance as a result of exposure to the effects of centrifugation, blast freezing, and gamma irradiation. Whereas centrifugation and blast freezing generally take place during processing at the blood center, gamma irradiation may be performed in either the blood center and/or prior to transfusion in the hospital. The studies were designed to simulate operational conditions equivalent to those a regular blood product would normally undergo since the solution will be commercialized in the transfusion medicine industry. Basic scenarios were devised to observe the behavior of the functional RFID tags before and after the simulated units experienced the demanding conditions. The survivability tests were intended to serve as a complement to the standard systems software test.

The first condition measured was centrifugation. The objective of the centrifugation protocol was to test the applicability of the use of RFID technology in the transfusion medicine supply chain. It was performed in order to evaluate the RFID tag survivability and resiliency when exposed to the effects of centrifugation under high levels of exposure conditions (higher number of processes than typically expected with three centrifugation cycles approximately 10 minutes long at a speed of 4,200 RPM (4750g), rather than the expected maximum of two centrifugation cycles for approximately 10 minutes in duration at a speed of 4,200 RPM (4750g). The duration and speed of the centrifugation

cycles were consistent with the maximum values normally used in standard manufacturing processes. Sixty operable RFID tags were sampled testing their post-test operability at each distance of 0cm, 5cm, and 10cm. The tags were tested for read/no read and write/no write capabilities, as well as the time to read (header), time to read (all blocks), time to write, and data integrity. The RFID Blood Center Consortium developed and undertook this testing regimen to ensure that the proper methods of control for mitigating the potential hazards were established.

The potential hazards that could result from centrifugation were the following:

1. RFID tag may not survive the exposure to centrifugation process. Evidence of survivability should be proven by complying with the acceptable performance criteria laid out by the other potential hazards described below.

2. Increased exposure to centrifugation processes may decrease the ability of the RFID tag to read tag data within 30 seconds of the start.

3. Increased exposure to centrifugation processes may decrease the ability of the RFID tag to write information within 30 seconds of the start.

4. Increased exposure to centrifugation processes may increase the time it takes to read the tag after it was seen for the first time (header) by greater than 20 seconds.

5. Increased exposure to centrifugation processes may increase the time it takes to read all blocks of tag memory by greater than 45 seconds.

6. Increased exposure to centrifugation processes may increase the time it takes to write information after the tag acknowledges encoding completion of all blocks by greater than 75 seconds.

The next condition investigated was blast freezing. The objective of the blast freezing protocol was to determine the applicability of using RFID technology in the transfusion medicine supply chain. It was performed in order to evaluate RFID tag survivability and resiliency when exposed to the effects of blast freezing under high levels of exposure conditions. Sixty operable RFID tags were sampled testing their post-test operability at each distance of 0cm, 5cm, and 10cm. The tags were tested for read/no read and write/no write capabilities, as well as the time to read (header), time to read (all blocks), time to write, and data integrity. The tags were affixed to plasma bags and subjected to blast freezing for approximately 50 minutes, and then placed in a walk-in freezer set to -30°C. After being stored in a frozen state for about 72 hours, the bags were thawed in a water bath using standard plasma thawing procedure. The RFID Blood Center Consortium developed and undertook this testing regimen to ensure that the proper methods of control for mitigating the potential hazards were established.

The potential hazards that could result from blast freezing include the following:

1. RFID tag may not survive the exposure to blast freezing techniques. Evidence of survivability should be proven by complying with the acceptable performance criteria laid out by the other potential hazards described below.

2. Exposure to blast freezing techniques may decrease the ability of the RFID tag to read tag data within 30 seconds of the start.

3. Increased exposure to blast freezing techniques may decrease the ability of the RFID tag to write information within 30 seconds of the start.

4. Exposure to blast freezing techniques may increase the time it takes to read the tag after it was seen for the first time (header) by greater than 20 seconds.

5. Exposure to blast freezing techniques may increase the time it takes to read all blocks of tag memory by greater than 45 seconds.

6. Exposure to blast freezing techniques may increase the time it takes to write information after the tag acknowledges encoding completion of all blocks by greater than 75 seconds.

7. Exposure to blast freezing techniques may affect the integrity of the written data.

The final condition examined under this protocol was gamma irradiation. The objective of this study was to determine the applicability of the use of RFID technology in the transfusion medicine supply chain. It was performed in order to evaluate the RFID tag survivability and resiliency when exposed to the worst-case effects of gamma irradiation under high levels of exposure conditions. Sixty operable RFID tags were sampled testing their post-test operability at each distance of 0cm, 5cm, and 10cm. The tags were tested for read/no read and write/no write capabilities, as well as the time to read (header), time to read (all blocks), time to write, and data integrity. The tags were affixed to blood product bags and subjected to a higher number of process cycles of Cs^{137} gamma irradiation than normal. In standard manufacturing processes, exposure to gamma irradiation will be limited to a total of approximately 3.8 minutes to reach the desired dose of 25 Gy. Under typical circumstances, an RFID tag is expected to be exposed to a maximum of two gamma irradiation cycles. The test units in the study were exposed to that maximum level of two 25 Gy doses of gamma irradiation exposure. The RFID Blood Center Consortium developed and undertook this testing regimen to ensure that the proper methods of control for mitigating the potential hazards were established.

The potential hazards associated with blast freezing include:

1. RFID tag may not survive the exposure to gamma irradiation processes. Evidence of survivability should be proven by complying with the acceptable performance criteria laid out by the other potential hazards described below.

2. Increased exposure to gamma irradiation processes may decrease the ability of the RFID tag to read tag data within 30 seconds of the start.

3. Increased exposure to gamma irradiation processes may decrease the ability of the RFID tag to write information within 30 seconds of the start.

4. Increased exposure to gamma irradiation processes may increase the time it takes to read the tag after it was seen for the first time (header) by greater than 20 seconds.

5. Increased exposure to gamma irradiation processes may increase the time it takes to read all blocks of tag memory by greater than 45 seconds.

6. Increased exposure to gamma irradiation processes may increase the time it takes to write information after the tag acknowledges encoding completion of all blocks by greater than 75 seconds.

7. Increased exposure to gamma irradiation processes may decrease the integrity of the written data.

Thus, although the harsh conditions may differ (i.e. centrifugation, blast freezing, gamma irradiation), the hazards that may ensue from exposure to these conditions are the same.

The testing methodology for these protocols included a simulation of operational conditions equivalent to those to which a regular blood product would be subjected under normal operating conditions. The basic scenarios were designed to observe RFID tag behavior before and after the simulated units underwent the demanding operational conditions of centrifugation, blast freezing, and gamma irradiation.

A total of 180 RFID tags were sampled. Prior to affixing the tags to the test units, each sample tag was validated to ensure only operable tags were tested. Different test parameters were measured for each tag before and after each survivability scenario, and were collected at three different distances from the reader antenna – 0cm, 5cm, and 10cm. The parameters measured included read success, write success, as well as time to read, time to write, data integrity, read rate, and signal strength.

The mitigation strategy followed for all of these hazards were related to the tags. The RFID tags used for the RFID Blood Center Solution are compliant with the ISO 15693 and ISO 18000-3 standards, and are specifically optimized for healthcare applications. Durable Avery Dennison AD-730 HF RFID tags were used and placed underneath the DIN barcode.

The risk mitigation strategy is three fold:

1. RFID tag suppliers will be required to certify the readability of tags supplied by implementing internal controls to statistically sample production batches and eliminating defective tags prior to shipping tags to the blood center. The blood centers should establish a procedure to periodically verify the certification levels established in the purchasing contract.

2. In case of an eventual tag failure, the operator must follow the general procedure established for proceeding when an inoperable tag is detected in any blood center process: The unit must be clearly identified as a "BAR CODE ONLY" unit and all subsequent operations with such unit must be performed thru the back up operating procedures (barcode scanning).

3. Failed tags will be reported documenting the potential cause for failure (when apparent). If failure rates surpasses the threshold established by the quality control department, a joint investigation with the manufacturer will be conducted to establish root causes.

The resulting performance levels observed for all of the survivability tests – centrifugation, blast freezing, and gamma irradiation – at least 92% of the tags survived with 95% confidence.

- Centrifugation secondary analyses: There was a statistically significant increase in time to read/write and read rate performance mainly after the third centrifugation cycle. Some degradation was expected because the tags were exposed to the high levels of centrifugation (4750g) conditions twice in succession. However, despite the statistically significant difference, the resulting performance level observed was well within the acceptable operational ranges expected for a normal tag.

- Blast freezing secondary analyses: There was no significant degradation in read rate or signal strength observed after the freezing and thawing cycles (Note that the tags rated operating temperature range is -40 to +85°C). Statistically significant degradation was observed for mean time to read and write all blocks mainly after thawing. However, despite the statistically significant difference, the resulting performance level observed is well within the acceptable operational ranges expected for a normal tag.

- Gamma irradiation secondary analyses: There was no significant degradation in read rate observed. However, there was a significant downward trend in signal

> strength when measured at 10cm distance after each irradiation cycle. Signal strength was not a hazard in itself but one of the measurements used to explain poor performance. In all cases except the time to read all blocks, there was not a statistically significant deterioration in tag functionality. The resulting performance levels observed were well within the acceptable operational ranges expected for a normal tag.

Overall, although there was some degradation in tag functionality after the last exposure cycles, the degree of degradation observed was not considered critical in practical terms as the post-test measurements were still deemed appropriate for acceptable tag operating performance.

The seven hazards which could impact the survivability of the RFID Tag subsequent to experiencing the most demanding conditions in the blood supply chain were all tested in the above Survivability Testing Protocol. All seven hazards are RFID-based, and they may affect the ability of the system to perform as desired. Additionally, the same method of control may be applied for all. This mitigation strategy is based on the tag itself. The durable Avery Dennison AD-730 HF RFID tags, which are compliant with the ISO 15693 and ISO 18000-3 standards and specifically optimized for healthcare applications, were used and placed underneath the DIN barcode.

Survivability tests were conducted in which tags were exposed to higher numbers of process cycles of centrifugation, blast freezing, or gamma irradiation than those regularly applied during normal operations. After the tests, the tags behaved within acceptable performance levels.

RFID tag suppliers will be required to certify the readability of tags supplied by implementing internal controls to statistically sample production batches and eliminating defective tags prior to shipping tags to the blood center. The blood centers should establish a procedure to periodically verify the certification levels established in the purchasing contract.

In case of an eventual tag failure, the operator must follow the general procedure established for when an inoperable tag is detected in any blood center process: The unit must be clearly identified as a “BAR CODE ONLY” unit and all subsequent operations with such unit must be performed following back up operating procedures (barcode scanning).

Failed tags will be reported by documenting the potential cause for failure. If failure rates surpass the threshold established, a joint investigation with the manufacturer will be conducted to establish root causes.

Furthermore, with the exception of the first hazard, which was given a severity and likelihood score of three and two respectively, the remaining hazards were given severity and likelihood scores of two and two respectively. The first hazard described the general risk that the tag failed to survive the process. Understandably, it is essential for the tag to maintain functionality throughout the entire process in order to achieve the objectives of the iTrace™. The severity rating illustrated the remote chance that moderate damage or loss of function could occur.

Thus far in the analysis, this hazard has presented the greatest risk. While the Pre-Mitigation Risk was still a **B**, the risk range was near the unacceptable region. Consequently, even though this hazard could be mitigated and the severity reduced, it may involve high cost expenditure.

The remaining hazards all had severity and likelihood levels of two and two, but they all presented a Pre-Mitigation Risk of **B**. Although they had the same rating as the previous hazard, these hazards all fell within the middle of the tolerable risk range. Therefore, the cost expenditure or efforts that must be taken to mitigate the hazard were lower for these hazards than the former.

The list of remaining hazards that fell in this category included:

- The ability of the RFID tag to read data within 30 seconds of the start is damaged.
- The ability of the RFID tag to write information within 30 seconds of the start is damaged.
- The time it takes to read the tag after it was seen for the first time (header) increases greater than 20 seconds.
- The time it takes to read all blocks of tag memory increases by more than 45 seconds.
- The time it takes to write information after the tag acknowledges encoding completion of all blocks increases by greater than 75 seconds.
- The integrity of the written data is compromised.

TECHNOLOGY – SAFETY CRITICAL DESIGN REQUIRMENT: ENSURE NO INTEREFERENCE OF RFID HIGH FREQUENCY (HF) AND ELECTROMAGNETIC INTERFERENCE (EMI) WITH OTHER SYSTEMS

There were 11 potential hazards identified that could impact the safety critical design requirement to ensure no interference of RFID High (HF) and electromagnetic interference (EMI) with other systems. Like the previous technology hazards described, these hazards were all tested through the use of a formal protocol. The protocol was

entitled: “Wireless Considerations Test – HF RFID Application in Blood Centers Wireless Considerations.”

The objective of this protocol was to outline testing methods and success criteria for evaluating the potential effects of electromagnetic interference (EMI) on existing medical equipment and systems, as well on and between High Frequency (HF) RFID entities. The RFID Consortium developed and undertook this systematic and repeatable protocol testing regimen based on the recommendation of the American National Standards Institute (ANSI) to ensure that the proper methods of control for mitigating the potential hazards were established.

There were four main goals of the study:

1. Identify potential electromagnetic interference (EMI) effects from High Frequency (HF)-based RFID systems on existing medical equipment found in donation and processing centers.

2. Identify potential EMI effects of HF RFID equipment on existing wireless devices and systems found in donation and processing centers.

3. Identify any potential for erroneous and/or incomplete communication between HF RFID entities (e.g. between tag and reader or between reader and server) due to EMI from other devices.

4. Suggest proactive measures to minimize or eliminate EMI effects.

A major prerequisite to understanding the possible effects that high frequency and electromagnetic energy from the iTrace™ could have on interfacing and communications transmission was learning how the iTrace™ itself operates. The implementation of the RFID blood center solution iTrace™ consists of RFID devices securely interfacing through servers to the Blood Establishment Computing System (BECS). The servers run the application iTrace™ that is built on a middleware developed by S3Edge that is based on the Microsoft BizTalk RFID platform.

Wireless considerations for interfacing and communication transmissions were taken into account for the iTrace™. The two types of wireless technologies that were applicable to this project were High Frequency (HF) RFID and Wi-Fi. HF RFID operating at 13.56 MHz is the recommended technology for use in the blood supply chain under the ISBT Guidelines. It utilizes near-field magnetic induction coupling and the electric field is suppressed. The tag types – ISO/IEC 18000-3 mode 1 and downward compatible ISO/IEC 15693 – use the ISO/IEC 15693 wireless communications protocol. Wi-Fi,

which is already used in blood centers and at mobile donation sites, consists of technologies using wireless local area network (WLAN) based on the IEEE 802.11 family of standards, device to device wireless connectivity. The coverage of one or more interconnected access points (hotspots) comprises an area the size of a few rooms depending on the number of access points with overlapping coverage. Both wired Ethernet LAN-based RFID readers and wireless battery-operated RFID readers interface to the iTrace^{TM} server over the existing T-100 LAN, 802.11b/g wireless LANs.

