USEC, Inc.

Independent Engineer's Interim June-11, 2011 Incident Evaluation Report

Matching Order No.
DE-MO01-09CF02009

July 2011 DRAFT

prepared by

}

in support of a

Loan Guarantee Application
for the
U.S. Department of Energy
Loan Programs Office

OFFICIAL USE ONLY

Pursuant to Title XVII of the Energy Policy Act of 2005
and the American Reinvestment and Recovery Act of 2009

of such data is not limited to the DOE Loan Guarantee Applicant for which Matching Order No. DE-MO01-09CF02009 was issued to this Independent Engineer.

Appendix XX Interim IE Incident Evaluation Report for June 11, 2011 Multiple Crash Incident at USEC Piketon

Executive Summary

Six centrifuge crashes occurred on June 11, 2011 at the United States (U.S.) Enrichment Corporation (USEC) Piketon Ohio (OH) American Centrifuge Plant (ACP) facility, two in Lead Cascade one (LC-1) and four in LC-3, with 38 total machines in operation at the time. The U.S. Department of Energy Loan Programs Office (DOE LPO) was promptly informed by USEC management following the multi-crash incident, and subsequently two members of the Independent Engineer (IE) team were sent to Piketon to observe the incident investigation and determine what meaning these crashes had for the USEC loan guarantee application. IE staff evaluated the USEC incident investigation as it progressed over several weeks and prepared this interim IE incident evaluation report as an eventual Appendix for inclusion in an updated IE Report (IER). A final IE incident evaluation report is planned to include final machine technical analyses that address potential centrifuge design changes that are still being evaluated.

The incident was unlike the previous machine crashes which were investigated by the IE at K-1600 in February and March of this year. Instead, they involved multiple problems occurring during the same incident. These problems involved electrical failure, backup diesel generator startup problems, cooling water pump problems, human operator error involving the Uninterruptible Power Supply (UPS) that controls much of the communication, valving, vacuum, and centrifuge controls, lack of procedures for some power problem situations, lack of preparation for communications restart, and an unexpected mode of centrifuge failure. The complexity of the situation required significantly more IE review than the previous incidents, and it has significantly more implications for the future commercial plant.

Details of the incident are presented in this report, and an overview is given here.

- The root cause of the incident was the shorting of a stab connector to a busbar in the Electrical Motor Control Center (EMCC) electrical panel. This might have been prevented if industry-standard Preventive Maintenance (PM) had been performed, although there were good reasons to use a lesser PM.
- The Diesel Generator (DG) was not immediately able to supply replacement power and had problems with accepting the required load that had been known and not addressed for some time.
- Ergonomic conditions, lack of procedures, and inadequate training for silencing UPS alarms resulting from the repeated attempts to restart the DG resulted in an inadvertent emergency shutoff of the UPS, compounded by a lack of procedures or documented information on how to restart it. The UPS restart was complicated by the power situation, and was only accomplished after more time had elapsed.

- When the Distributed Control System (DCS) was resupplied with power from the restarted UPS, three of the four communication servers were in idle and unavailable for use. A lack of procedures and training prevented these from being used rapidly, resulting in more time delays.
- During the time delays involved in this evolution, six machines failed in crash mode.
- One machine breached, which had not been observed since 1977. This is a more serious crash mode than any other witnessed during the USEC program.
- Problems were magnified by mis-installation of Machine Cooling Water (MCW) valves that was not detected prior to the incident, resulting in a temporary cutoff of cooling water to pumps and machines.
- Diffusion pumps had not been provided with any redundant power supply.

One by one, these problems can be explained by the environment, such as shortage of funds and personnel during the demobilization period, but the number of them is surprising. It also is not clear how many other problems with LC equipment and procedures may exist that were not involved in this incident. The existence of this many problems indicate a lack of a nuclear plant "atmosphere" or "culture", in which testing is obsessive and finding 'faults' by personnel is rewarded if it leads to a stronger environment. Multiple discussions with USEC management indicate they desire to have such an atmosphere, and this incident came as a shock to them, revealing that this atmosphere did not exist to the extent they desired. This is a repairable situation, but DOE LPO should ensure that the desired atmosphere prevails before the commercial plant is built.

The recent IER noted that USEC had demonstrated technical competency in performing centrifuge design work, to plan for and manage machine build-out, and to attract and maintain a talented and motivated staff, but had financial considerations judged as a 'very significant' risk. The IE does not retract its IER conclusions based on this incident. USEC staff's response to this incident reflects USEC's ability to respond to catastrophic incidents in an organized, calm, and diligent manner to resolve unknown issues and seek solutions to those that have been diagnosed. USEC's ability to satisfactorily diagnose the unknowns associated with this incident is a good indicator of their ability to respond to any incidents which occur during commercial operation. The IE judged the overall USEC response to the incident as comprehensive, timely, and professional.

