Tevatron Collider Experiment Vulnerability Review

Committee:

Dan Green (Chair)
Alan Bross
Irwin Gaines
Bob Kephart
Rob Kutschke
Jim Patrick
Dan Wolff

Charge:

Conduct a review to identify vulnerabilities in the detector hardware and software systems. Things we have in mind are points of failure which could result in long term crippling of the detectors, or irreparable damage to critical software components. The issues should be graded in terms of the potential negative impact on the experiment.

Class I - major impact (12 months)
Class II – serious impact (6 months)
Class III – moderate impact

While the primary goal is to identify the vulnerabilities, the committee may also comment on possible remediation.

We imagine the review to be conducted by relatively focused meetings between the review committee or parts thereof and knowledgeable people on the experiments.

A report by September 1 or soon thereafter is desired.

Meetings:

The Committee met twice by itself in order to self organize. In parallel the point of contact to CDF, Mike Lindgren, and to D0, George Ginther, were contacted and made aware of the charge to the committee.

A short meeting between the Committee Chair and the Spokespersons of CDF and D0 was also held on July 23 to make sure that the Committee and the experiments were in full synchronization.

At the first Committee meeting of July 10, we agreed to explore the experimental vulnerabilities as a coherent body. It was also agreed that the Chair would solicit

from each experiment their self assessment of their specific vulnerabilities. In addition, issues of data storage beyond the confines of the experiment halls were defined to be outside the charge of the Committee as were vulnerabilities of the Tevatron itself. The outcome of the first meeting was a list of vulnerabilities common to both experiments and a short list of accelerator vulnerabilities. In addition, some CDF and D0 specific items were enumerated.

The experiments responded with documents describing their vulnerabilities. CDF gave the Committee documents specific to the Silicon Vertex Detector, the Central Outer Tracker (COT), and an overall vulnerability self-assessment. D0 also sent a document describing their specific vulnerability self-assessment.

A second meeting of the Committee on Aug. 3 served to digest this input. The working spreadsheet listing common and experiment specific issues was then updated. The Committee was also sent a report on Accelerator Vulnerabilities authored by Tom Dombeck. Based on this document, the decision to keep most accelerator issues beyond the purview of this Committee was reaffirmed.

The revised spreadsheet was communicated to the CDF and D0 points of contact. The Committee decided to take advantage of the shutdown to visit the experiments and "kick the tires". The Committee visited D0 on Aug. 16 and CDF on Aug 17. In both cases the Committee was able to tour the experimental detector hall and the off-detector electronics used for trigger and data acquisition. During both visits relevant experts from the experiment were on hand to answer the questions posed by Committee members. At the end of each visit the Committee had a chance to discuss in detail any remaining questions with the experts on each experiment.

Each experiment supplied their assessment of the Class/Impact of the listed vulnerabilities. In addition, it was decided that the impact had to be "weighted" by the probability. Each experiment also made their own evaluation of the probability of occurrence of each item in their list.

Findings:

Quite generally, both CDF and D0 have given considerable thought and attention to the possible vulnerabilities which exist in their respective experiments. In almost all cases, mitigating design and actions have been taken.

Both experiments feel that there has been and continues to be sufficient budget authority for the purchase of safety equipment and purchasable spares. Fire protection has been well thought through. Rack protection of the on-detector and counting room electronics has been properly carried out in both cases.

Procedures were found to be in place for routine actions such as access, repair and shutdowns.

For both CDF and D0 there were major worries about the silicon detectors/beam pipe and some issues with the solenoid magnets. Other systems were thought to be less likely to cause major negative impacts on the continued operation of the experiments.

Both experiments felt that there were issues of keeping a sufficient inventory of electronic spares since in some cases there were non-commercial and unique, critical, objects. For example, there are few spares (1 ?) in CDF or D0 for the master accelerator clock fanout.

Both CDF and D0 were worried about the shrinking base of expertise available to the experiment. CDF were most worried about inexpert people working on M&O activities and making a catastrophic error due to inexperience; an example is their silicon system for which they have lost most expertise. For D0 the stress was slightly different. They felt their ability to recover fully and expeditiously from unusual conditions might be seriously compromised by limited availability of expertise with detailed knowledge of the detectors.

Recommendations:

These recommendations are in priority order as defined by the Committee.

- **As the issue of "institutional memory" and turnover of skilled personnel is a major problem, the experiments should examine the existing documentation and procedures and assess if it is sufficient. The experts should be prevailed upon to write sufficiently detailed and comprehensive procedures. The addition of "what not to do" items would be useful. In addition →**

- **The Laboratory should consider authorizing CDF and D0 to each make one or two targeted new hires at the Associate Scientist or Senior Engineer level to fill critical holes in their operations and to increase the depth and expertise of people responsible for critical systems. Both experiments felt that the silicon systems were the most vulnerable to the loss of skilled personnel. Both experiments have seen a reduction of operating staff as Run II becomes "asymptotic". FNAL should insure that staffing levels do not fall below a critical point as experts in CDF and D0 move on to other tasks.**

- **The experiments should review access to critical systems and implement any additional needed training updates to further reduce the possibility of operator error.**

- **The experiments should act to insure that all test stands and test procedures for legacy electronics are in place and functioning. Both experiments have a few critical modules in the trigger/DAQ systems that should be well documented and with backup spares made available.**

- **The experiments should make sure that legacy computers, operating systems and code are in place for maintenance and reprogramming of specialty firmware and FPGA.**

- **The Laboratory management should consider whether it is cost effective to have an expert review of the ensemble of fire protection systems at CDF and D0. The Operations Heads of the experiments should be informed of alarms, interlocks, fire safety system tests and status performed by all organizational entities cutting completely across the Laboratory as they inform on the status of the integrity of the experiments.**