Prior research has shown that RFID systems, because of their wireless communication transmitters, may have the potential to both generate and fall victim to electromagnetic interference (EMI). In order for successful adoption and deployment of RFID technology in blood centers, key areas of concern such as quality of service, data corruption, security, and electromagnetic compatibility must be properly addressed, examined, and approved.

The testing methodology for this protocol included three sub-protocols. The first was the *HF Electromagnetic Compatibility (EMC) Test Protocol (Protocol ID 1).* For this protocol, medical devices at the blood center were set up to operate in normal working conditions with relevant measurements taken from each device and compared against the expected range of values. Operations of the RFID system were also monitored to assess successful completion of blood center software transactions. Two types of outcomes were

used in a binary pass/fail measurement – normal (i.e. no deviation from the expected range of operating values) and abnormal (i.e. deviation from outside the normal expected range of operating values). The acceptance criteria for this sub-protocol were as follows:

- Blood center routine must be successfully completed in all the test locations. Failure is indicated by the following situations: 1) The reader is unable to complete the operation and/or emit error beeps, and 2) The routine is completed but the data in the server database has some mismatch with what is expected or is corrupted.

- No medical device should show abnormal measurement pre-, in-, or post-test.

The second sub-protocol was the *Wi-Fi EMI/EMC Test Protocol (Protocol ID 2).* The goal of this test was to verify the wireless functioning of the Unitech RFID handheld reader, as well as multiple medical and blood product handling and processing devices. The acceptance criteria for this sub-protocol were as follows:

- The fraction of packets lost when running a ping command from the handheld must not exceed 10% in any location.

- The blood center software routine must be successfully completed in all the test locations within the protocol. Transaction failure was indicated by the following

situations: 1) an error message appeared on the handheld indicating that the process was terminated prematurely for any reason whatsoever, and 2) the routine was completed but the data in the backend database had some mismatch with what was expected or was corrupted.

- No medical device should show abnormal measurements pre-, in-, or post-test.

The third sub-protocol was the *Failure Recovery Test Protocol (Protocol ID 3).* This protocol was designed to examine the behavior of the RFID blood center solution in the event of a sudden failure in Wi-Fi signal connectivity and to analyze the recovery mechanisms of the system. The acceptance criteria here were as follows:

- There should be a clear indication on the device itself that informs the user about an interruption in wireless connectivity.
- The handheld should clearly indicate that the transaction must be repeated in the instance of a failed attempt to store information to the central database field.
- The central database should not contain erroneous or misleading information about the intermittently stopped transaction. It should notify the user of an incomplete entry.

- The handheld should complete the transaction when the wireless connection is resumed.
- If applicable, entries created in the database after completion of the handheld routine should match up with the information on the RFID tag.

Finally, the HF RFID tag write failure recovery application was examined. The purpose was to perform a write-read-verify cycle to confirm proper tag commissioning. If an error was indicated during the process, the solution used a configurable number of automatic retries to ensure the tag was correctly commissioned. The acceptance criteria here was an assessment of functionality, examining whether the software first detected a verified write, then a failed write, then another verified write to demonstrate the capability of the automatic retry.

The potential hazards investigated under this protocol and sub-protocols included the following:

1. Electromagnetic interference (EMI) effects could cause connections to be lost without warning.
2. EMI effects could cause a failure to establish connections.
3. EMI effects could lead to degradation of service.

4. EMI effects could produce delays and packet loss in the transmission of information to and from a handheld reader or a netbook/laptop.
5. EMI effects could negatively impact the wireless transmission of critical medical device alarms.
6. EMI effects could impede the transmission of physiological waveform data.
7. EMI effects could prevent the real-time control of therapeutic medical devices.
8. EMI effects could hinder the transmission of time-critical medical telemetry.
9. EMI effects could obstruct the wireless control of therapeutic devices.
10. EMI effects could lead to data corruption and/or errors.
11. Communication between the transmitter and receiver could lead to unauthorized access.

The mitigation strategy applied for these hazards was extensive. Several considerations were taken into account in the creation of the RFID blood center solution application. The first was RFID interference with wireless devices. This posed minimal concern because, aside from the extensive frequency separation between 13.56 MHz RFID and 2.4 GHz for wireless communication that enables excellent signal filtering, the signal

propagation characteristics of RFID make interference with wireless communications unlikely.

Next, the near-field magnetic propagation of the application reduced the potential for electromagnetic interference in all but the closest objects. The RFID reader operated at 13.56 MHz and 22m wavelength with the electric field suppressed. Additionally, the magnetic field strength was largely limited to the antenna and the propagated field strength was inversely proportional to the cube of the distance from the antenna. Although the maximum operational range varied by reader power and antenna size, this generally remained less than 50cm. Consequentially, the magnetic field strength at $\lambda/2$ = 11m made far field electromagnetic propagation essentially non-existent.

Furthermore, the 2.4 GHz wireless antennas of the application lacked a metallic loop-shaped device. This structure eliminates the possibility of EMI because the RFID magnetic field in the air cannot be induced without a complete loop.

In general, EMI may be avoided in three ways: suppressing the source, breaking the interference path, or shielding the device at risk. The potential hazards depended on the severity of the EMI, which was determined by the power of both the electromagnetic leakage and channels. The two general guidelines applicable to reduction in all types of EMI are diminishing electromagnetic leakage and suppressing electromagnetic channels.

Electromagnetic radiation leakage is a consequence of most electronic devices operating with digital signals that have sharp temporal transitions. As a result, these devices serve as sources for EMI. As performance requirements increase, the speed of digital signals and the strength of radiation and leakage increase. Higher electromagnetic output power boosts the risk for EMI. Agencies such as the FCC regulate the amount of radiated and leaked electromagnetic power. EMI can be reduced by modifying the internal circuit design of the device. Two of the most commonly used methods to achieve this are the filtering and the spread spectrum techniques. The filtering technique blocks the frequency bands while the spread spectrum technique spreads the energy over a wider frequency range. With proper design following these principles, electromagnetic leakage from devices can be greatly reduced. Nevertheless, the operational frequency bands of HF RFID readers and Wi-Fi devices are restricted to specific regions of the electromagnetic spectrum, and most medical devices fail to generate electromagnetic fields at these frequencies.

The next guideline, suppressing electromagnetic channels, consisted of three different types of electromagnetic channels that warrant consideration: electro-coupling, magnetic-coupling, and electromagnetic radiation. Among them, magnetic-coupling may play a primary role in producing EMI between HF RFID readers and medical devices. Yet, electromagnetic radiation is the dominating factor of the EMI in Wi-Fi devices. For HF

RFID readers, suppressing the magnetic-coupling between devices can be implemented by providing electromagnetic shielding or pulling devices away from potential sources of EMI. Electromagnetic shielding blocks electromagnetic fields and is typically achieved by surrounding the susceptible device with a good conductor such as a metal film or foil cover.

Another strategy was to pull HF RFID readers away from all medical devices as much as possible to significantly lessen electromagnetic channels which are constrained to within a few centimeters of the HF RFID antennas. The strength of the channels drops dramatically with distance. Most HF RFID readers that operate as per FCC regulations for maximum power have magnetic fields spreading less than 20 cm from the antenna.

Electromagnetic shielding or spreading the distance between devices are valid measures for Wi-Fi as well. Even a thin sheet of metal is sufficient to provide significant electromagnetic shielding. As well, increasing distances between medical devices and Wi-Fi devices can reduce the efficiency of the channels since the radiation energy density is inversely proportional to the square of the distance.

Furthermore, there are two EMI-related hazard mitigation strategies that blood centers and hospitals may need to implement. The first is to incorporate EMI test requirements into the new medical device/equipment sourcing policy. Device sourcing involves several

practices which are geared towards finding, evaluating, and engaging suppliers of goods and services. The first EMI-test related step entails defining the specific electromagnetic frequencies and wireless communication protocols utilized in blood centers and hospitals. This will facilitate effective communication and reduce damaging interference between devices. The next EMI-test related step is to communicate those specifications in Request for Proposal (RFP) and Request for Quotation (RFQ) documents that are customized to particular use cases in order to record business requirements for and competitively price potential solutions. The final step in the sourcing strategy is to ensure that manufacturers provide evidence of EMI shielding specifications or methodology and testing of their products to confirm the safety of their use.

The second strategy is to incorporate EMI test requirements into the procurement of new medical device/equipment or existing medical device/equipment upgrades policy. For implementing this policy, it is necessary to first define the appropriate EMI test protocols applicable for the device in question. It is also essential to consider the operating environment where the device will be employed. This will enable a comprehensive analysis of the effects of utilizing the device. The policy should then require the performance and documentation of the applicable EMI testing protocol prior to installing the device.

The results of the testing showed that all hazards successfully passed acceptance criteria, and that EMI and wireless communication issues will only be minor risks in the implementation of the iTrace™.

The 11 hazards tested with this protocol were all RFID hazards caused by EMI/Wireless communication and were capable of impacting the system. Two of the hazards: 1) Connections/communication links are lost without warning and, 2) Degradation of service/ transmission of information share the same method of control. The method of control involved the HF RFID 13.56 MHz radio communication protocols as dictated by the ISO/IEC 15693 standard, as well as the ISO/IEC 18000-3 mode 1 standard, which are used in the RFID readers for this application. The 16-bit cyclic redundancy check (CCITT CRC-16) is run on the message bits right from the start of the flags to the end of data and the CRC-16 accompanies the message as it is sent. This is used for communication both from the reader to the tag as well as from the tag to the reader, and is capable of detecting 99.998% of all possible bit errors. When an error is detected, a complete bit sequence must be retransmitted. Furthermore, the CCITT 16-bit CRC on the data stored in the tag memory serves as a second layer of protection against the remaining 0.002% cases of bit stream corruption not caught by the original transmission CRC.

Another hazard in this category was the possibility that the systems will experience a failure to establish communication. Here, the strategy was to revert to the current standard. The key information for safe transfusion is carried in ISBT-128 barcodes, as well as in human readable form, on the bag itself. In the event of any communication failure of the RFID system, bar code data will be used.

The next five hazards utilize the same method of control. The hazards which comprise this group are the following:

1. The wireless transmission of critical medical device alarms is disabled.
2. The transmission of physiological waveform data is impeded.
3. The real-time control of therapeutic medical devices is prevented.
4. The transmission of time-critical medical telemetry is hindered.
5. The wireless control of therapeutic devices is obstructed.

The method of control was reflective of the strategies as previously described for this protocol. All wireless communication and EMI interference tests in this protocol successfully passed acceptance criteria for the existing key devices operating in the Blood Center. EMI and wireless communications issues will involve minor risks in the implementation of the RFID blood center solution.

There are two steps for effective control for preventing these hazards from occurring for future acquisition or upgrading of key equipment. The first is at the new medical device/equipment sourcing stage. The EMI study protocol described above defined the specific electromagnetic frequencies and wireless communication protocols utilized in blood centers. The specifications were documented and tested. These specifications are to be used as templates for defining EMI-related specification for new/upgraded equipment

The second step is at the procurement of new or upgrading of existing medical device/equipment stage. Here, the appropriate EMI test protocols applicable for this device will be executed. The test results will be documented.

Going a step further than the general practice described with the former hazards, the method of control for the next hazard – delays and packet loss in the transmission of information to and from a handheld reader or a netbook/laptop – took into account formal standards useful for WLAN communication. The WLAN communication used for the iTrace^{TM} adhered to the IEEE 802.11b and 802.11g standards which define one Medium Access Control (MAC) layer and multiple physical layers (PHY). Various error detection and corrections steps were employed at both layers including Reed-Solomon codes (that can detect up to 8 byte errors) and 32-bit CRC that can detect more errors than a 16-bit

CRC in ISO 15693. The error detection and correction steps were achieved by appending a frame check sequence (FCS) at the end of each packet.

All of the nine aforementioned hazards in this category were rated at a level two severity and a level one likelihood. That means that these hazards all represented improbable instances which would only lead to minor loss of function or impairment if they did actually come to pass. As such, they were all assigned a Pre-Mitigation Risk Level **A**. They were all acceptable risks that can be disregarded in comparison to other risks.

However, the remaining two risks which threaten the fulfillment of the safety critical design requirement to ensure no interference of RFID HF and EMI with other systems both received severity and likelihood scores of three and one respectively. This moderate severity in conjunction with an improbable likelihood resulted in a Pre-Mitigation Risk of **B**. These risks were considered tolerable, yet the effort to mitigate the hazards may be greater.

One of these hazards – data corruption and/or errors are produced – utilized the combined mitigation strategies of a few of those described above. The HF RFID 13.56 MHz radio communication protocols as dictated by the ISO/IEC 15693 standard, the ISO/IEC 18000-3 mode 1 standard, the 16-bit cyclic redundancy check (CCITT CRC-16), the tag data encoding procedure, and the WLAN communication error detection and correction

(i.e. IEEE 802.11b and 802.11g) standards demonstrated a comprehensive mitigation and correction strategy for preventing and rectifying this hazard.

The second of these hazards was the event in which unauthorized access during the communication between the transmitter and receiver transpired. The method of control engaged formal guidelines concerning access, encryption, and data manipulation security. There were particular provisions in the air protocols and standards that made it difficult to inappropriately access data while the transmitter and receiver were communicating.

Furthermore, the RFID reader operates at 13.56 MHz and 22m wavelength with the electric field suppressed. Additionally, although the maximum operational range varied by reader power and antenna size, this generally remained less than 50cm. Because the communications range is limited to within a few centimeters around the RF tag and reader, it is almost impossible for an unauthorized individual to access or steal information. Also, the tag structure design included data bits stored on the tag with an associated CCITT 16-bit CRC stored in the tag memory to ensure data integrity and making malicious alteration difficult.

Moreover, the key information for safe transfusion is carried in ISBT-128 barcodes and human readable form on the bag itself. The application does not and will not involve storage or transmission of confidential medical data, and all key information. Finally, the

wireless network included data encryption security that prevented hackers from connecting to protected networks and stealing information. The application utilizes the WPA2 AES security key as well as wireless intrusion prevention systems as an added layer of security.

CHAPTER 5: IMPLEMENTATION HAZARD ANALYSIS

SysLogic, Inc. maintains a list of recognized or foreseeable hazards associated with medical devices under both normal and abnormal conditions. Previously identified hazards were also taken into account. The implementation hazards encompass the broad range of issues related to the realization or execution of the device specifications. They include matters involving the database, interface, processing, data corruption or loss, and audit trail items. The safety critical design requirements associated with the implementation hazards include the following:

- Prevent Sequencing Timing Error
- Prevent Data Loss/Corruption
- Prevent External Interface Errors

IMPLEMENTATION – SAFETY CRITICAL DESIGN REQUIREMENT: PREVENT SEQUENCING TIMING ERROR

There were three implementation hazards found to have the potential to jeopardize the realization of the safety critical design requirement to prevent sequencing timing errors. The first was that processing steps did not occur in the sequence expected. This system hazard may be caused by user error. The feature of the iTrace™ which served as the method of control included the RFID tracking system. This system employed a finite state machine, which only enabled valid state transitions for each business object. The finite state machine also indicated the acceptable and anticipated series of events for given objects. Furthermore, the iTrace™ is made up of wizard-like user interfaces that are used to guide users through the sequence of steps necessary to accomplish tasks.