Balance of Plant (BOP) system failures initiated the incident that were subsequently exacerbated by a critical operator error (i.e., inadvertent UPS shutdown) which caused the machines to move into off-normal machine operating conditions that were not remedied in time to prevent some machine crashes. This off-normal operating environment was not considered in the original machine failure modes analysis. The IE judged that the initiating factors for the incident were equivalent for machines that crashed, but exact timing and description of 'failure mode' sequences, i.e., which parts did what and went where during the time from crash initiation to crash conclusion, is still uncertain due to a lack of machine

operational data during the incident due to the unavailability of the DCS during the incident. The examination of the machine which suffered the breach led to a physically reasonable understanding of the mode of collapse as well as the cause of the breach. The IE team concludes that the breach was not instigated by any internal failure or design flaw in the centrifuge, but arose from external power failure. However, the cause of the breach is a result of the machine design and the lack of recognition by the design staff that the failure mode that occurred was credible and requires further design consideration. Furthermore, all six machines which crashed did so because of this power failure.

Incident event response by operators showed that some required measures to remedy the BOP system failures were not covered by procedures and operator training. Other Conduct of Operations (CONOPS) and test program issues were evident. The IE team acknowledges how the actions of experienced and knowledgeable operations and maintenance staff called to the scene by on-shift operations staff provided solutions for the problems at hand that were key in limiting machine crash extent by restoring critical systems. However, incident extent could have been significantly greater in terms of machine crashes if these same individuals had not been available.

The IE team reviewed photographs and data associated with a surviving machine which received the greatest heating, and there was no indication of internal damage or weakening of any component. USEC did not subject this machine to destructive testing to determine if any non-visible weakening had occurred, and the temperatures that were recorded when DCS power was restored, which should have been the highest experienced, were not close to the lowest temperature where damage would be expected. The IE concurs with the reasonable assumption that this and nine other over-heated machines were not damaged, but there remains the possibility that a hidden and unexpected mode of temperature damage has occurred. The machines will be monitored to confirm they operate within known parameters.

The IE recommends that DOE require USEC to take advantage of the opportunity afforded by ongoing LC-1 and LC-3 operations to pilot their incident prevention activities, rather than waiting until the build-out of the new cascades and trains is underway, including performing a BOP – Human Performance Failure Modes and Effects Analysis (FMEA) for the LC as a precursor to performing an ACP BOP – Human Performance FMEA or Failure Modes, Effects, and Criticality Analysis (FMECA). The ACP BOP is clarified as including all the non-machine systems, structures, and components in facilities such as Feed and Withdrawal (FW), Recycle and Assembly (RA), Process Area (PA), etc. The precursor LC FMEA should be conducted with the same format and rigor used in the centrifuge failure modes analysis conducted by USEC Oak Ridge staff. The failure mode analysis done for centrifuges should be expanded to address externally caused failures, and should not simply concentrate on providing redundant controls so there will be no externally caused failures. IE staff believe that risk No. 18, "*Poor Conduct of Operations and Conduct of Maintenance Practices and Procedures Resulted in Excessive Human Errors Causing Recent Machine Failures*" previously identified in the IER should be raised to "Significant" with risk mitigation focused upon USEC completion of noted FMEA work.

The IE recommends that DOE require USEC to revise the ACP reliability and availability estimates consistent with the FMEA(s) results. The FMEA results need to lead to commercial plant design inputs (requirements) that, when implemented through the design into the physical plant, enhance the overall plant reliability and availability. USEC machine dynamic analyses regarding failure mechanisms are still ongoing and prevent IE conclusions on performance impacts of potential machine design changes at this time.

The IE recommends that DOE require USEC to prepare a Lessons Learned document that addresses the details of the June 11th incident and derives lessons learned from them with a broad extent of condition analysis. This Lessons Learned document should be used as an important predecessor document for the FMEA work.

In summary, the incident might have been prevented or consequences sufficiently mitigated if:

- Industry-standard PM had been performed on the EMCC to preclude its failure as the incident initiating event;
- Known DG startup problems had been promptly corrected to ensure its timely use as a backup power source;
- Procedures had been available for UPS and DCS communication server restarts;
- Proper testing had been done of MCW pumps fail-safe mode after installation to prevent diversion of operator attention to remedy while other important incident events were progressing;
- More attention to human factors (CONOPS) had been observed in human-machine-interface facility design to preclude inadvertent shutdown of the UPS along with development of additional operator screen functions to better monitor the facility electrical system status; and
- A FMEA had been performed on the BOP systems supporting the LCs along with consideration of potential human performance problems to identify failure modes that could significantly impact machine operation.

