

**Risk Assessment
for the MiniBooNE Detector Data
Acquisition, Storage,
and Monitoring System
[ID 993]**

Prepared by: _____ Date: _____

System Coordinator
Ray Stefanski

Approved by: _____ Date: _____

System Owner
Steve Brice

Approved by: _____ Date: _____

GCSC
Jason Heddon

Approved by: _____ Date: _____

Division Head
Victoria White

1. SYSTEM IDENTIFICATION

1.1. System Name/Title

Fermilab Experiment E-898/944 - MiniBooNE.(MiniBooster Neutrino Experiment) is responsible for the system discussed throughout this risk assessment. Fermilab Identifier CSP-MA-993 has been assigned to the system and will be referred to as the MiniBooNE data acquisition, storage and monitoring system, or MBDAQ.

1.2. System Type

This system is a Major Application (MA) and is contained in the General Computing Enclave

1.3. OMB 53 Exhibit Information

This system is contained in OMB 53 Exhibit “FNAL IT and Cyber Security Information Systems”, 019-20-01-21-01-XXXX-00-404-138.

1.4. Responsible Organization

Fermi National Accelerator Laboratory
PO Box 500
Batavia, IL 60510

1.5. Information and Security Contact(s)

Security contacts are given in table 1. The system manager is registered in the MISCOMP database. The GCSC is identified at <http://computing.fnal.gov/security/contacts.html>

Table 1, security contacts for the MBDAQ:

Title	Name	Email	Telephone
System Owner	Steve Brice	sbrice@fnal.gov	630.840.8748
Management Contact	Ray Stefanski	stefanski@fnal.gov	630.840.3872
MA Coordinator	Chris Green	greenc@fnal.gov	630.840.2167
System Manager	Amber Boehnlein	cope@fnal.gov	630-879-5105
GCSC	Jason Hedden	jhedden@fnal.gov	630-840-6669
Physical Key Holders	MBCR Operator	www-boone.fnal.gov	630.840.2757
	MCR Crew Chief	www-bd.fnal.gov	630.840.3721

1.6. System Operational Status

The MBDAQ is in the Operational phase of its life-cycle.

1.7. Information Gathering Technique

This assessment was carried out by the preparer, and vetted with document review by system experts and users.

1.8. General Description/Purpose

This system provides for data acquisition, storage and monitoring for MiniBooNE. MinibooNE is a neutrino experiment that runs in the Booster Neutrino Beam (BNB) – a facility roughly consisting of a target to produce secondary particles, and a magnetic horn to focus the beam to a detector that resides at the MiniBooNE detector building (MDB).

1.9. System Description and Boundaries

1.9.1 System Description

MiniBooNE operates from a control room located in WH10W, where operators observe and monitor the beam, horn and detector. Control and operation of the proton beam and horn are in the hands of the Main Control Room operators, who cooperate with the MiniBooNE operators in finding and resolving problems. We can think of operations in two parts: control or, more accurately, monitoring of the beam and experiment, and data acquisition, which requires high bandwidth transfer of information from the beam and detector to the data storage center at the Feynman Computing Center, FCC. A third component of the system involves data storage in the Enstore facility at the FCC. MiniBooNE also uses terabyte servers for storage of processed data and simulated events. The computers involved in monitoring, data acquisition and data storage are listed in table 2.

The main DAQ computers are located at the MDB. Two additional DAQ machines are located in the BNB and collect data from the Resistive Wall Monitor (RWM - measures proton beam intensity and timing) and the Little Muon Chamber (LMC – detects muon flux in the neutrino beam), which are located in MI12 and MI13A respectively. Data from these computers are transmitted to the MDB where the HAL9002 and HAL9004 collect all of the data and send it to Enstore.

The Monitor computers are standard PCs that have redundant functions. These computers are used to collect and present data to the operators in a coordinated fashion. Loss of any one of these computers is easily replaced with data collected by other computers, so that the operation of the beam or experiment is not dependent on them.

1.9.1 System Boundaries

The boundary of MBDAQ is at its network interface which connects the devices in Table 2 to the General Computing Enclave.

Table 2: List of computers in the MiniBooNE DAQ, data storage and monitoring systems.