Additionally, each component form contained validation logic preventing users from proceeding through the process unless the prior step was successfully completed. This method guaranteed that the correct sequence of events was followed, and that any errors were reported.

This hazard received a severity score of two and likelihood score of one. As a result of its minor gravity and highly unlikely threat of occurrence, this hazard was given a Pre-

Mitigation Risk level of **A**. The risk of this technology was acceptable due to the slight risk this hazard may pose.

The second hazard described the event in which multiple users were provided with access to update the same record. This system hazard was a consequence of software design or unavailable software capability. The features and functions of the iTrace™ included a variety of techniques that were applied to mitigate this hazard. Included in this were relational database and transaction processing procedures that were incorporated throughout the tool's software to allow for atomic, consistent, isolated, and durable (ACID) properties. The database transactions were designed to allow precise failure recovery, supply reliable units of work, and maintain consistency within the database, as well as inhibit multiple users from accessing the database simultaneously.

Furthermore, the transactions used also apply "all-or-nothing" semantics, meaning that the transaction is either completed entirely or not at all. Additionally, in order to sustain the integrity of the database and make certain that data is successfully written into it, transactions that were initiated concurrently by multiple users were isolated from one another. These functions of the tool had been shown to be effective strategies for hazard mitigation of electronic devices.

The level of severity for this hazard was two. The level of likelihood for this hazard was three. As a result of its believed propensity to transpire occasionally and lead to minor injury in its occurrence, this hazard was given a Pre-Mitigation Risk of **B**. Although it made the cutoff, it still lies on the borderline of tolerable and intolerable risks.

The next potentially hazardous event involved the system failure to receive timely data from an external application. There were two primary features of the design notable in this instance. The first was that external interface data remained parallel to database updates except in the case of dependencies. When data is not received, the omission is recorded in the log file. The second is reflective of the Blood Establishment Computing System (BECS). The interface of the BECS is defined based on Web services that produce definitions for error messages and information exchanged between applications. If an error were to arise that is outside of one of the definitions provided, a system-level assertion would appear forcing the operation to roll back.

This hazard was given a level two severity and level one likelihood. Due to its minor severity and improbable likelihood of occurrence, it received a Pre-Mitigation Risk level of **A**. Thus, this risk was deemed acceptable.

IMPLEMENTATION – SAFETY CRITICAL DESIGN REQUIREMENT: PREVENT DATA LOSS/CORRUPTION

There were five hazards which could potentially impact the requirement to prevent data loss and corruption. The first hazard in this category dealt with the instance in which user error caused the data to be corrupted. This system error caused by the user was deemed likely to occur occasionally (three) but with a negligible severity (one). The function utilized to mitigate this hazard was again validation logic. Validation logic is incorporated in all forms – Web and handheld – in which the user enters information into the system. Additionally, before data is recorded in the database, the BECS may also be interrogated to verify the validity of the information. When invalid data is entered, the user will receive an error message and further action will be inhibited until the error is corrected.

The second hazardous event in this set was the scenario in which data was lost or corrupted due to a hardware disk crash or other hardware or power failure. This was a borderline tolerable hazard, receiving a moderate severity score of three and remote likelihood of occurrence score of two. This hazard was tackled and mitigated as a result of the aforesaid ACID properties and all-or-nothing semantics. Additionally, it was recommended that multiple disks be used so that a back-up would be available to avert the potential loss of data. Finally, SQL can supply a warehouse for database backup and

recovery. The database may undergo refreshing and back-up procedures daily, and all data entered after the back-up took place would be restored from the SQL log-file.

The third hazard referred to the situation in which data was lost or corrupted due to the malfunction of the program routine. This system hazard was caused by incomplete transactions. The seriousness of the event was deemed negligible (one) and there was an occasional probability of it happening (three). As with many of the above-mentioned hazards, the functions employed to mitigate this hazard were the ACID properties and all-or-nothing semantics. Moreover, the iTrace™ itself, as well as the system's middleware and the related relational database technology have all been constructed to work in conjunction with various fault tolerant hardware configurations. These included support for the redundant array of independent disks (RAID) subsystems, SQL server clusters, and completely redundant configurations with fail over support.

The next hazardous event was the instance in which data encountered was outside the range of expected values. This system hazard was the result of an undetected anomaly or user error. Here, again, the seriousness of the hazard was negligible (one) and the chance of occurrence (three) was occasional. As described previously for other hazards, the hazard mitigation features relevant in this case included validation logic and BECS interrogation. Furthermore, all system critical data is stored in reference tables. Because

users must choose from drop-down lists, all selected values are valid. Other data was scanned via barcodes. Also, in the case of invalid data entry, the user was alerted with an error message and prohibited from proceeding until the error was corrected.

Finally, the last hazard in this set was the event in which duplicate data entered the system. This system hazard was the result of user error. It fell on the borderline of tolerable/intolerable risks with a severity score of two and likelihood score of three. This indicated that it will produce minor injury/loss of function in the occasional instance that it does happen. The method used to mitigate this hazard involved the unique ID assigned to all products and business subjects within the RFID blood supply chain tracking system. The presence of the unique ID inhibited the user from creating or entering duplicate information. Also, here the BECS may again undergo interrogation to confirm the validity of the data being entered into the system.

All five of the hazards described were assigned a Pre-Mitigation Risk of **B**. All are tolerable risks, although some appear on the borderline of tolerable and intolerable in the matrix. This simply means that greater effort or higher cost may be associated with the mitigation of these hazards than those in the middle or closer to the acceptable risk level.

IMPLEMENTATION – SAFETY CRITICAL DESIGN REQUIREMENT: PREVENT EXTERNAL INTERFACE ERRORS

There were five hazards discovered which may present a threat to the safety critical design requirement of preventing external interface errors. The first was the event in which the system fails to receive accurate data from the RFID reader interface. This was a system hazard caused by hardware failure. It received level two severity (minor) and level three (occasional) likelihood scores. The method of control to mitigate this hazard involves the large number of technologies integrated into the system design to ensure detection in case of a failure in an RFID read point. The technologies consisted of reader self-test diagnostics, inactivity timers, periodic heart beat signals, and positioning sentinel tags to verify the accurate operation of the readers.

The second hazardous event described the instance in which the tag and barcode were both unreadable. This system hazard was caused by physical damage from handling the product. It was assessed as very unlikely to occur (one) yet with moderate severity (three) when it does transpire. The mitigation strategy applied was quite simple. If both the RFID tag and barcode become unreadable, the user is instructed to proceed with standard operating procedures in which the blood product is disposed of appropriately due to the inability to reliably determine, track, and monitor the unique unit ID and related information.

The next hazardous event was the inability to read or write the RFID tag data due to a tag failure. This event was also a system hazard that resulted from the physical damage of improperly handling the product. This hazard presented a minor severity (two) which occurred on an occasional (three) basis. The mitigation procedure employed for this technology involved the RFID tracking system applications that write information to the user data portion of the RFID tags. These applications include:

1. Collection (handheld reader).
2. Label Product (pad reader).
3. Check-in Imports (pad or handheld reader).
4. Check-in Returns (pad or handheld reader).

For these applications, the software writes blood bag information into the RFID tag. The software then immediately rereads the tag to confirm that the data was successfully written and, if the write/read cycle failed, then an error message is delivered. Additionally, because none of these applications depend on information read from the user data portion for subsequent processing, there is no risk of misreading the tag information. Furthermore, the TIN is read at numerous times throughout the supply chain. The hardware and air-protocols used for communication between the reader and the tag ensure that tag IDs are properly read and written to the application.

The fourth hazardous event in this set was the situation in which data received from BECS does not pass correct data structure. This system hazard was due to unrecognized data being received from the BECS. It is a fairly serious hazard, receiving a moderate severity score (three) and remote likelihood of occurrence score (two). The function responsible for mitigating this hazard was related to the interface definition and communication between the iTrace™ and the BECS. The definition of the BECS interface to iTrace™ is based on a set of web services and consists of error messages and information exchanged between the applications. Also, a system-level assertion is raised and the operation rolled back in the instance that an error outside of the definition appears.

The final hazard that fell under this category was the event in which errors detected in the BECS were not handled properly. Like the previous hazard, this hazard was caused by unrecognized data from the BECS. This hazard was perhaps the least impactful of all potential hazards described thus far, receiving severity and likelihood scores of one and one. Here, again, the mitigation method involved the way in which the BECS is defined. Furthermore, the BECS executes different procedures when dealing with critical vs. non-critical data. For critical data, the BECS will deliver an error message to the user. For non-critical data, the BECS will not update the data, but will log the exception using normal BECS functionality.

While this hazard received a Pre-Mitigation Risk score of **A**, the other four hazards described in this set were given a score of **B**. Therefore, the risk of the BECS not handling errors appropriately can be deemed negligible in comparison to the others described in this category. It is believed to have the least impact on the safety critical design requirement of preventing external interface errors.

CHAPTER 6: FUNCTIONAL HAZARD ANALYSIS

The functional hazards identified and tested are also components of SysLogic, Inc.'s known and foreseeable list of risks associated with medical devices. Functional hazards consist of any known risks to the performance of the system or device in an operational setting. They are comprised of concerns related to the ability of the system to record read and written information appropriately and accurately. They also include other software design and capability issues such as security, access, traceability, notification, alerts, monitoring, tracking, and labeling. The following safety and critical design requirements will be addressed in this chapter:

- Preventing Unauthorized Entry or Override of System Data
- Preventing Loss of Traceability

- Preventing Packing in Improper Containers at Collection Sites
- Ensuring Reconciliation of Materials from Collection Site
- Ensuring Blood Product Labeling Information is Properly Captured from BECS
- Preventing Unsuitable Products from Being Released to Distribution

FUNCTIONAL – SAFETY CRITICAL DESIGN REQUIREMENT: PREVENT UNAUTHORIZED ENTRY OR OVERRIDE OF SYSTEM DATA

There were three system security hazards that could potentially impact the safety critical design requirement of preventing unauthorized entry or override of system data. The first and second hazards described situations in which the system was accessed by unauthorized and untrained users respectively, and the third hazard went a step further in that the unauthorized personnel was able to actually modify records. All instances were due to security failures in which the system failed to prevent entry of undesignated users into the system. The middleware application of the iTrace™ was based on Microsoft Windows.Net authentication and authorization services. This application employs a role-based security subsystem that is designed to prohibit and regulate access as desired. Moreover, standard operating procedures are in place that give the system administrator control over who may obtain access as well as the process by which to do so.

All three hazards were given a Severity score of two and a Likelihood score of one. As a result, the Pre-Mitigation Risk for all were **A**. Due to the controls in place, it is improbable that these hazards will take place and, if they were to occur, would have only a minor effect.

FUNCTIONAL – SAFETY CRITICAL DESIGN REQUIREMENT: PREVENT LOSS OF TRACEABILITY

Six hazards were found to be capable of affecting the system's ability to prevent loss of traceability. The first was the circumstance in which someone other than a responsible user enters or modifies the data. This hazard may be caused by a system failure to track those responsible for making database modifications. As with the hazardous events described above, this hazard can be controlled by the design features of the middleware and the standard operating procedures in place. Additionally, activity logs and audit trails were created and maintained for each business object in the iTrace™ RFID tracking system. The activity logs, which may be viewed, extracted, and reported from the application, detail what the activity was, when the activity occurred, and who initiated the activity.

The Severity and Likelihood scores assigned to this hazard were two and one respectively. Hence, the Pre-Mitigation Risk was **A**. This shows that the hazard is an acceptable risk for the implementation of the iTrace^{TM}.

The remaining five hazards within this category dealt with the incorrect recording of blood unit information. These hazards may be caused by the failure of the system to record data for whole blood collection, the breakdown of the system in capturing data for apheresis collection, and the malfunctioning of the system in distinguishing between autologous and therapeutic donation types. All can be mitigated by the validation logic incorporated into the system. Furthermore, before information is submitted to the database for further processing, the BECS may also be subject to interrogation to verify that this information being input is valid. When invalid data is entered as a result of user errors, the user receives an error message and is prevented from proceeding until the error is resolved.

Moreover, the application requires that collection data is entered in sequential order and designated format. The user is prohibited from varying from the process order. Data capture must be complete in order for the acceptance of the donation. The user would have to revert to manual procedures in this circumstance.

What is more, the procedural methods further enabled the correct identification of donation type by mandating that autologous donations were tie tagged with a label to

identify them as a donation to fill physician orders. Therapeutic donations were given discarded labels which were attached to collection bags to identify them as unacceptable donations. BECS functionality may be used in this instance as well to correct the donation type.

These five hazardous events were rated a three and one respectively on the Severity and Likelihood scales. In the very unlikely instance that they would occur, they could have a moderate impact. Blood unit information must be accurate to enable the most precise collection of data and reduce the potential transfusion errors that could arise. The Pre-Mitigation Risk given is a level **B**. As such, the hazard is tolerable, yet mitigation may lead to some costs.

FUNCTIONAL – SAFETY CRITICAL DESIGN REQUIREMENT: PREVENT PACKING IN IMPROPER CONTAINER AT COLLECTION SITE

Three system hazards were identified as being able to possibly affect the need for packing products in appropriate containers at collection sites. All of these hazards were due to software design or unavailable software capability. The first hazardous event was the general case in which the system fails to ensure that product is packed in the correct container. The method of control initiated in this case primarily involved assigning a specification for the type of shipping container required for each product to each product

code. There are four types of containers utilized by this system: 1) Blood Donation Record (BDR) pouches, 2) blood bag coolers, 3) platelet containers, and 4) test tube coolers. The secondary method of control was the five properties by which each container was further distinguished. The five properties included: 1) container type (including rated description), 2) label prefix, 3) ISBT bar code, 4) capacity, and 5) RFID TIN. Consequently, when a user attempts to pack products in inappropriate or unsuitable containers, an error message is displayed.

The next hazard in this group described the situation when the system fails to maintain appropriate container capacity for packed product. Similar to the mitigation method provided for the aforementioned hazard, the strategy here also relied on type of containers and their properties thereof. One of these properties is capacity. On the occasion when a user exceeds the capacity suitable for packing a particular container, the user will receive an error message.

The two hazards discussed thus far received severity and likelihood scores of two and two, as well as Pre-Mitigation Risks of level **B**. These hazards were believed to have a minor impact in the rare instances that they occur. As such, they were deemed tolerable hazards.

The last hazard in this category was a bit more acceptable than the two previously mentioned. The event in which the system fails to notify the user when attempting to

pack an already packed item was given a Pre-Mitigation Risk level of **A**. The severity score was a one, indicating a negligible risk, and the likelihood score was a two, signifying a rare occurrence. The mitigation strategy for this hazard involved the unique Tag ID (TID) attached to each product. The tracking mechanisms of the iTrace™, in conjunction with the TID, reduce the potential of multiple records existing for DIN/bag type combinations. As a result, the user receives an error message when trying to pack a product multiple times.