The IE incident report includes recommended conditions for loan approval based on IE incident evaluation.

CONTENTS

Executive Summary ii
Acronyms and Glossary vii
XX.1. Introduction 1
XX.2. Mode of Incident Evaluation 1
XX.3. Incident Description 2
XX.3.1 Incident Sequence of Events 2
XX.3.2 IE Verification of Incident Timeline 4
XX.3.3 Impact on the Centrifuges 4
XX.3.4 Peripheral Phenomena Occurring During the Incident 6
XX.4. Incident Response 6
XX.4.1 USEC Related Actions before the Incident 6
XX.4.2 USEC Response During and After Incident 7
XX.5. Restoration of Operational Status 8
XX.6. Lessons Learned 9
XX.7. Impacts 10
XX.7.1 Cost 10
XX.7.2 Schedule 10
XX.8. Conclusions and Recommendations 11
XX.8.1 Conclusions 11
XX.8.2 Recommendations 13
XX.8.3 Possible Conditions for the Loan Guarantee 15
XX.8.4 IE Actions to Complete the Incident Evaluation 17
XX.8.5 Risk Issues and Recommended Mitigation Actions 18
XX.9. Technical Appendix 21
XX.9.1 Electrical Fault 21
XX.9.2 Inverted Controls on MCW Pump Discharge Valves 23
XX.9.3 Diesel Generator Use during the Event 24
XX.9.4 Response to UPS Loss of Power 26
XX.9.5 DCS Operations 27

Acronyms and Glossary

Acronym	Definition
2002 DOE USEC Agreement	An agreement between USEC and DOE to ensure the long-term stability of the U.S. enrichment industry. This agreement contains specific milestones relating to the Plant
ACP	American Centrifuge Plant; USEC's planned commercial uranium enrichment facility using DOE-developed centrifuge technology. USEC plans to install thousands of centrifuge machines and to operate the facility in the DOE-owned gas centrifuge enrichment plant buildings in Piketon, Ohio
BOP	Balance of Plant including all the non-machine systems, structures, and components (FW, RA, PA, etc.)
CATSWEB	Corrective Action Tracking System – web or internet based
CCB	Configuration Control Board
CCC	Configuration Change Control
CDR	Critical Design Review
Centrifuge	A machine that enriches uranium by spinning UF_6 at a high speed to use centrifugal force to separate the heavier $_{238}U$ from the lighter $_{235}U$
CONOPS	Conduct of Operations
CRB	Change Review Board
DCS	Distributed Control System
DG	Diesel Generator
DOE	U.S. Department of Energy
EMCC	Electrical Motor Control Center
EPC	Engineering, Procurement, and Construction
FMEA	Failure modes and effects analysis
FMECA	Failure modes, effects, and criticality analysis
FW	Feed and Withdrawal (Facility)
GCEP	DOE's original Gas Centrifuge Enrichment Plant in Piketon, Ohio; where the ACP is being constructed
HVAC	Heating Ventilation and Air Conditioning
IE	Independent Engineer
IER	Independent Engineer Report
IPT	Integrated Product Team
IROFS	Items Relied On For Safety
LC	Lead Cascade; An array of full-sized centrifuge machines operating in a closed-loop configuration, from which samples are withdrawn for testing, and the enriched and depleted uranium streams are recombined into feed material
LEU	Low Enriched Uranium; Uranium enriched in the isotope $_{235}U$ to an assay of between 0.712% and 19,999%. Commercial-grade LEU typically has an assay of 3% to 5% and is used as fuel in nuclear reactors for the generation of electric power
LPO	Loan Programs Office
Machine Failure	Material defect or fault in a centrifuge machine that prevents it from continued operation and requires temporary removal from service for repair or replacement (also see catastrophic machine failure). Term is used in reliability calculations
MCW	Machine Cooling Water
MD	Maryland
MDU	Machine Drive Unit
MIP	Machine Instrument Package
M-Yr	Machine-year
NQA-1	Nuclear Quality Assurance – Level 1