Type	System Name	Purpose	Location	Owner	Computer Specs
DAQ	hal9000	Will be replaced by mbdaq01.	MBD	Fermilab	VALINUX; 2230
DAQ	mbdaq01	Will replace hal9000.	MBD	Fermilab	KOI: D-X-3200-2U-RM
DAQ	southport	Backup for mbdaq01; Currently serves as hal9004 replacement.	MBD	Fermilab	POLYWELL: 935X4A
Near-Line	hal9002	DAQ coordinator-will be replaced.	MBD	Indiana U.	PENGUIN: REL110-D-P3-1000-RM
Near-Line	hal9004	Died - temporarily replaced by southport.	MBD	Indiana U.	PENGUIN: REL110-D-P3-1000-RM
Near-Line	mbnl01	Will replace hal9004.	MBD	Fermilab	KOI: D-X-3200-1U-RM
DAQ	damen	Booster Neutrino Beam ACNET DAQ.	MBD	LANL	DELL" OPTIPLEX GX150
DAQ	dorchester	LMC DAQ	MI13A	U. of Colorado	DELL: POWER EDGE 2650
DAQ	walcott	RWM DAQ	MI12	LANL	DELL: DIMENSION XPS
DB Server	mbdb01	DB Server	FCC/2/218	Fermilab	KOI: D-X-3200-1U-RM
CR Terminal	colfax	MBCR Detector Monitor	WH1050	U. of Colorado	DELL: PRECISION WORKSTATION
CR Terminal	Magnolia	On-line eventy display/Booster monitor.	WH1050	Fermilab	DELL: PRECISION WORKSTATION
CR Terminal	cns22pc	MBCR ACNET monitor.	WH1050	Fermilab	GATEWAY: E4200-800P3
MI12 Terminal	hotspur	Horn monitor	MI12	Fermilab	DELL: XPS-T800_MT
Data Storage	mbdata05	Terabyte File Servers	FCC/2/218	Fermilab	On Order.
Data Storage	mbdata04	Terabyte File Servers	FCC/2/218	Yale	POLYWELL: D-X-3.2G-SATA-5U
Data Storage	mbdata03	Terabyte File Servers	FCC/2/218	Fermilab	POLYWELL: 2*X-3.06G-5U-RM
Data Storage	mbdata02	Terabyte File Servers	FCC/2/218	Fermilab	POLYWELL: 2*3.06G-XEON-4U-RM
Data Storage	mbdata01	Terabyte File Servers	FCC/2/218	Fermilab	POLYWELL: 2*3.06G-XEON-4U-RM
Data Storage	lake	Terabyte File Servers	FCC/2/218	Fermilab	POLYWELL: 2*3.06G-4U-RM
Data Storage	bishopford	Terabyte File Servers	FCC/2/218	Fermilab	POLYWELL: 935X8
Data Storage	edens	Terabyte File Servers	FCC/2/218	LANL	POLYWELL: 935X8
Data Storage	kingery	Terabyte File Servers	FCC/2/218	Princeton U.	POLYWELL:n2*-2.4G-3.8T-5U-RM
Data Storage	danryan	Terabyte File Servers	FCC/2/218	U. of Michigan	POLYWELL: 935X8
DB DataBase		RWM Resitive wall Monitor	MI12	BNB Service Building	
DAQ Data Acquisition		LMC Little Muon Counters	MI13A	Counting House for the LMC	
MB MiniBooNE		CR Control Room	MBD	MB Detector Building	
ACNET Accelerator Control Net					