FUNCTIONAL – SAFETY CRITICAL DESIGN REQUIREMENT: ENSURE RECONCILIATION OF MATERIALS FROM COLLECTION SITE

Two key hazardous events threatened to impede the accuracy of the material reconciliation process from collection sites. These system hazards were also due to software design or unavailable software capacity. The first was the situation in which a container is left at the collection site. The system employs a thoroughly defined pick-up operation as the method of control for this hazard. As characterized in the system, a pick-up entails the identification and loading of all containers holding collection materials. The system will not enable the release of a pick-up unless and until all packed containers have been loaded.

This was a tolerable hazard. It was assigned severity and likelihood scores of two for each, and a Pre-Mitigation Risk level of **B**. Therefore, it was considered to be a minor hazard that will transpire only under rare circumstances.

The second hazard was slightly less significant, receiving a Pre-Mitigation Risk level of **A**. This risk was acceptable as it was given severity and likelihood scores of one and two respectively. It described the incident when the system failed to generate a manifest. This hazard will have only a negligible impact during the rare times that it will actually take place. This is because the mitigation strategy involving the manifest data consisted of two components. The first is that database is updated with manifest data whenever containers are added to pick-up. The second is that the system generates a manifest report listing all containers included in the pick-up process. Thus, even if the manifest report is not obtained at the production facility, the manifest can be viewed online. Materials from the pick-up are then reconciled using the database.

FUNCTIONAL – SAFETY CRITICAL DESIGN REQUIREMENT: ENSURE BLOOD PRODUCT LABELING INFORMATION IS PROPERLY CAPTURED FROM BECS

Two system hazards may impact the appropriate capturing of blood product labeling information from the BECS. The first – system fails to receive labeling data from BECS

– may be mitigated by features of the BECS interface design. The BECS interface consists of web services which include a definition of the error messages and information exchanged between applications. When an error takes place outside of this definition, three events will transpire: 1) an error message will be sent to the user, 2) a system-level assertion will be raised, and 3) the operation will be rolled back.

Consequently, in the instance that this occurs, the severity was rated only minor (two) and the likelihood only rare (two). A Pre-Mitigation Risk of level **B** was assigned to this hazard, as it was a tolerable risk. The costs were not expected to be high in reducing this hazard.

The second hazard had an even lower cost expectation in reducing the hazard with a Pre-Mitigation Risk of level **A**. It denoted the incident in which the system failed to verify data received from BECS was written to the RFID tag. This hazard possessed a likelihood factor score of one and a severity of two, meaning that, in the improbable instance that it does actually occur, it will only have a minor impact.

The method of control for this hazard began with the use of ISBT standards to physically label all blood products. The ISBT label serves as a system of record label that is used throughout the lifecycle of the product as a form of identification. The system uses web services to request label information from the BECS. The information was then written to the iTrace™ database and subsequently to the RFID tag. Finally, the tag was read again

to confirm that the data was written correctly. As with the previous hazard, when an error arises, a message is sent to the user, a system-level assertion is raised, and the operation is rolled back.

FUNCTIONAL – SAFETY CRITICAL DESIGN REQUIREMENT: PREVENT UNSUITABLE PRODUCT FROM BEING RELEASED TO DISTRIBUTION

The only hazard found that may impact the ability of the system to prevent an unsuitable product from being released to distribution was the event in which an unsuitable product was released into inventory. This hazard may be prevented with inherent functionality of the BECS. The BECS may perform multiple checks to ensure the appropriateness of all products prior to their being checked into inventory, packed, or released. If the product is unsuitable for any reason, the user is notified via an error message and the state of the product remains the same.

This hazard represented an extremely low risk. It was given a one on the severity scale showing that it is of negligible consequence. It was also given a one on the likelihood scale, indicating that its occurrence is highly unlikely. In other words, in the implausible instance that this hazard does transpire, it will induce only a trivial effect. Hence, the Pre-Mitigation Risk level was **A**, as this was deemed an acceptable risk.

CHAPTER 7: RESULTS

This chapter summarizes the findings obtained during the protocol, unit, and system testing approaches.

PROTOCOL TESTING RESULTS

The results of the protocol testing are all discussed in the technology hazard analysis above. Worst-case scenarios, traditional performance expectations, survivability tests, and EMI/communications investigations, accompanied by methods of control either in the features, design, or functioning of the technology, confirmed the benefits of utilizing the iTrace™. All of the study results fell under the threshold and within the acceptance criteria designated. The outcomes essentially showed that the technological design and capabilities of the iTrace™ may be relied upon to perform as expected without any significant impact to the safety and critical design requirements of applying the device to everyday operations.

UNIT TESTING RESULTS

The results of the unit tests were all favorable. The operations all performed as expected, and there were no discrepancies or deviations from the anticipated scenarios. Hence, the

potential hazards had no significant effect on the safety critical design requirements. The system was highly functional and effective throughout all of the processes tested from donor to Blood Center of the Blood Transfusion Supply Chain.

SYSTEM TESTING RESULTS

As with the results of the unit testing, the outcomes of the system testing proved to be very promising. The system testing results also displayed a great deal of usability and efficiency in the system. The potential hazards had no significant impact on operations.

There was, however, one minor discrepancy in the system testing. During test case six (ST6), in which the processing of multiple donations and procedure types in the collection techniques, as well as the attributes and interdictions triggered based on donation and procedure types were all tested, there was an error in the transmission to the BECS. The autologous type of donation should have a CUE passed as “S.” Instead, the CUE was passed as “Y.” This incorrect read/write or transmission of information of information would have a minor impact. Nevertheless, this error was retested in ST22. This time, the outcome was successful. Therefore, the appropriate fix was applied and this hazard appeared to be reduced. The results may be viewed in the Traceability Matrix tables (Appendix A).

CHAPTER 8: TRACEABILITY MATRIX

The RFID Transfusion Consortium recruited my assistance in creating a traceability matrix for the hazards and their associated verification/validation tests. The goal of constructing a traceability matrix is to achieve the following:

- Ensure that identified hazards may be traced to either an approved protocol/study or to the software requirements specification (SRS) for each function and/or various third-party tools.
- Validate that the appropriate methods of control and acceptable results were achieved to mitigate or eliminate hazards.

The importance of the traceability matrix underscores the need for documenting all possible hazards, and ultimately making them known and accessible in central repositories. The potential hazards evaluated for the application of the iTrace™ are all accounted for in the system requirements specifications, through study exploration, or through unit (UT) and/or system testing (ST). Appendix A displays the connection of the hazards to one or more of these aforesaid sources.

CHAPTER 9: DISCUSSION

This chapter contains thorough analyses of each research question evaluated in this study. The following inquiries were answered:

RQ 1: How do the benefits of using the iTrace™ outweigh the potential RFID-related hazards?

RQ 2: How sufficient are the mitigation and correction strategies for managing RFID-related hazards in the blood transfusion medicine supply chain from the donation to blood center distribution?

RQ3: How can the methods utilized in this paper effectively qualify and quantify the associated hazards into standard categories which may be transferable to other newly deployed RFID-based healthcare technologies?

BENEFITS VS. RISKS

The benefits of implementing the iTrace™ have been referenced comprehensively throughout this document. This novel RFID-enabled solution has been shown to possess valuable abilities and functionalities which can significantly revamp the processes of the blood transfusion supply chain. These processes include: labeling, tracking, monitoring, packing, and documenting, leading to improved traceability and increased productivity of workflow operations.

On the other hand, the risks of employing the system have also been illustrated. There were a total of 62 possible hazards identified throughout the analysis of the iTrace™. In order to compare the advantages vs. disadvantages of utilizing the system, the level of the risks must be weighed and measured in relation to the benefits.

As described above, a Pre-Mitigation Risk of Level A is indicative of an acceptable risk. The likelihood of these risks tends to be rare, while the severity is minor at most. This score suggests that the risk is so slight that it can be neglected compared to the risks of other hazards, and there may not be a need to reduce the risk.

Of the 62 hazards discovered, 28 received Pre-Mitigation Risk Levels of A. The hazards which fall into this category are illustrated in Appendix B.

The architecture of the system, as well as the procedures designed for its use, play a role in the low risk rating of these hazards. It is important to note that the hazards listed in this category include those which essentially define the iTrace™ application. They may potentially impact what the system was created to do. This group contains the hazards identified as adversely impacting the safety and usability of blood products, the performance of the tags, the security of the system, the appropriate packing and labeling of items, and ultimately the release of damaged products into inventory. Since the

hazards which may, arguably, best characterize the application appear to be trivial, it appears that the cost of employing the iTrace™ is outweighed by the benefits.

In contrast, the next set of hazards fall into the Pre-Mitigation Risk level of B. A risk level of B signifies tolerable hazards. Tolerable hazards are not detrimental to the employment of the application, but can have a meaningful impact. Consequently, they must be reduced, mitigated, or corrected to ensure the best and safest use of the system. The strategies undertaken to do so may lead to significant resource and labor costs.

There were 34 hazards that attained the rating of Pre-Mitigation Risk Level B, as shown in Appendix C.

As opposed to the defining traits encompassed by the Level A hazards, the Level B hazards represent the utility attributes of the iTrace™. The Level B hazards consist of those involved in read/write failures, data loss/corruption, tag survivability, external interface errors, product and information traceability, and interference and communication transmission disruptions. These hazards embody the risks to the system's functional efficacy. They could possibly impact how the system performs and sustains operational integrity. Therefore, these hazards are substantial as well.

The methods of control associated with these hazards were either incorporated into the system design, or were thoroughly assessed via system, unit, and protocol testing. The

positive results of all tests demonstrated the low cost that would need to be expelled in order to mitigate the hazards. Thus, the resource and labor cost for employing the system appears to be lower than the benefits.

In addition to the resource and labor cost, there is the necessity for economic justification. Briggs et al (2009) assessed the economic cost for RFID-enablement. They noted the quality gains which could be earned by eliminating the number of damaged products and facilitating increased traceability by reducing the number of misplaced products. Additionally, quality gains can be viewed through better reconciliation and tracking of products. Furthermore, they evaluated efficiency gains. These benefits were illustrated through faster reconciliation, enhanced productivity, and decreased labor. Ultimately, this would lead to a return on investment by a blood center of approximately three years. Hence, the advantages of implementing the iTraceTM significantly offset the costs. The technology will serve as a valuable means of improving the blood transfusion supply chain processes.

EVALUATING THE EFFECTIVENESS OF MITIGATION AND CORRECTION STRATEGIES

The method of control listed for each hazard included strategies to prevent the hazard from happening, resolving the hazard post-occurrence, or a combination of both. There are three categories under which each approach may fall. They are the following:

- I. Prevents/Mitigates the Hazard from Occurring: This measurement reflects the ability of the method of control to deter the risk from happening. It is the most highly desired effect of the controls.
- II. Corrects/Remedies the Situation Following the Occurrence of the Hazard: This measurement reflects the ability of the method of control to respond to the hazard post-occurrence. It includes resolution strategies and back-up plans to account for hazards. It is not as appealing as the prevention methodologies, but it does provide an effective solution to dilemmas that may unfold.
- III. No Effect on Hazard Mitigation or Correction: This measurement reflects the total inability of the strategy to proactively inhibit or counter the risks associated with iTraceTM use. It consists of the most undesired methodologies due to the lack of efficiency in negating or amending processes in the face of hazards.

Each hazard's method of control was placed into one of these categories. If the strategy consisted of a combination of both prevention and correction measures, then it was given a **I** rating, as it demonstrated the reduction and resolution of the hazard.

There were 58 hazard strategies that received an I rating. Included in this group were those which apply aversion or resolution design features and procedures for each hazardous event. The great amount of strategies belonging to the I category confirm their efficacy.

The remaining four hazards fell into the II category. They are shown in Table 8.

Table 8: Hazards in Risk Mitigation Category II

Hazard ID	Hazardous Event	Hazard Type	Safety Critical Design Requirement	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Risk Mitigation Category (I, II, III)
T.1.2.	RFID Read/Write Fails	RFID Technology	Prevent Data Read/Write Error/Failure	B	II
T.1.5.	DIN number on tags created at final labeling is altered	RFID Technology/System	Prevent Data Read/Write Error/Failure	B	II
T.1.6.	ABO rewritten on tag	RFID Technology/System	Prevent Data Read/Write Error/Failure	B	II

Hazard ID	Hazardous Event	Hazard Type	Safety Critical Design Requirement	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Risk Mitigation Category (I, II, III)
I.3.2.	Tag and barcode are both unreadable	System	Prevent External Interface Errors	B	II

Ultimately, since the majority of methods fall in the I category, the design elements and processes instituted to mitigate the hazards appear to be highly effective. Even the hazards that require resolution only after the hazard has transpired have pre-mitigation risk levels of B, indicating they are tolerable hazards. Moreover, none of the hazards had a risk level of III. This means that all of the approaches taken to reduce the threat of the hazard have some positive impact. Hence, the strategies are successful. Therefore, the mitigation and correction strategies for managing RFID-related hazards in the blood transfusion medicine supply chain from the donor to blood center distribution are effective.

EVALUTATING THE EFFECTIVNESS OF THE METHODS UTILIZED IN THIS PAPER TO QUALIFY AND QUANTIFY HAZARDS INTO STANDARD, TRANSFERABLE, AND GENERALIZABLE CATEGORIES

The process described in this paper consisted of several tactical steps. It began with the research and recognition of previously discovered hazards that are applicable to similar medical devices. These hazards were related to the use of RFID technology in clinical settings. Additionally, due to the familiarity with some of these comparable devices, the FDA CBER and CDRH governing bodies were able to provide guidance on particular protocols to perform. The devised protocols were examined to uncover potential harms which could be caused through application of the system and the technology itself. RFID technology, functions, and the use of the system in both traditional and extreme settings were analyzed to discover the effects of implementing and verify the usability of the system.

The system design, requirements, and standard operating procedures were then evaluated. These documents were used to determine what other hazards could occur from utilizing the iTrace^{TM}. They were also assessed to reveal both the system features which could be employed and/or measures which could be taken to avoid and/or correct each hazard.

After that, further validation tests were performed. These tests examined the likelihood of the hazard existence and the strategies for mitigating and correcting them. I included an additional measure to account for the distinction between when the strategy prevents or resolves the hazard to provide a further calculation of its efficiency. The validation tests also assessed the use of the iTrace™ in its normal setting. Unit and system tests were performed for all functions and applications of the iTrace™ along the blood transfusion supply chain to ensure that the system executed all desired capabilities as expected.

Next, a traceability matrix was created to record and track the hazards and tests. The matrix served as a record of the specific design component and/or test performed to evaluate each hazard, establishing an important link between each hazard and its means of evaluation. As a result, if the same hazards were to be identified in other similar devices, the characteristics and tests associated with them would be evident, and the knowledge would be readily available for those evaluating them. Thus, the necessity for documenting each hazard and its associated tests so that they may be recognizable and accessible was highlighted with the formation of the traceability matrix.

The next steps consisted of several analyses. The first was weighing the benefits versus the risks of employing the device based on the existence of the identified hazards, their severity, likelihood, and the ability to mitigate and correct them. Then, the effectiveness

of these strategies was assessed to gauge whether these methods were suitable and efficient enough to reduce the threat of the hazard. Finally, standard risk assessment measures to quantify the hazards into categories of severity and likelihood, as well as a novel measure to group the strategies based on their ability to either prevent the hazard from occurring or resolve it post-occurrence were employed. The process for building the framework for iTrace^{TM}-related hazards in the blood transfusion supply chain – identifying, measuring, and analyzing the risks – was very thorough and may be used for the deployment of other similar medical devices using RFID technology. Therefore, the methods utilized in this paper effectively quality and quantify the associated hazards into standard categories which may be transferable to other newly-deployed RFID-based healthcare technologies.