- **The experiments should make sure that spares for critical systems, e.g. clock fanout, are sufficient.**

- **The experiments should check the infrastructure systems for aging, e.g. cooling lines and heat exchangers, on a regular basis.**

Vulnerabilities Spreadsheet:

Tevatron Collider Experiment Vulnerabilities

	Subsystem	Vulnerability	Impact/Class	Mitigation	Probability	Added Mitigation?
Accelerator						
	Previous Accelerator study	Assessment done		Outside of this scope		
	Low beta failure	Tevatron program interrupted		Install the sole spare		Procure additional spare
	Major beam loss	Large fraction of Si destroyed		Beam DCS. Loss monitors		
	Accident or death, lab stands down	Loss of data taking for extended period		FNAL safety training		
Common			see CDF/D0 below			
	Fire protection systems	Fire suppression systems fire by mistake due to aging or pilot error		Scheduled exercise of systems. Improved documentation		
	Detector Control System failure	Voltage, temp uncontrolled/iunmonitored				
	Detector Safety System failure	Accident condition develops				
	Data loss at Feynman	Assume covered by CD		Outside of this scope		
	Loss of institutional memory					
	Software upgrade is required,	Unsupported software no longer works		Training for new students/postdocs.		better written procedures
	Not enough people to do analysis or run	Reduced ability to do complete analysis of all topics		Focus on "discovery" physics - prioritize		
	Loss of technical expertise	Major accident occurs due to insufficient expertise		Increased recruiting and proactive training of new people		Assign/hire added tech help
	FPGA requires replacement/upgrade	Obsolete computer, op system, legacy code		Must "warehouse" computers, op systems, code		purchases
	Test stands for ASICs/boards	Lost ability to test/repair devices		Must store and document all test stands and procedures		purchases
CDF Specific						
	Be Beam pipe	Failure ->install spare, impact on Si	3	Contained in COT - training and access limited to experts	moderate	new beampipe?
	Magnet	Thermal shock opens major Watt can leak	1 to 3	Good proceedures for power outage and recovery, training	moderate	run magnet without secondary
	Magnet	Thermal cycle opens up internal leak	1 to 3	avoid thermal cycles	low	live with leak or fix it
	Magnet	Mistake causes open circuit in dump resistor or buss, HV arc to ground	1	Good proceedures for power supply, maintenance, training	low	
	Magnet	Aging of support o-rings causes major leak	3	monitor secondary vacuum vs time	low	
	Si Vertex	Cooling leaks are systemic	3 or less		moderate	
	Si Vertex	Interlocks defeated by mistake, Si burns up	1	Limited access to interlock controls, documentation of "what if"	low	
	Si Vertex	Resonant condition in DAQ damages many bonds	1 to 3	DCS - alarma and limits	low	
	COT	Loss of large sectors of wires	1 to 3	Plan for wire repair developed	low	
	COT	Aging of wires accelerates	1 to 3	Monitoring the gas, improved filtration	low	
	Calorimeter	Large He release damages phototubes	1-2	Testing ventilation system, N2 purge on PMT ?	low	
	Endplug	Move by inexperienced people crushes Si and COT micro-coax	3	Restrict access to trained people	low	
	Muon	Lower yoke muon chambers flooded	2 or less	Schedule for sump tests	low	
	LV Supplies	Fans reach end of lifetime on Caen supplies	Less than 3	MTBF analysis made. DCS - temp monitor. Halon system	moderate	
	LV, HV	End of lifetime loss of LV modules	Less than 3	Rack protection system, FIRUS. Fused, DCS, spares	low	
	Electronics Spares	End of lifetime loss of TDC boards	Less than 3	Define reduced channel set requiring timing?	low	
	LN2, LHe, Gases	Failure of supply	1 to 3	Spare inventory on site - tube trailers	low	
	AC Power	Loss of 1500 KVA transformer	Less than 3	Spare exists	moderate	
D0 Specific						
	Be Beam pipe	Failure of the pipe - spare does not accommodate L0	3	Limited access, training of personnel	low	new beampipe
	Magnet	Resistive joint - degrade during warmup	at least 2	Stay cold, 3000 l LHe inventory and 24/7 operator coverage	low	additional cold compressor
	Si Vertex	Continued degradation of disks	*	Backup chiller,	high	
	Si Vertex	Leaks due to joint failure and/or corrosion, damage	likely 3 or less	Monitor coolant conductivity, sub atmospheric operation	low	
	Si Vertex	Shorts	*	Dry gas purge, backup tube trailer	low	
	Fiber tracker	Un-planned warm-up of VLPC system leading to large loss of channels	*	Temp sensors, alarms and limits	low	
	LAr Calorimeter	Contamination of LAr supply due to cryostat failure	3	Alarms. Tests of new inventory - "canaries".	low	LAr inventory
	Muon	Failure of gas recirculation	3 or less	Backup bottled gas. Monitor new gas with "canaries".	low	additional gas inventory
	Trigger	trigger framework and master clock concentrated in single location	3 or less		low	build spare(s)
	DAQ-Online	fire or power glitches	3 or less		low	
	LV, HV	Cooling interlock failure, smoke detection failure, HALON failure	likely less than 3	Scheduled maintenance. Tests of DCS, DSS systems	moderate	
	Electronics Spares	Major accident - insufficient spares	potentially 3 or worse	Increased inventory. "warehousing"	low	additional spares inventory
	AC Power	Glitches interruptions	generally less than 3	DCS on UPS, backup generator	high	
	Air for controls	Compressor failure	less than 3	Tube trailer backup, alarms, autodialers	moderate	
	Cable bridge	Rigging accident	3 or worse	Control of rig locations. Increased training of responsible people	low	

* Impacts detector efficiency but probably does not result in major subsystem loss