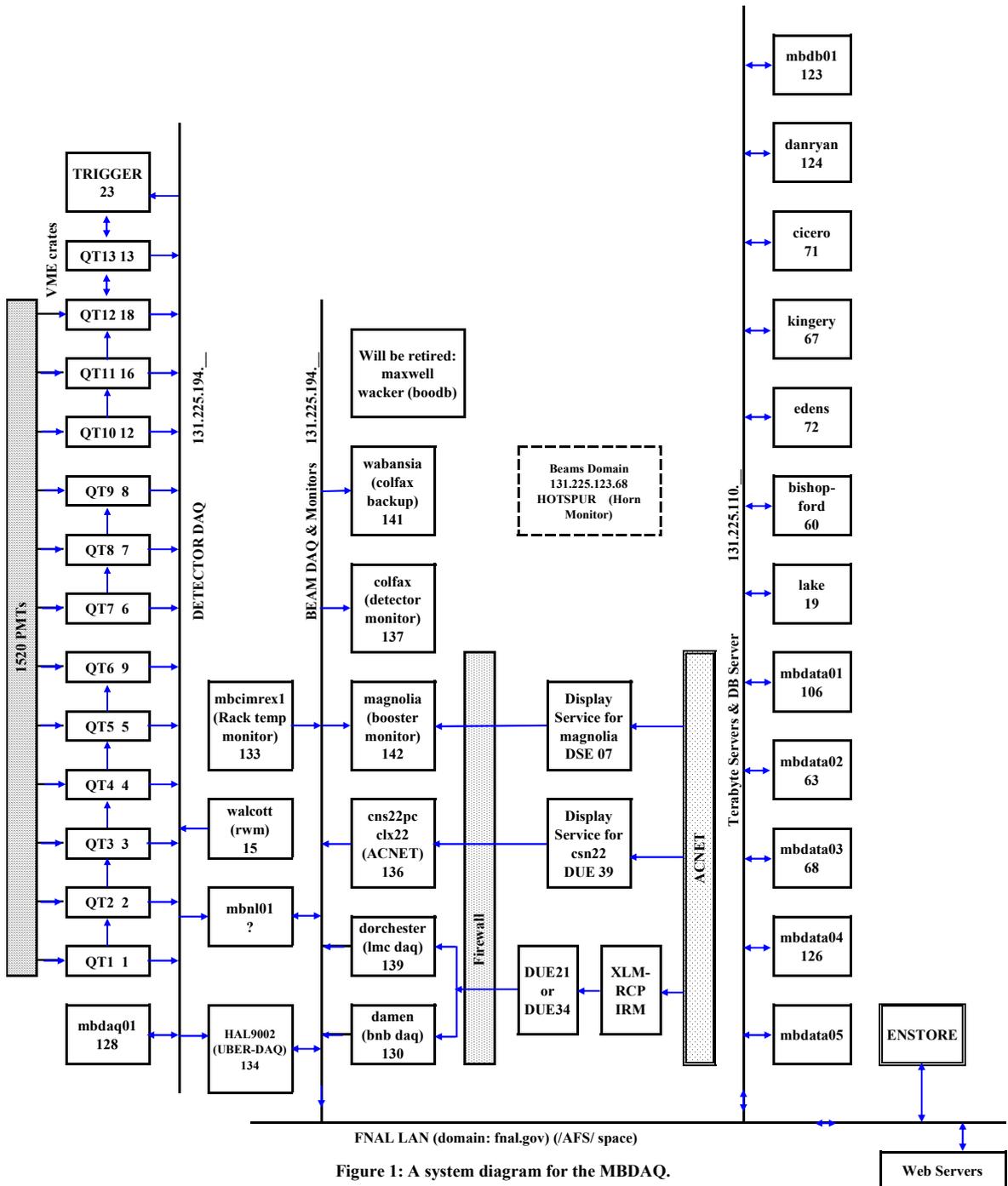


Figure 1: A system diagram for the MBDAQ.

1.10. Information Sensitivity

The data sensitivity on the MiniBooNE data acquisition, storage and monitoring system is classified in the following table:

Relative Importance of Protection Needs			
	HIGH (Critical Concern)	MEDIUM (Important Concern)	LOW (Minimum Concern)
Confidentiality			X
Integrity			X
Availability			X

The information available in the MBDAQ is relevant only to the physicists using the data. It has no relevance beyond the basic science carried out by the experiment.

1.11. Privacy Impact Assessment (PIA)

This system will not collect Personal Identification Information and no PIA is required.

2. Threat Identification

Risk is the potential for a threat-source to successfully take advantage of system vulnerability. Vulnerability is defined as a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present risk when there is no vulnerability that can be exercised.

2.1. Threat Source Identification

There are no threat sources which have not been identified in the Risk Assessment for the General Computing Enclave.

2.2. Motivation and Threat Actions

There are no motivations or threat actions which have not been identified in the Risk Assessment for the General Computing Enclave.

3. Vulnerability Identification

MiniBooNE protects data from corruption from any one of several sources:

- a. Misuse of the MBDAQ by terminal access:
 1. from outside of Fermilab.
 2. from inside of the Lab.
 3. by trespassers.
 4. due to operator error
 5. during data analysis.

- b. Malfunction of MBDAQ or supporting systems that lead to
 1. loss of original, unprocessed data from the experiment;
 - i. due to aging, or lack of current updates
 - ii. due to the unavailability of Enstore.
 2. loss of processed data from the experiment;
 - i. due to a failure of one of the terabyte servers.
 - ii. due to an analyst failure to create backups.

4. Control Analysis

Mitigation A1: User access is limited to individuals with an account on FNALU, a Kerberos password, and an account on the BooNE cluster. The MiniBooNE computer coordinator assigns accounts on the BooNE cluster.

Mitigation A2: Access to the location of computers in the MBDAQ is restricted to individuals with a key that can be obtained either from only from the MBCR (MDB) or the MCR (MI12 or MI13). The Computer Division System Management also has a key.

Mitigation A3: Computers in the MBCR are monitor computers only, and are not used in the DAQ process as such. A trespasser could have access to these machines when the operator is not present. The potential for loss is avoided because the essential files are stored on machines in the 194 subnet and are backed up on mirror drives.

Mitigation A4: No operator intervention is required in the data acquisition process, so corruption of data due to this source is unlikely.

Mitigation A5: Corruption of data during analysis is not likely, because data cannot be written into Enstore by a data analyzer. Only the Data Acquisition computer, Hal9002/4, can write into Enstore. There is no other mode available to write to Enstore. Data stored in the Terabyte servers can be reconstructed from Enstore when necessary, so does not represent a threat of loss.