CHAPTER 10: CONCLUSION

The RFID Blood Center Consortium is implementing the first ever RFID-enabled solution for the tracking and maintaining of blood products throughout the entire blood transfusion supply chain. The iTrace^{TM} will serve as a purposeful approach towards reducing medical errors originated in the blood transfusion supply chain and, ultimately, transforming the delivery of care. There are numerous benefits of the iTrace^{TM}, but there

are also several hazards. The costs for implementing the device are offset by the benefits. The hazards may be successfully mitigated via valuable design features and operating procedures.

The RFID Transfusion Consortium needed help in identifying possible RFID technology hazards and analyzing all of the potential hazards that could come about from using the iTrace™. The comprehensive analysis presented in this paper, which focused on the blood transfusion supply chain from the donor to blood center distribution, is a valuable starting point for RFID hazard management in the blood supply chain. The 62 hazards identified include those associated with the technology, implementation, and functionality of the device. All of these hazards were accompanied by successful methods of control, demonstrating the effectiveness of the strategies and the tool itself. All new medical devices must undergo detailed examination of the potential benefits and harms it may cause. Due to the extensiveness of the research presented through my work and in this paper, the iTrace™ was shown to be useful and worthwhile. Ultimately, this study showed that the benefits of the iTrace™ outweighed the costs and that the correction and mitigation strategies were effective. Thus, the answers to research questions 1 and 2 were derived.

As a result, the foundation for establishing a systematic framework for RFID hazard mitigation in the blood transfusion supply chain from donation to distribution at the blood

center was set for this system as well as for future use with other similar technologies. The methods revealed the overall approach of identifying the hazards, validating and verifying the hazards, determining the means of mitigating and correcting the hazards, qualitatively and quantitatively ranking their level of severity, and assessing the effectiveness of the correction strategies. As the project lead for the technology hazard analysis component, I identified the technology hazards, evaluated all of the hazard types, investigated the mitigation and correction methods for all of the hazards, assisted in protocol tests, and prepared valuable documentation for all of these steps. My work, which significantly bridged the gaps in RFID technology hazard identification and overall system hazard analysis, is considered an important step towards the commercialization and implementation of the iTrace™. Since this evaluation of the possible hazards that could occur from utilization of this novel medical device is all-encompassing, it is possible to apply the aforementioned methodology to other medical devices and technologies. Additionally, as technology continues to advance, this methodology will become increasingly practical and important. The strategies discussed and hazards identified may be generalizable and usable for other RFID-enabled medical devices. Therefore, the answer to research question 3 was received as well.

Moreover, the hazard identification, analysis, and mitigation processes discussed in this paper may also be effective for Phase Two of this device analysis: blood center

distribution to patient. The means used take into account technology hazards and mitigation strategies will not change. For example, verification strategies such as the Wireless Considerations Protocol evaluated the interference of HF RFID on wireless and communication systems. The methods and results of this study may be applicable in a hospital setting as well, where there are several such potential instances for disturbance. In addition, the functional and implementation identification and analysis processes are similar in some areas as well. For instance, validation strategies such as system and unit testing, as well as pilot and performance qualification studies will be essential towards determining whether the iTrace^{TM} is fully applicable in a hospital environment. Even in the many areas where differences do exist, the need for identification, validation, verification, and analysis will remain.

Nevertheless, there are several additional hazards that may potentially occur from the use of this system in the different environment examined during Phase Two. This phase represents the remaining steps of supply chain. For example, safety hazards – hazards affecting the patient receiving the actual transfusion and staff involved in the blood supply chain – may also occur. The effects of interaction with other hospital systems and safety hazards that may come about during the actual transfusion portion of the blood supply chain may lead to other complex hazards and, consequently, additional analysis techniques. Yet, the framework established in this paper may certainly be used as a

foundation. Upon completion of the hazard analysis throughout this portion of the process, a wholly conclusive framework for RFID hazard management may be formulated.

Future research may consist of a Post-Mitigation Risk study. Although this study included references to several protocols and tests utilized to assess the efficacy of the mitigation strategies, it will be valuable to fully assess the methods after the system has been put to use daily. Similar tactics may be used at this stage to verify the risk levels assigned.

Future research may also investigate any potential hazards that may be triggered by the mitigation strategies themselves. For instance, it may be possible that the data locking feature applied to the memory fields could malfunction and render the RFID tags incapable of being reused. It would be valuable to ensure that no further hazards transpired as a result of the methods employed to reduce the originally-discovered hazards.

Nevertheless, the approach taken in this paper to evaluate the tool and its potential hazards are effective. The groundwork of the strategic framework for managing RFID-enabled hazards in the blood transfusion supply chain has been laid. As such, an important step on the road towards the elimination of avoidable medical errors has been taken with the development of the iTrace™.

REFERENCES

1. Bates DW, Cohen M, Leape LL, Overhage JM, Shabot MM, Sheridan T. Reducing the frequency of errors in medicine using information technology. Journal of the American Medical Informatics Association. 2001;8(1):299-308.

2. Briggs L, Davis R, Gutierrez A, Kopetsky M, Young K, Veeramani R. RFID in the blood supply chain--increasing productivity, quality and patient safety. Journal of Healthcare Information Management : JHIM, 2009, Vol.23(4), P.54-63. 2009;23(4):54-63.

3. Institute of Medicine. To err is human: Building a safer health system. Washington, DC: National Academy Press; 2000.

4. Thomas EJ, Studdert DM, Newhouse JP, Zbar BIW, Howard KM, Williams EJ, et al. Costs of medical injuries in utah and colorado. Inquiry. 1999;36(6):255-264.

5. Thomas EJ, Studdert DM, Burstin HR, Orav EJ, Zeena T, Williams EJ, et al. Incidence and types of adverse events and negligent care in utah and colorado. Medical Care Research & Review. 2000;38(3):x,261-271.

6. Perrin RA, Simpson N. RFID and bar codes - critical importance in enhancing safe patient care. Journal of Healthcare Information Management. 2004;18(4):33-39.

7. Leape LL, Bates DW, Cullen DJ. Systems analysis of adverse drug events. JAMA: Journal of the American Medical Association. 1995;274(1):35-43.

8. Whitaker BI, Sullivan M. The 2005 nationwide blood collection and utilization survey report. Washington, DC: US Department of Health and Human Services; 2005.

9. Trace of blood. Industrial Engineer: IE. 2008;40(5):13-.

10. Dzik WH. Transfusion safety in the hospital. Transfusion. 2003;43(1):1190-1199.

11. Dzik WH. New technology for transfusion safety. British Journal of Haematology. 2007;2(1):181-190.

12. Minz PD. Nishot: On target, but there's no magic bullet. American Journal of Clinical Pathology. 2001;116(6):802-805.

13. Sazama K. Reports of 355 transfusion-associated deaths: 1976 through 1985. Transfusion. 1990;30:583-590.

14. Love EM, Soldan K. SHOT annual report 2000-2001. Serious Hazards of Transfusion; 2002.

15. Ahrens N, Pruss A, Kiesewetter H, Salama A. Failure of bedside ABO testing is still the most common cause of incorrect blood transfusion in the barcode era. Transfusion & Apheresis Science. 2005;33(1):25-9.

16. Lockwood WB. Transfusion medicine today: Mission accomplished? MLO: Medical Laboratory Observer. 2009;41(1):12-6.

17. Knels R. Radio frequency identification (RFID): An experience in transfusion medicine. ISBT Science Series. 2006;1:238-241.

18. Knels R, Kurz M. Improvement of the logistics in transfusion medicine and of the safety of blood transfusion by radio frequency identification. Vox Sanguins. 2005;89(1):191.

19. Davis R, Gottschall J, Gutierrez A, Hohberger C, Veeramani D, Holcombe J. Absence of acute adverse in-vitro effects on AS-1 RBCs and whole blood-derived platelets following prolonged exposure to 13.56 MHz radio energy. Transfusion. 2010;50(7):1596-603.

20. Adding RFID layer to blood safety loop [Internet].: College of American Pathologists; 2005; cited January 2012]. Available from: http://www.cap.org/apps/cap.portal?_nfpb=true&cntvwrPtlt_actionOverride=%2Fportlets%2FcontentViewer%2Fshow&_windowLabel=cntvwrPtlt&cntvwrPtlt%7BactionForm.contentReference%7D=cap_today%2Ffeature_stories%2F0705RFID.html&_state=maximized&_pageLabel=cntvwr.

21. Dzik S. Radio frequency identification for prevention of bedside errors. Transfusion. 2007;47(Suppl):125S-129S.

22. Mississippi blood services improves processes with RFID from texas instruments and AARFID. [Internet].: More RFID; 2006; cited January 24, 2012]. Available from: http://www.morerfid.com/details.php?subdetail=Report&action=details&report_id=2039&display=RFID.

23. Sandler G, Langeberg A, Carty K, Dohnalek LJ. Bar code and radio-frequency technologies can increase safety and efficiency of blood transfusions. Lab Med. 2006;37:436-429.

24. Sandler GS, Langeberg A, DeBandi L, Gibble J, Wilson C, Feldman CL. Radiofrequency identification technololgy can standardize and document blood collections and transfusions. Transfusion. 2007;47:763-770.

25. Using location, time, and temperature data to monitor the blood transfusion chain in a hospital [Internet].: American; 2008; cited January 24, 2012]. Available from: http://www.aacc.org/events/meeting_proceeding/Documents/using_location.pdf.

26. Bendavid Y, Boeck H, Philippe R. Redesigning the replenishment process of medical supplies in hospitals with RFID. Business Process Management Journal, 2010, Vol.16(6), P.991-1013. 2010;16(6):991-1013.

27. Med-tech notes. Medical Device Daily. 2011;15(155):6-.

28. Kebo V, Klement P, Cermakova Z, Gottfried J, Sommerova M, Palecek A. The potential of RFID technology in blood center processes. Studies in Health Technology and Informatics. 2010;156(1):71-77.

29. Radio-frequency identification: Its potential in healthcare. Health Devices. 2005;34(5):149-60.

30. Knels R, Davis R, Ashford P, Bidet F, Bocker W, Briggs L, et al. Guidelines for the use of RFID technology in transfusion medicine. Vox Sang. 2010;98:1-24.

31. Wart R. An introduction to RFID technology. Pervasive Computing IEEE. 2006;5(1):25-33.

32. Sedlmayr M, Becker A, Muench U, Meier F, Prokosch H, Ganslandt T. Towards a smart object network for clinical services. AMIA Annu Symp Proc. 2009;2009:578-82.

33. Glabman M. Room for tracking. RFID technology finds the way. Materials Management in Health Care. 2004;13(5):26-28, 31-34.

34. Choi Y, Kim S, Son S, Cho K. Design of the RFID for storage of biological information. Journal of Systemics, Cybernetics & Informatics. 2009;7(1):13-7.

35. Hohberger C, Davis R, Briggs L, Gutierrez A, Veeramani D. Applying radio-frequency identification (RFID) technology in transfusion medicine. Biologicals. 2011(10).

36. Roark DC, Miguel K. RFID: Bar coding's replacement? Nurs Manage. 2006;37(2):28-31.

37. Mehrjerdi YZ. RFID-enabled healthcare systems: Risk-benefit analysis. International Journal of Pharmaceutical and Healthcare Marketing, 2010, Vol.4(3), P.282-300. 2010;4(3):282-300.

38. Davis R, Geiger B, Gutierrez A, Heaser J, Veeramani D. Tracking blood products in blood centres using radio frequency identification: A comprehensive assessment. Vox Sang. 2009;97(1):50-60.

39. Carrasco VN, Jackson SS. IT world. real time location systems and asset tracking: New horizons for hospitals. Biomedical Instrumentation & Technology. 2010;44(4):318-23.

40. Attaran M. RFID: An enabler of supply chain operations. Supply Chain Management: An International Journal, 2007, Vol.12(4), P.249-257. 2007;12(4):249-57.

41. Ohashi K, Ota S, Ohno-Machado L, Tanaka H. Smart medical environment at the point of care: Auto-tracking clinical interventions at the bed side using RFID technology. Computers in Biology & Medicine. 2010;40(6):545-54.

42. Puckett F. Medication-management component of a point of care information system. American Journal of Health-System Pharmacy. 1995;52(1):1305-1309.

43. Larrabee S, Brown MM. Recognizing the institutional benefits of barcode point of care technology. Community Journal of Quality Safety. 2003;29(1):345-353.

44. Anderson S, Wittwer W. Using bar-code point of care technology for patient safety. Journal of Healthcare Quality. 2004;26(1):5-11.

45. Koppel R, Wetterneck T, Telles JL, Karsh BT. Workarounds to barcode medication administration systems: Their occurrences, causes, and threats to patient safety. Journal of the American Medical Informatics Association. 2008;15(4):408-423.

46. Coyle GA, Heinen M. Evolution of BCMA within the department of veterans affairs. Nurs Adm Q. 2005;29(1):32-38.

47. Fenner D. An intelligent supply chain is a unified one. MHD Supply Chain Solutions, May/June 2010, Vol.40(3), P.24. 2010;40(3):24.

48. Quinn MJ. Ethics for the information age. 5th ed. Seattle University: Addison-Wesley; 2012.

49. Christe B, Cooney E, Maggioli G, Doty D, Frye R, Short J. Management & technology. testing potential interference with RFID usage in the patient care environment... radio frequency identification. Biomedical Instrumentation & Technology. 2008;42(6):479-84.

50. Knels R, Kurz M. Improvement of the logistics in transfusion medicine and of the safety of blood transfusion by radio frequency identification. Vox Sanguins. 2005;89(1):191.

51. Goyal N. Role of information technology in donor management. Asian Journal of Transfusion Science. 2008;2(1):41-2.

52. Mehrjerdi YZ. RFID and its benefits: A multiple case analysis. Assembly Automation, 2011, Vol.31(3), P.251-262. 2011;31(3):251-62.

53. McGrady E, McGrady , Conger S, Blanke S, Landry BJL. Emerging technologies in healthcare: Navigating risks, evaluating rewards. Journal of Healthcare Management, Sept-Oct, 2010, Vol.55(5), P.353(13). 2010;55(5):353-Oct,.

54. Bassen H. An exposure esystem for evaluating possible effects of RFID on various formulations of drug products. IEEE international conference on RFID; March 26-28; ; 2007.

55. Bassen H. Liquid pharmaceuticals and 915 MHz radio frequency identification systems, worst-case heating and induced electric fields. RFID Journal [Internet]. 2005 September. Available from: http://www.rfidjournal.com/whitepapers/download/77.

56. Hohberger C, Tsirline B. Design of a 13.56 MHz segmented helmholtz coil for RF exposure testing of biologics to simulated RFID readers. International Journal of Radio Frequency Identification Technology Applications. 2009;2:65-92.

57. Davis R, Gottschall J, Gutierrez A, Hohberger C, Graminske S, Veeramani D, et al. *Absence of acute adverse in-vitro effects on aged AS-1 RBCs and thawed plasma following prolonged exposure to 13.56 MHz radio energy.*. Transfusion. 2011;in press.

APPENDIX A: TRACEABILITY MATRIX

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
T.1.1.	RFID Read/Write Fails	Handheld or pad RFID reader fails to read/write the tag for any number of reasons.	B	Design	Audible sound signaled each time tag is read/written; handheld and/or work station display is updated; error detection software included.	N/A	N/A	3.1.	N/A
T.1.2.	RFID Read/Write Fails	Tunnel reader fails to read the tag for any number of reasons.	B	Design/ Direction for Use	Tunnel reader reconciles items, flagging them as excess or missing. The operator then manually inspects contents to correct issue.	N/A	N/A	4.2.1.	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
T.1.3.	Bad data on the tag	Data is corrupted on the tag	B	Design	A new ISBT128 data structure was developed to facilitate detection of tag memory corruption.	Survivability Testing Protocol - Centrifugation; Survivability Testing Protocol - Blast Freezing; Survivability Testing Protocol - Gamma Irradiation	Survivability Testing Results	3.2. Appendix B	N/A
T.1.4.	DIN number written on tag at collection is subsequently altered	DIN field locking on the tag not enforced	B	Design	The application is configurable to allow the organization to use the DIN locking feature at the point of collection or at labeling.	N/A	N/A	Appendix B 3.2.	N/A
T.1.5.	DIN number on tags created at final labeling is altered	DIN field locking on the tag not the tag not enforced	B	Design/ Direction for Use	Programming the ISBT128 label data structure and launching the application	N/A	N/A	4.2.2. Appendix B	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
T.1.6.	ABO rewritten on tag	---	B	Design/ Direction for Use	Programming the ISBT128 ABO data structure and launching the appl9cation	N/A	N/A	4.2.2. Appendix B	N/A
T.2.1.	The maximum temperature increase of the RBCs and Platelets exceed acceptable level of 1.5 °C	RF Radiation	A	Direction for Use	Tested using Limit Test Protocol which confirmed lack of significant effect RF Radiation had on blood products.	Limit Testing - Part One - Protocol - RBCs/Platelets ; Limit Testing - Part Two - (Continuation) - Protocol - Aged RBCs/Plasma	Limit Testing - Part One - Results - RBCs/Platelets (Temperature Impact); Limit Testing - Part Two - Results - Aged RBCs/Plasma (Temperature Impact)	N/A	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
T.2.2.	The cellular and protein structures of RBCs (complete blood counts including sample weight, RBC count, Hb, Hct, MCV; potassium, aluminum; free hemoglobin; level of blood gases) are degraded or altered beyond the acceptable level of ≤1% hemolysis.	RF Radiation	A	Direction for Use	Tested using Limit Test Protocol which confirmed lack of significant effect RF Radiation had on blood products.	Limit Testing - Part One - Protocol - RBCs/Platelets ; Limit Testing - Part Two - (Continuation) - Protocol - Aged RBCs/Plasma	Limit Testing – Part One – Results – RBCs/Platelets (Cellular and Protein Impact); Limit Testing – Part Two – Results – Aged RBCs/Plasma (Biological Impact)	N/A	N/A
T.2.3.	The cellular and protein structures (Lactate, Aluminum, P-Selectin, and complete blood counts including sample weight, WBDP count, Plt, and MPV) of WBDPs are degraded such	RF Radiation	A	Direction for Use	Tested using Limit Test Protocol which confirmed lack of significant effect RF Radiation had on blood products.	Limit Testing – Part One – Protocol – RBCs/ Platelets.	Limit Testing – Part One – Results – RBCs/Platelets (Cellular and Protein Impact)	N/A	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
	that the pH decreases beyond acceptable level of ≥6.2								
T.2.4.	The maximum temperature increase of plasma types (FFP, FP24, and TP) exceeds acceptable level of 4 °C.	RF Radiation	A	Direction for Use	Tested using Limit Test Protocol which confirmed lack of significant effect RF Radiation had on blood products.	Limit Testing – Part Two (Continuation) – Protocol – Aged RBCs/Plasma	Limit Testing – Part Two – Results – Aged RBCs/Plasma (Temperature Impact)	N/A	N/A
T.2.5.	The activity of coagulation factors (PT, aPTT, Antithrombin Activity, Factor V, Factor VIII, Factor XI, Protein C, Protein S, VWF: RCo)	RF Radiation	A	Direction for Use	Tested using Limit Test Protocol which confirmed lack of significant effect RF Radiation had on blood products.	Limit Testing – Part Two (Continuation) – Protocol – Aged RBCs/Plasma	Limit Testing – Part Two – Results – Aged RBCs/Plasma (Biological Impact)	N/A	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
	levels of all types (FFP, FP24, and TP) of thawed plasma products are altered beyond an acceptable level of 20%								
T.3.1.	The time to read headers of 20-bags-equivalent exceeds maximum threshold established for specific container/reader combinations.	System Capability	A	Direction for Use	Tested using Performance Test Protocol which confirmed ability of device to sustain operational efficiency under different circumstances	*RFID Performance Testing*	*RFID Performance Testing*	N/A	N/A
T.3.2.	The time to read/write all 28 memory blocks of 20-bags-equivalent exceeds maximum threshold established for specific container/reader combinations.	System Capability	A	Direction for Use	Tested using Performance Test Protocol which confirmed ability of device to sustain operational efficiency under different circumstances	*RFID Performance Testing*	*RFID Performance Testing*	N/A	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
T.3.3.	The time to write all blocks exceeds maximum threshold established for specific container/reader combinations	System Capability	A	Direction for Use	Tested using Performance Test Protocol which confirmed ability of device to sustain operational efficiency under different circumstances	*RFID Performance Testing*	*RFID Performance Testing*	N/A	N/A
T.4.1.	The tag does not survive the process	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	B	Design/ Direction for Use	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.	Survivability Testing Protocol - Centrifugation; Survivability Testing Protocol - Blast Freezing; Survivability Testing Protocol - Gamma Irradiation	Survivability Testing Results	3.2. Appendix B	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
T.4.2.	The ability of the RFID tag to read data within 30 seconds of the start is damaged	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	B	Design/ Direction for Use	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.	Survivability Testing Protocol - Centrifugation; Survivability Testing Protocol - Blast Freezing; Survivability Testing Protocol - Gamma Irradiation	Survivability Testing Results	N/A	N/A
T.4.3.	The ability of the RFID tag to write information within 30 seconds of the start is damaged.	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	B	Design/ Direction for Use	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.	Survivability Testing Protocol - Centrifugation; Survivability Testing Protocol - Blast Freezing; Survivability Testing Protocol - Gamma Irradiation	Survivability Testing Results	N/A	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
T.4.4.	The time it takes to read the tag after it was seen for the first time (header) increases greater than 20 seconds.	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	B	Design/ Direction for Use	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.	Survivability Testing Protocol - Centrifugation; Survivability Testing Protocol - Blast Freezing; Survivability Testing Protocol - Gamma Irradiation	Survivability Testing Results	3.2. Appendix B	N/A
T.4.5.	The time it takes to read all blocks of tag memory increases by more than 45 seconds	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	B	Design/ Direction for Use	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.	Survivability Testing Protocol - Centrifugation; Survivability Testing Protocol - Blast Freezing; Survivability Testing Protocol - Gamma Irradiation	Survivability Testing Results	3.2. Appendix B	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
T.4.6.	The time it takes to write information after the tag acknowledges encoding completion of all blocks increases by greater than 75 seconds	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	B	Design/ Direction for Use	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.	Survivability Testing Protocol - Centrifugation; Survivability Testing Protocol - Blast Freezing; Survivability Testing Protocol - Gamma Irradiation	Survivability Testing Results	3.2. Appendix B	
T.4.7.	The integrity of the written data is compromised	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	B	Design/ Direction for Use	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.	Survivability Testing Protocol - Centrifugation; Survivability Testing Protocol - Blast Freezing; Survivability Testing Protocol - Gamma Irradiation	Survivability Testing Results	3.7. and Appendix B	

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
T.5.1.	Connections/communication links are lost without warning	EMI/Wireless Communication	A	Design/ Direction for Use	The HF RFID 13.56 MHz radio communication protocols as dictated by the ISO/IEC 15693 standard, as well as the ISO/IEC 18000-3 mode 1 standard, are used in the RFID readers for this application. The 16-bit cyclic redundancy check (CCITT CRC-16) is run on the message bits right from the start of the flags to the end of data and the CRC-16 accompanies the message as it is sent. Furthermore, additional protection is provided via the tag data encoding procedure.	Wireless Test Protocol	Wireless Test Summary	2.1.	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
T.5.2.	Systems experience a failure to establish communication	EMI/Wireless Communication	A	Design/ Direction for Use	The key information for safe transfusion is carried in ISBT-128 barcodes, as well as in human readable form, on the bag itself. In the event of any communication failure of the RFID system, bar code data will be used.	Wireless Test Protocol	Wireless Test Summary	2.1. and Appendix B	N/A
T.5.3.	Degradation of service/transmission of information	EMI/Wireless Communication	A	Design/ Direction for Use	The HF RFID 13.56 MHz radio communication protocols as dictated by the ISO/IEC 15693 standard, as well as the ISO/IEC 18000-3 mode 1 standard, are used in the RFID readers for this application. The 16-bit cyclic redundancy check (CCITT CRC-16) is run on the message bits right from the start of the flags to the end of data and the CRC-16 accompanies the message as it is sent. Furthermore, additional protection is provided	Wireless Test Protocol	Wireless Test Summary	2.1. and Appendix B	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
					via the tag data encoding procedure.				
T.5.4.	Delays and packet loss in the transmission of information to and from a handheld reader or a netbook/ laptop	EMI/Wireless Communication	A	Design	The WLAN communication used adheres to the IEEE 802.11b and 802.11g standards which define one Medium Access Control (MAC) layer and multiple physical layers (PHY).	Wireless Test Protocol	Wireless Test Summary	3.7.3.	N/A
T.5.5.	The wireless transmission of critical medical device alarms is disabled	EMI/Wireless Communication	A	Design/ Direction for Use	There are two steps for effective control for preventing this hazard from occurring for future acquisition or upgrading of key equipment: sourcing and procurement.	Wireless Test Protocol	Wireless Test Summary	N/A	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
T.5.6.	The transmission of physiological waveform data is impeded	EMI/Wireless Communication	A	Design/ Direction for Use	There are two steps for effective control for preventing this hazard from occurring for future acquisition or upgrading of key equipment: sourcing and procurement.	Wireless Test Protocol	Wireless Test Summary	N/A	N/A
T.5.7.	The real-time control of therapeutic medical devices is prevented	EMI/Wireless Communication	A	Design/ Direction for Use	There are two steps for effective control for preventing this hazard from occurring for future acquisition or upgrading of key equipment: sourcing and procurement.	Wireless Test Protocol	Wireless Test Summary	N/A	N/A
T.5.8.	The transmission of time-critical medical telemetry is hindered	EMI/Wireless Communication	A	Design/ Direction for Use	There are two steps for effective control for preventing this hazard from occurring for future acquisition or upgrading of key equipment: sourcing and procurement.	Wireless Test Protocol	Wireless Test Summary	N/A	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
T.5.9.	The wireless control of therapeutic devices is obstructed	EMI/Wireless Communication	A	Design/ Direction for Use	There are two steps for effective control for preventing this hazard from occurring for future acquisition or upgrading of key equipment: sourcing and procurement.	Wireless Test Protocol	Wireless Test Summary	N/A	N/A
T.5.10.	Data corruption and/or errors are produced	EMI/Wireless Communication	B	Design/ Direction for Use	The HF RFID 13.56 MHz radio communication protocols as dictated by the ISO/IEC 15693 standard, as well as the ISO/IEC 18000-3 mode 1 standard, are used in the RFID readers for this application. The 16-bit cyclic redundancy check (CCITT CRC-16) is run on the message bits right from the start of the flags to the end of data and the CRC-16 accompanies the message as it is sent. Furthermore, additional protection is provided via the tag data encoding procedure. The WLAN communication used	Wireless Test Protocol	Wireless Test Summary	3.2.	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
					adheres to the IEEE 802.11b and 802.11g standards which define one Medium Access Control (MAC) layer and multiple physical layers (PHY).				
T.5.11.	Unauthorized access during the communication between the transmitter and receiver	EMI/Wireless Communication	B	Design/ Direction for Use	Provisions in the air protocols and standards that make it difficult to inappropriately access data while the transmitter and receiver are communicating. Also, the tag structure design includes data bits stored on the tag that have an associated CCITT 16-bit CRC stored in the tag memory. Moreover, the key information for same transfusion is carried in ISBT-128 barcodes and human readable form on the bag itself. Finally, the wireless network includes data encryption security that prevents hackers from connecting to protected	Wireless Test Protocol	Wireless Test Summary	3.2.	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
					networks and stealing information.				
I.1.1.	Processing steps do not occur in sequence expected	User Error	A	Design	Finite state machine, wizard-like interfaces, and validation logic	N/A	N/A	3.7., 4.1.1., 5.0., 5.1., 5.2., 7.0.	N/A
I.1.2.	Multiple users are allowed access to update the same record	Software design or unavailable software capability	B	Design	Relational Database and Transaction Processing Techniques, ACID Properties, "All-or-Nothing" Semantics	N/A	N/A	3.7.	N/A
I.1.3.	System fails to receive timely data from an external application	Software design or unavailable software capability	A	Design	BECS interface, definition of error messages, system-level assertion, rolled back operations	N/A	N/A	7.0.	N/A
I.2.1.	User error causes data to be corrupted	User Error	B	Design	Validation logic; BECS interrogation	N/A	N/A	3.7., 7.0.	N/A
I.2.2.	Data is lost or corrupted due to hardware disk crash, other hardware or power failure	Disk crash, other hardware or power failure	B	Design/ Direction for Use	Relational Database and Transaction Processing Techniques, ACID Properties, "All-or-Nothing" Semantics; Best Practice Back-Up Techniques; SQL	N/A	N/A	3.7., 7.0.	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
I.2.3.	Data is lost or corrupted due to malfunction of program routine	Incomplete transaction	B	Design	Relational Database and Transaction Processing Techniques, ACID Properties, "All-or-Nothing" Semantics; Spotlight middleware and related relational database technology	N/A	N/A	2, 3.7., 7.0.	N/A
I.2.4.	Data encountered is outside the range of expected values	Undetected anomaly or user error	B	Design	Validation logic; BECS interrogation; reference tables; drop-down lists; error messages	N/A	N/A	3.7., 7.0.	N/A
I.2.5.	Duplicate data enters the system	User Error	B	Design	Validation logic; DIN; BECS interrogation	N/A	N/A	1.2., 3.1., 3.7., 4.1.1., 7.0.	N/A
I.3.1.	System fails to receive accurate data from the RFID reader interface	Hardware failure	B	Design	Technologies such as reader self-test diagnostics, inactivity timers, periodic heart beat signals, and positioning sentinel tags to confirm correct end-to-end operation of readers	N/A	N/A	3.2.	N/A
I.3.2.	Tag and barcode are both unreadable	Physical damage from handling product	B	Direction for Use	Product disposal	N/A	N/A	3.2. Appendix B	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
I.3.3.	Unable to read or write the RFID tag data due to a tag failure	Physical damage from handling product	B	Design	Read/Write applications; RFID TIN	N/A	N/A	3.2. Appendix B	N/A
I.3.4.	Data received from BECS does not pass correct data structure	Unrecognized data is received from BECS	B	Design	BECS interface, definition of error messages, system-level assertion, rolled back operations	N/A	N/A	7.0.	N/A
I.3.5.	Errors detected in BECS are not handled properly	Unrecognized data is received from BECS	A	Design	BECS interface, definition of error messages, system-level assertion, rolled back operations	N/A	N/A	7.0.	N/A
F.1.1.	The system is accessed by an unauthorized person	Security failure	A	Design/ Direction for Use	System Administration of user access; Spotlight Microsoft Windows.Net Authentication and Authorization	N/A	N/A	3.7.	N/A
F.1.2.	An untrained user accesses the system	System fails to prevent untrained user access	A	Design/ Direction for Use	System Administration of user access; Spotlight Microsoft Windows.Net Authentication and Authorization	N/A	N/A	3.7.	N/A