Mitigation B1-i: the main data acquisition computers (Hal9000/2/4) and local data storage are kept in climate controlled racks, and have uninterruptible power sources. It's known that power cycling can shorten equipment lifetime, so this equipment is never turned off. The strategy is to keep the computers on and running cool to maximize lifetime. Furthermore, these computers are being replaced by more modern machines running under the current Fermilab Linux Operating System so that the security systems are integrated with the general computing enclave..

Mitigation B1-ii: Data is stored in a buffer (Hal9002/4) as the experiment is run. From the buffer it is transmitted to Enstore. The buffer is sufficiently large to store several days of normal data acquisition. This has proven to be adequate protection against a failure in the Enstore system, and no data loss has occurred due to this vulnerability.

Mitigation B2-i: Processed data and simulations are stored in the Terabyte servers. The servers are RAID arrays of about ten hard-drives apiece. A single server can hold several terabytes of data. The server could lose an entire store of data if two of the hard drives in the set fail simultaneously, since that causes the server to lose control of the array.

Mitigation involves:

1. Maintaining at least two spare hard drives for each server.
2. Monitoring the servers with a continuous monitoring system (Big Brother).
CD personnel are ready to replace a failed drive typically within 24 hours, including weekends and holidays.

Mitigation B2-ii: Individuals that write applications and process data for MiniBooNE, are responsible for protecting their data by using CVS or by taking advantage of appropriate backup opportunities.

5. Likelihood Determination, Impact Analysis, and Risk Level

Risk is related to the likelihood of occurrence of a failure due to a vulnerability or weakness in the system, and the related impact. We use Table3 to define risk and the dependence of risk on likelihood and impact.

Definitions:

- A. Low implies less than ten occurrences in one year,
- B. Very low means less than one occurrence in one year,
- C. Extremely low means less than one occurrence in five years.

Table 3: Risk Analysis:

Threat Likelihood	Impact		
	Low	Medium	High
Low	Low	Low	Low
Medium	Low	Medium	Medium
High	Low	Medium	High

Table 4: Risk Analysis applied after mitigation:

Threat Likelihood	Low	Very Low	Extremely Low
A1			X
A2			X
A3			X
A4		X	
A5			X
B1-i			X
B1-ii			X
B2-i		X	
B2-ii		X	

5.A.1 Misuse of the MBDAQ by users from outside Fermilab:

Access to the Fermilab computing environment is controlled by the Security Plan for the General Computing Environment, which applies to the MBDAQ. To access the MBDAQ, users must also possess an account on the BooNE cluster. The computers directly involved in data acquisition are further protected by residing on a not-accessible network. The risk is extremely low.

5.A.2 Misuse of the MBDAQ by users from within Fermilab:

Access by computer within the Lab is restricted to employees with an account on the BooNE cluster. Access keys are issued to Fermilab employees only if they are on a list of qualified users. The risk due to loss of data because of an accidental or forced access by a Fermilab employee is extremely low.

5.A.3 Misuse of the MBDAQ by trespassers:

The MBDAQ is open to visitors at all times, and is usually occupied by an operator. During normal working hours there are a sufficient number of experimenters on the floor that a negligent use of the MBDAQ is not likely. The time of vulnerability is during off-hours, when the operator leaves the control room. The probability of occurrence is very low, but not negligible. (Computer theft has been known to occur at the Lab in off-hours.) The risk is considered to be extremely low.

5.A.4 Misuse of the MBDAQ due to operator error:

The process of acquiring data from the experiment is fully automated, including data acquisition from beam devices and the detector itself. The risk of data loss due to

operator error is very low. (Except for one week of running that was compromised because no-one recognized that the horn timing was off.)

5.A.5 Corruption of data during analysis:

Aside from the possible loss of a tape in Enstore, which represents a small part of the MB data set, loss of data from this source is unlikely. The risk is considered to be extremely low.

5.B.1-i Loss of original data due to equipment failure:

Some of the computers are old, and are being replaced with modern machines, currently up-to-date OS, and mirrored disk systems. This category is considered extremely low risk.

5.B.1-ii. Loss of original data due to failure of the data storage devices.

The data storage backup system at the MDB has been very reliable and the risk associated with this source is considered to be extremely low.

5.B.2-i. Loss of processed data due to failure of the data storage devices.

The administrative system that is implemented to avoid a catastrophic loss of a terabyte server has worked well. However, the installation of a hot-spare would remove any remaining vulnerability, and should be given serious consideration. The risk is rated as very low.

5.B.2-ii. Loss of processed data due to failure by an analyst:

The responsibility for protecting data lies with the analysts, all of whom are highly qualified. The risk is considered very low.

5.C Conclusions

As applied to the MBDAQ, all instances of identified threat likelihood are very low, and therefore any potential impact would also be very low.

6. Control Recommendations

No additional controls are recommended at this time.

7. Residual Risk

There are no residual risks at this time.