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
F.1.3.	Unauthorized personnel modify computer records	System fails to restrict access to computer records	A	Design/ Direction for Use	System Administration of user access; Spotlight Microsoft Windows.Net Authentication and Authorization	N/A	N/A	3.7.	N/A
F.2.1.	Someone other than a responsible user enters or modifies data	System fails to track persons responsible for database modifications	A	Design/ Direction for Use	System Administration of user access; Spotlight Microsoft Windows.Net Authentication and Authorization; Activity Logs/Audit Trails	N/A	N/A	3.7.	N/A
F.2.2.	Blood unit information is recorded incorrectly	System fails to record data for whole blood collection	B	Design/ Direction for Use	Validation logic; error messages and disabled proceeding; application requirements of data entry in specific order and format for particular collections	N/A	N/A	3.7., 4.1.1., 5.0., 5.1., 5.2., 7.0.	UT1, UT2, ST1, ST4, ST5, ST7, ST8, ST12, ST13
F.2.3.	Blood unit information is recorded incorrectly	System fails to capture data for apheresis collection	B	Design/ Direction for Use	Validation logic; error messages and disabled proceeding; application requirements of data entry in specific order and format for particular collections	N/A	N/A	3.7., 4.1.1., 5.0., 5.1., 5.2., 7.0.	UT3, ST2, ST3, ST4, ST5, ST9, ST10, ST12, ST13, ST15, ST16

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
F.2.4.	Blood unit information is recorded incorrectly	System fails to identify donation type	B	Design/ Direction for Use	Validation logic; error messages and disabled proceeding; application requirements of data entry in specific order and format for particular collections	N/A	N/A	3.7., 4.1.1., 5.0., 5.1., 5.2., 7.0.	UT1, UT2, UT3, UT4, UT6, UT7, UT8, UT9, UT11, UT12, ST1, ST2, ST3, ST4, ST5, ST6, ST7, ST8, ST9, ST10, ST11, ST12, ST13, ST15, ST16, ST19, ST22, ST24, ST28
F.2.5.	Blood unit information is recorded incorrectly	System fails to identify autologous donation	B	Design/ Direction for Use	Validation logic; error messages and disabled proceeding; application requirements of data entry in specific order and format for particular collections	N/A	N/A	3.7., 4.1.1., 5.0., 5.1., 5.2., 7.0.	UT4, ST6, ST11, ST22, ST24, ST28
F.2.6.	Blood unit information is recorded incorrectly	System fails to identify therapeutic donation	B	Design/ Direction for Use	Validation logic; error messages and disabled proceeding; application requirements of data entry in specific order and format for particular collections	N/A	N/A	3.7., 4.1.1., 5.0., 5.1., 5.2., 7.0.	UT4, ST6, ST11, ST22, ST24, ST28

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
F.3.1.	System fails to ensure that product is packed in the correct container	Software design or unavailable software capability	B	Design/ Direction for Use	Product code/product reference table; container properties; user packing	N/A	N/A	4.1.2.	UT5, UT6, UT7, UT8, UT9, UT11, UT12, ST1, ST2, ST3, ST4, ST5, ST6, ST7, ST8, ST9, ST10, ST11, ST12, ST13, ST15, ST16, ST19, ST22, ST24, ST28
F.3.2.	System fails to maintain appropriate container capacity for packed product	Software design or unavailable software capability	B	Design/ Direction for Use	Container properties; user packing	N/A	N/A	4.1.2.	UT5, UT6, UT7, UT8, UT9, UT11, UT12, ST1, ST2, ST3, ST4, ST5, ST6, ST7, ST8, ST9, ST10, ST11, ST12, ST13, ST15, ST16, ST19, ST22, ST24, ST28

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
F.3.3.	System fails to notify user when trying to pack an item already packed	Software design or unavailable software capability	A	Design/ Direction for Use	TID assignments; user packing	N/A	N/A	4.1.2.	UT5, UT6, UT7, UT8, UT9, UT11, UT12, ST1, ST2, ST3, ST4, ST5, ST6, ST7, ST8, ST9, ST10, ST11, ST12, ST13, ST15, ST16, ST19, ST22, ST24, ST28
F.4.1.	A container is left at the collection site	Software design or unavailable software capability	B	Design/ Direction for Use	Numerous pick-up states; disabled release until loading complete; user standard operating procedures	N/A	N/A	4.1.3., 4.1.4.	UT7, UT8, UT9, UT10, UT11, UT12, ST1, ST2, ST3, ST4, ST5, ST6, ST7, ST8, ST9, ST10, ST11, ST12, ST13, ST15, ST16, ST19, ST22, ST24, ST28

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
F.4.2.	System fails to generate a manifest	Software design or unavailable software capability	A	Design/ Direction for Use	Manifest report generation & database updating; user standard operating procedures.	N/A	N/A	4.1.3., 4.1.4.	UT7, UT8, UT9, UT10, UT11, UT12, ST1, ST2, ST3, ST4, ST5, ST6, ST7, ST8, ST9, ST10, ST11, ST12, ST13, ST15, ST16, ST19, ST22, ST24, ST28
F.5.1.	System fails to receive labeling data from BECS	Software design or unavailable software capability	B	Design	BECS interface, definition of error messages, system-level assertion, rolled back operations	N/A	N/A	4.2.2., 7.0.	UT13, ST15, ST16, ST17, ST18, ST19, ST20, ST21, ST22, ST23, ST28
F.5.2.	System fails to verify data received from BECS is written to RFID tag	Software design or unavailable software capability	A	Design/ Direction for Use	ISBT labeling; BECS interrogation; BECS interface, definition of error messages, system-level assertion, rolled back operations; user standard operating procedures	N/A	N/A	4.2.2., 7.0.	UT13, ST15, ST16, ST17, ST18, ST19, ST20, ST21, ST22, ST23, ST28
F.6.1.	Unsuitable product is released into inventory	Software design or unavailable	A	Design	BECS interface, definition of error messages, system-level assertion, rolled back	N/A	N/A	4.2.3., 7.0.	UT5, UT6, UT7, UT8, UT9, UT11, UT12, UT14,

Hazard ID	Hazardous Event	Cause	Pre-Mitigation Risk Level	Method of Control Type	Method of Control Description	Protocol Test Document	Protocol Results Document	Software Requirements Specification (SRS) Number	Unit/ System Test Number
		software capability			operations; final verification				ST1, ST2, ST3, ST4, ST5, ST6, ST7, ST8, ST9, ST10, ST11, ST12, ST13, ST15, ST16, ST17, ST18, ST19, ST20, ST21, ST22, ST23, ST24, ST26, ST28

APPENDIX B: PRE-MITIGATION RISK LEVEL A HAZARDS

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
T.2.1.	The maximum temperature increase of the RBCs and Platelets exceed acceptable level of 1.5 °C	Ensure No Adverse Effects of RFID Technology on Blood Products	Product/ Patient	RF Radiation	2	1	A	Tested using Limit Test Protocol which confirmed lack of significant effect RF Radiation had on blood products.
T.2.2.	The cellular and protein structures of RBCs (complete blood counts including sample weight, RBC count, Hb, Hct, MCV; potassium, aluminum; free hemoglobin; level of blood gases) are degraded or altered beyond the acceptable level of ≤1% hemolysis.	Ensure No Adverse Effects of RFID Technology on Blood Products	Product/ Patient	RF Radiation	2	1	A	Tested using Limit Test Protocol which confirmed lack of significant effect RF Radiation had on blood products.

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
T.2.3.	The cellular and protein structures (Lactate, Aluminum, P-Selectin, and complete blood counts including sample weight, WBDP count, Plt, and MPV) of WBDPs are degraded such that the pH decreases beyond acceptable level of ≥6.2	Ensure No Adverse Effects of RFID Technology on Blood Products	Product/ Patient	RF Radiation	2	1	A	Tested using Limit Test Protocol which confirmed lack of significant effect RF Radiation had on blood products.
T.2.4.	The maximum temperature increase of plasma types (FFP, FP24, and TP) exceeds acceptable level of 4 °C.	Ensure No Adverse Effects of RFID Technology on Blood Products	Product/ Patient	RF Radiation	2	1	A	Tested using Limit Test Protocol which confirmed lack of significant effect RF Radiation had on blood products.

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
T.2.5.	The activity of coagulation factors (PT, aPTT, Antithrombin Activity, Factor V, Factor VIII, Factor XI, Protein C, Protein S, VWF: RCo) levels of all types (FFP, FP24, and TP) of thawed plasma products are altered beyond an acceptable level of 20%	Ensure No Adverse Effects of RFID Technology on Blood Products	Product/ Patient	RF Radiation	2	1	A	Tested using Limit Test Protocol which confirmed lack of significant effect RF Radiation had on blood products.
T.3.1.	The time to read headers of 20-bags-equivalent exceeds maximum threshold established for specific container/reader combinations.	Ensure Performance Capability of RFID Tags During the Most Common Blood Supply Chain Processes	System	System Capability	1	2	A	Tested using Performance Test Protocol which confirmed ability of device to sustain operational efficiency under different circumstances

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
T.3.2.	The time to read/write all 28 memory blocks of 20-bags-equivalent exceeds maximum threshold established for specific container/reader combinations.	Ensure Performance Capability of RFID Tags During the Most Common Blood Supply Chain Processes	System	System Capability	1	2	A	Tested using Performance Test Protocol which confirmed ability of device to sustain operational efficiency under different circumstances
T.3.3.	The time to write all blocks exceeds maximum threshold established for specific container/reader combinations	Ensure Performance Capability of RFID Tags During the Most Common Blood Supply Chain Processes	System	System Capability	1	2	A	Tested using Performance Test Protocol which confirmed ability of device to sustain operational efficiency under different circumstances

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
T.5.1.	Connections/communication links are lost without warning	Ensure No Interference of RFID High Frequency (HF) and Electromagnetic Interference (EMI) with other systems	System	EMI/Wireless Communication	2	1	A	The HF RFID 13.56 MHz radio communication protocols as dictated by the ISO/IEC 15693 standard, as well as the ISO/IEC 18000-3 mode 1 standard, are used in the RFID readers for this application. The 16-bit cyclic redundancy check (CCITT CRC-16) is run on the message bits right from the start of the flags to the end of data and the CRC-16 accompanies the message as it is sent. Furthermore, additional protection is provided via the tag data encoding procedure.
T.5.2.	Systems experience a failure to establish communication	Ensure No Interference of RFID High Frequency (HF) and Electromagnetic Interference (EMI) with other systems	System	EMI/Wireless Communication	2	1	A	The key information for safe transfusion is carried in ISBT-128 barcodes, as well as in human readable form, on the bag itself. In the event of any communication failure of the RFID system, bar code data will be used.

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
T.5.3.	Degradation of service/transmission of information	Ensure No Interference of RFID High Frequency (HF) and Electromagnetic Interference (EMI) with other systems	System	EMI/Wireless Communication	2	1	A	The HF RFID 13.56 MHz radio communication protocols as dictated by the ISO/IEC 15693 standard, as well as the ISO/IEC 18000-3 mode 1 standard, are used in the RFID readers for this application. The 16-bit cyclic redundancy check (CCITT CRC-16) is run on the message bits right from the start of the flags to the end of data and the CRC-16 accompanies the message as it is sent. Furthermore, additional protection is provided via the tag data encoding procedure.
T.5.4.	Delays and packet loss in the transmission of information to and from a handheld reader or a netbook/ laptop	Ensure No Interference of RFID High Frequency (HF) and Electromagnetic Interference (EMI) with other systems	System	EMI/Wireless Communication	2	1	A	The WLAN communication used adheres to the IEEE 802.11b and 802.11g standards which define one Medium Access Control (MAC) layer and multiple physical layers (PHY).

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
T.5.5.	The wireless transmission of critical medical device alarms is disabled	Ensure No Interference of RFID High Frequency (HF) and Electromagnetic Interference (EMI) with other systems	System	EMI/Wireless Communication	2	1	A	There are two steps for effective control for preventing this hazard from occurring for future acquisition or upgrading of key equipment: sourcing and procurement.
T.5.6.	The transmission of physiological waveform data is impeded	Ensure No Interference of RFID High Frequency (HF) and Electromagnetic Interference (EMI) with other systems	System	EMI/Wireless Communication	2	1	A	There are two steps for effective control for preventing this hazard from occurring for future acquisition or upgrading of key equipment: sourcing and procurement.
T.5.7.	The real-time control of therapeutic medical devices is prevented	Ensure No Interference of RFID High Frequency (HF) and Electromagnetic Interference (EMI) with other systems	System	EMI/Wireless Communication	2	1	A	There are two steps for effective control for preventing this hazard from occurring for future acquisition or upgrading of key equipment: sourcing and procurement.

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
T.5.8.	The transmission of time-critical medical telemetry is hindered	Ensure No Interference of RFID High Frequency (HF) and Electromagnetic Interference (EMI) with other systems	System	EMI/Wireless Communication	2	1	A	There are two steps for effective control for preventing this hazard from occurring for future acquisition or upgrading of key equipment: sourcing and procurement.
T.5.9.	The wireless control of therapeutic devices is obstructed	Ensure No Interference of RFID High Frequency (HF) and Electromagnetic Interference (EMI) with other systems	System	EMI/Wireless Communication	2	1	A	There are two steps for effective control for preventing this hazard from occurring for future acquisition or upgrading of key equipment: sourcing and procurement.
I.1.1.	Processing steps do not occur in sequence expected	Prevent Sequencing Timing Error	System	User Error	2	1	A	Finite state machine, wizard-like interfaces, and validation logic

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
I.1.3.	System fails to receive timely data from an external application	Prevent Sequencing Timing Error	System	Software design or unavailable software capability	2	1	A	BECS interface, definition of error messages, system-level assertion, rolled back operations
I.3.5.	Errors detected in BECS are not handled properly	Prevent External Interface Errors	System	Unrecognized data is received from BECS	1	1	A	BECS interface, definition of error messages, system-level assertion, rolled back operations
F.1.1.	The system is accessed by an unauthorized person	Prevent Unauthorized Entry or Override of System Data	System	Security failure	2	1	A	System Administration of user access; Spotlight Microsoft Windows.Net Authentication and Authorization
F.1.2.	An untrained user accesses the system	Prevent Unauthorized Entry or Override of System Data	System	System fails to prevent untrained user access	2	1	A	System Administration of user access; Spotlight Microsoft Windows.Net Authentication and Authorization
F.1.3.	Unauthorized personnel modify computer records	Prevent Unauthorized Entry or Override of System Data	System	System fails to restrict access to computer records	2	1	A	System Administration of user access; Spotlight Microsoft Windows.Net Authentication and Authorization

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
F.2.1.	Someone other than a responsible user enters or modifies data	Prevent Loss of Traceability	System	System fails to track persons responsible for database modifications	2	1	A	System Administration of user access; Spotlight Microsoft Windows.Net Authentication and Authorization; Activity Logs/Audit Trails
F.3.3.	System fails to notify user when trying to pack an item already packed	Prevent Packing in Improper Container at Collection Site	System	Software design or unavailable software capability	1	2	A	TID assignments; user packing
F.4.2.	System fails to generate a manifest	Ensure Reconciliation of Materials from Collection Site	System	Software design or unavailable software capability	1	2	A	Manifest report generation & database updating; user standard operating procedures.
F.5.2.	System fails to verify data received from BECS is written to RFID tag	Ensure Blood Product Labeling as Data is Properly Received from BECS	System	Software design or unavailable software capability	1	2	A	ISBT labeling; BECS interrogation; BECS interface, definition of error messages, system-level assertion, rolled back operations; user standard operating procedures

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
F.6.1.	Unsuitable product is released into inventory	Prevent Unsuitable Product from Being Released to Distribution	System	Software design or unavailable software capability	1	1	A	BECS interface, definition of error messages, system-level assertion, rolled back operations; final verification

APPENDIX C: PRE-MITIGATION RISK LEVEL B HAZARDS

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
T.1.1.	RFID Read/Write Fails	Prevent Data Read/Write Error/Failure	System	Handheld or pad RFID reader fails to read/write the tag for any number of reasons.	1	3	B	Audible sound signaled each time tag is read/written; handheld and/or work station display is updated; error detection software included.
T.1.2.	RFID Read/Write Fails	Prevent Data Read/Write Error/Failure	System	Tunnel reader fails to read the tag for any number of reasons.	1	3	B	Tunnel reader reconciles items, flagging them as excess or missing. The operator then manually inspects contents to correct issue.
T.1.3.	Bad data on the tag	Prevent Data Read/Write Error/Failure	System	Data is corrupted on the tag	3	1	B	A new ISBT128 data structure was developed to facilitate detection of tag memory corruption.
T.1.4.	DIN number written on tag at collection is subsequently altered	Prevent Data Read/Write Error/Failure	System	DIN field locking on the tag not enforced	2	2	B	The application is configurable to allow the organization to use the DIN locking feature at the point of collection or at labeling.
T.1.5.	DIN number on tags created at final labeling is altered	Prevent Data Read/Write Error/Failure	System	DIN field locking on the tag not the tag not enforced	2	2	B	Programming the ISBT128 label data structure and launching the application
T.1.6.	ABO rewritten on tag	Prevent Data Read/Write Error/Failure	System	---	3	1	B	Programming the ISBT128 ABO data structure and launching the application
T.4.1.	The tag does not survive the process	Ensure RFID Tag Survivability after Experiencing the Most Demanding	System	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	3	2	B	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
		Conditions in the Blood Supply Chain						
T.4.2.	The ability of the RFID tag to read data within 30 seconds of the start is damaged	Ensure RFID Tag Survivability after Experiencing the Most Demanding Conditions in the Blood Supply Chain	System	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	2	2	B	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.
T.4.3.	The ability of the RFID tag to write information within 30 seconds of the start is damaged.	Ensure RFID Tag Survivability after Experiencing the Most Demanding Conditions in the Blood Supply Chain	System	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	2	2	B	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.
T.4.4.	The time it takes to read the tag after it was seen for the first time (header) increases greater than 20 seconds.	Ensure RFID Tag Survivability after Experiencing the Most Demanding Conditions in the Blood Supply Chain	System	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	2	2	B	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.
T.4.5.	The time it takes to read all blocks of tag memory increases by more than 45 seconds	Ensure RFID Tag Survivability after Experiencing the Most Demanding Conditions in the Blood Supply	System	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	2	2	B	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
		Chain						
T.4.6.	The time it takes to write information after the tag acknowledges encoding completion of all blocks increases by greater than 75 seconds	Ensure RFID Tag Survivability after Experiencing the Most Demanding Conditions in the Blood Supply Chain	System	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	2	2	B	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.
T.4.7.	The integrity of the written data is compromised	Ensure RFID Tag Survivability after Experiencing the Most Demanding Conditions in the Blood Supply Chain	System	Centrifugation, Blast Freezing, or Gamma Irradiation Effects	2	2	B	Tag design, tag supplier certification, and reversion to barcode only procedure in the event of tag failure.
T.5.10.	Data corruption and/or errors are produced	Ensure No Interference of RFID High Frequency (HF) and Electromagnetic Interference (EMI) with other systems	System	EMI/Wireless Communication	3	1	B	The HF RFID 13.56 MHz radio communication protocols as dictated by the ISO/IEC 15693 standard, as well as the ISO/IEC 18000-3 mode 1 standard, are used in the RFID readers for this application. The 16-bit cyclic redundancy check (CCITT CRC-16) is run on the message bits right from the start of the flags to the end of data and the CRC-16 accompanies the message as it

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
								is sent. Furthermore, additional protection is provided via the tag data encoding procedure. The WLAN communication used adheres to the IEEE 802.11b and 802.11g standards which define one Medium Access Control (MAC) layer and multiple physical layers (PHY).
T.5.11.	Unauthorized access during the communication between the transmitter and receiver	Ensure No Interference of RFID High Frequency (HF) and Electromagnetic Interference (EMI) with other systems	System	EMI/Wireless Communication	3	1	B	Provisions in the air protocols and standards that make it difficult to inappropriately access data while the transmitter and receiver are communicating. Also, the tag structure design includes data bits stored on the tag that have an associated CCITT 16-bit CRC stored in the tag memory. Moreover, the key information for same transfusion is carried in ISBT-128 barcodes and human readable form on the bag itself. Finally, the wireless network includes data encryption security that prevents hackers from connecting to protected networks and stealing

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
								information.
I.1.2.	Multiple users are allowed access to update the same record	Prevent Sequencing Timing Error	System	Software design or unavailable software capability	2	3	B	Relational Database and Transaction Processing Techniques, ACID Properties, "All-or-Nothing" Semantics
I.2.1.	User error causes data to be corrupted	Prevent Data Loss/Corruption	System	User Error	1	3	B	Validation logic; BECS interrogation
I.2.2.	Data is lost or corrupted due to hardware disk crash, other hardware or power failure	Prevent Data Loss/Corruption	System	Disk crash, other hardware or power failure	3	2	B	Relational Database and Transaction Processing Techniques, ACID Properties, "All-or-Nothing" Semantics; Best Practice Back-Up Techniques; SQL
I.2.3.	Data is lost or corrupted due to malfunction of program routine	Prevent Data Loss/Corruption	System	Incomplete transaction	1	3	B	Relational Database and Transaction Processing Techniques, ACID Properties, "All-or-Nothing" Semantics; Spotlight middleware and related relational database technology
I.2.4.	Data encountered is outside the range of expected values	Prevent Data Loss/Corruption	System	Undetected anomaly or user error	1	3	B	Validation logic; BECS interrogation; reference tables; drop-down lists; error messages
I.2.5.	Duplicate data enters the system	Prevent Data Loss/Corruption	System	User Error	2	3	B	Validation logic; DIN; BECS interrogation
I.3.1.	System fails to receive accurate data from the RFID reader interface	Prevent External Interface Errors	System	Hardware failure	2	3	B	Technologies such as reader self-test diagnostics, inactivity timers, periodic heart beat signals, and positioning sentinel tags to confirm correct end-to-

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
								end operation of readers
I.3.2.	Tag and barcode are both unreadable	Prevent External Interface Errors	System	Physical damage from handling product	3	1	B	Product disposal
I.3.3.	Unable to read or write the RFID tag data due to a tag failure	Prevent External Interface Errors	System	Physical damage from handling product	2	3	B	Read/Write applications; RFID TIN
I.3.4.	Data received from BECS does not pass correct data structure	Prevent External Interface Errors	System	Unrecognized data is received from BECS	3	2	B	BECS interface, definition of error messages, system-level assertion, rolled back operations
F.2.2.	Blood unit information is recorded incorrectly	Prevent Loss of Traceability	System	System fails to record data for whole blood collection	3	1	B	Validation logic; error messages and disabled proceeding; application requirements of data entry in specific order and format for particular collections
F.2.3.	Blood unit information is recorded incorrectly	Prevent Loss of Traceability	System	System fails to capture data for apheresis collection	3	1	B	Validation logic; error messages and disabled proceeding; application requirements of data entry in specific order and format for particular collections
F.2.4.	Blood unit information is recorded incorrectly	Prevent Loss of Traceability	System	System fails to identify donation type	3	1	B	Validation logic; error messages and disabled proceeding; application requirements of data entry in specific order and format for particular collections

Hazard ID	Hazardous Event	Safety Critical Design Requirement	Entity at Risk	Cause	Severity (1 - Negligible 2 - Minor 3- Moderate 4 - Critical)	Likelihood (1 - Improbable 2 - Remote 3 - Occasional 4 - Probable 5 - Frequent)	Pre-Mitigation Risk Level (A - Acceptable B - Tolerable C - Intolerable)	Method of Control Description
F.2.5.	Blood unit information is recorded incorrectly	Prevent Loss of Traceability	System	System fails to identify autologous donation	3	1	B	Validation logic; error messages and disabled proceeding; application requirements of data entry in specific order and format for particular collections
F.2.6.	Blood unit information is recorded incorrectly	Prevent Loss of Traceability	System	System fails to identify therapeutic donation	3	1	B	Validation logic; error messages and disabled proceeding; application requirements of data entry in specific order and format for particular collections
F.3.1.	System fails to ensure that product is packed in the correct container	Prevent Packing in Improper Container at Collection Site	System	Software design or unavailable software capability	2	2	B	Product code/product reference table; container properties; user packing
F.3.2.	System fails to maintain appropriate container capacity for packed product	Prevent Packing in Improper Container at Collection Site	System	Software design or unavailable software capability	2	2	B	Container properties; user packing
F.4.1.	A container is left at the collection site	Ensure Reconciliation of Materials from Collection Site	System	Software design or unavailable software capability	2	2	B	Numerous pick-up states; disabled release until loading complete; user standard operating procedures
F.5.1.	System fails to receive labeling data from BECS	Ensure Blood Product Labeling as Data is Properly Received from BECS	System	Software design or unavailable software capability	2	2	B	BECS interface, definition of error messages, system-level assertion, rolled back operations

CURRICULUM VITAE

NATALIE S. RAHMING
6956 North Raintree Dr., Unit B, Milwaukee, WI 53223 | 414-587-2292 | rahming@uwm.edu

EDUCATION

University of Wisconsin-Milwaukee
Ph.D. in Biomedical and Health Informatics **2012**
Dissertation: "Systematic Framework for Radio Frequency Identification Hazard Mitigation in the Blood Transfusion Supply Chain from Donor to Distribution"

University of Wisconsin-Madison
B.S. Biology **2004**
Area of Concentration: Neuroscience

University of Wisconsin-Madison
B.S. Psychology **2004**

AWARDS

UW-Milwaukee Chancellor's Graduate Student Award **January 2008 – January 2009**
Undergraduate Excellence Award **January 2004 – January 2004**
National Dean's List **2003 – 2004**
Lawton Minority Grant **2001 – 2004**
UW-Madison Chancellor's Scholarship **January 2000 – January 2004**

TEACHING EXPERIENCE

University of Wisconsin-Madison
Instructor – Neuroscience, PEOPLE Program **2004**

- Designed course structure
- Provide students with lectures geared toward learning, memory, and the senses
- Lead dissections of the sheep brain and cow eye
- Supply numerous worksheets and assignments on brain anatomy and physiology

RELATED EXPERIENCE

General Electric (GE) Healthcare, Wauwatosa, WI **2011 – Present**
Data Governance Analyst

- Lead development and implementation actions for effective execution of aggregate spend tracking and monitoring reports.
- Organize and oversee owners and activities fundamental to the successful implementation of the Research Module of the Aggregate Spend Tool.
- Manage and launch data governance program for the Aggregate Spend Tool in order to ensure that data of the highest integrity is tracked, maintained, and reported.
- Direct, organize, coordinate, and plan user testing and system evaluation in preparation for system launch.
- Combine business policy and system design into functional, documented procedures.
- Compose and organize system requirements and specifications for successful system construction.

Medical College of Wisconsin, Milwaukee, WI **2005-2011**
Data Coordinator/Clinical Research Coordinator II

- Coordinate research protocols and projects
- Monitor and report data quality metrics and trends
- Develop and manage data governance issue log to capture, analyze and remediate issues
- Assure compliance with all relevant Internal Review Board's rules and regulations
- Recruit, screen, enroll, and obtain consent from participants
- Collect, analyze, maintain, and disseminate data
- Assist director with implementation of LEAN Six Sigma into the Neurosurgery Dept.

University of Wisconsin-Milwaukee, Milwaukee WI **2011 – 2011**
Student – Norris Health Center Practicum

- Document current operations and organization culture of Norris Health Center
- Assist in the formulation of a current state analysis
- Provide a recommendation for an Electronic Medical Records solution

Brynwood Country Club, Milwaukee, WI **1998 – 2007**
Server

- Take and distribute orders in a fast paced environment
- Banquet setup and break down
- Maintain sanitation and miscellaneous office duties

University of Wisconsin-Milwaukee, Milwaukee, WI **2004 – 2004**
Vice Chancellor Summer Intern

- Support objectives and functions of department
- Plan and organize meetings with community partners
- Aid Vice Chancellor on projects and with collaborations

UW-Hospital, Madison, WI **2003 - 2004**
Clinical Research Assistant (Neuropsychology)

- Administer cognitive assessment batteries to research participants
- Score level of cognitive ability in participants
- Maintain accuracy of files and database with participant information
- Recruit, screen, enroll, and consent patients

Time Warner Cable, Milwaukee, WI **2002 - 2002**
Summer Intern

- Data entry, handling, and resolving customers' problems
- Upgrading customers' service with new, innovational equipment
- Emphasis on customer service and communication skills

PUBLICATIONS AND PAPERS

"EMR Practicum at University of Wisconsin-Milwaukee
American Medical Informatics Association (AMIA) – Abstract **2011**

MEMBERSHIPS

Golden Key International Honor Society
Phi Kappa Phi Honor Society
Phi Delta Sigma Honor Society
Delta Sigma Theta Sorority, Inc.