Acronym	Definition
NRC or USNRC	U.S. Nuclear Regulatory Commission
OH	Ohio
O&M	Operations and Maintenance
PA	Process Area
Piketon	The location (Piketon, Ohio) where USEC is constructing the Plant
Plant	The American Centrifuge Plant or ACP
PLC	Programmable Logic Controller
Project or ACP Project	The project's name
PM	Preventive Maintenance
PV	Purge Vacuum
QC	Quality Control
RA	Recycle and Assembly
REASON	software used to determine and isolate the root causes of a problem
SIS	Secondary Isolation System
SWU	Separative Work Unit; The standard unit of enrichment in the uranium-enrichment industry. An SWU represents the effort that is required to transform a given amount of natural Uranium into two streams of uranium, on enriched in the $_{235}U$ isotope and the other depleted of the $_{235}U$ isotope, and is measure using a standard formula based on the physics of uranium enrichment. The amount of enrichment contained in LEU under this formula is commonly referred to as the SWU component
TER	Technical Evaluation Report
TN	Tennessee
UF_6	Uranium Hexafluoride; Chemical compound produce from converting natural UO_2 into a fluoride at a conversion plant. UF_6 is the feed material for uranium-enrichment plants
Under Secretary	The Under Secretary of Energy or a duly authorized designee or successor in interest
UPS	Uninterruptible Power Supply
Uranium	One of the heaviest elements found in nature. Approximately 993 of every 1000 uranium atoms are $_{238}U$, while approximately seven atoms are $_{235}U$, which can be made to split, or fission, and generate heat energy using thermal (or slow) neutrons
U.S.	United States
USEC or USEC Inc. or Applicant	United States Enrichment Corporation
VTM	Verification Test Machine

XX.1. Introduction

In the morning of June 11, 2011, a series of events took place at the United States (U.S.) Enrichment Corporation (USEC) Piketon American Centrifuge Plant (ACP) lead cascade (LC) facility that ultimately led to the crash of six centrifuges. This is an interim report, prepared by the Independent Engineer (IE) Incident Evaluation Team that describes the team's determination of what happened during the incident. Some initial recommendations are provided for the U.S. Department of Energy (DOE) Loan Programs Office (LPO) to support decisions related to USEC's loan application, including what conditions to impose on USEC to reduce the probability that a multi-centrifuge incident could occur after loan approval. Centrifuge crashes may be important to the DOE LPO as the causes of these crashes can reveal otherwise hidden design defects and insufficient Balance of Plant (BOP) system redundancy design that could impact machine operation and impinge on the ability of the loan recipient to repay the amounts. For example, a crash that was caused by an unforeseen design failure could reveal that progress would have to be delayed for a period while design issues are diagnosed and rectified, and this delay may have a loan repayment impact.

The IE Incident Evaluation Team from Parsons included Brad Knutson, IE leader, and Stan Erickson, IE member. Charles Moseley also assisted in reviewing Quality Control (QC) and procedure issues. It is expected that more IE team members will be involved in preparing the final incident evaluation report.

XX.2. Mode of Incident Evaluation

The IE incident evaluation team made four visits to Piketon Ohio (OH) and one visit to Oak Ridge Tennessee (TN), along with two visits to USEC Headquarters in Bethesda Maryland (MD). At Piketon, the IE team was given presentations by USEC management, along with access to classified and unclassified documents related to the incident investigation and to the equipment involved in the incident. Most importantly, the IE team was given open access to Piketon USEC employees who were involved with the incident itself, or involved with the incident investigation, as well as Oak Ridge technical engineering team members. The IE team obtained USEC training needed to permit unescorted access in the Piketon office and plant areas. The IE team was given tours to see the equipment involved in the incident first-hand, which included observing the electrical panel involved while it was still disassembled, the centrifuges before removal, the Diesel Generator (DG) and the Machine Cooling Water (MCW) pumps, and nearby piping, Heating Ventilation and Air Conditioning (HVAC) systems, electrical wiring, and other support equipment. The IE team also viewed the Uninterruptible Power Supply (UPS) system involved in the incident, and spent time in the control room viewing the screens that were used before and after the incident, discussing with the operators what they were able to observe.

The IE team requested and received documents from the Gas Centrifuge Enrichment Plant (GCEP) related to past machine crashes and reviewed them. The IE team reviewed classified daily updates of a USEC spreadsheet being used to compile the detailed incident timeline, and attended the classified 12:30pm daily status meetings between Piketon, Oak Ridge, and

Bethesda USEC staff via video conference lines. The IE team was given detailed reviews of the photographs of the damaged centrifuges after they had been removed from the LCs and disassembled. The IE team also was shown disassembled circuit monitors, "targets" that were used to diagnose the electrical short details, along with detailed circuit diagrams and tables. IE staff reviewed the classified USEC Interim and Final Investigation Reports.

The IE team traveled to Oak Ridge to review USEC technical staff understanding of the details of how the centrifuges were damaged, and read the draft USEC Technical Evaluation Report (TER) on that topic. The IE team discussed in detail with the technology project director and deputy director the physics involved in the crashes, and what photographs of the machines after disassembly had revealed, and what was still uncertain. The IE team disagreed with some findings in the report version available at that time, and Oak Ridge concurred with these points, and is in or has completed the process of modifying the report accordingly, along with continuing their modeling of the details of the crash phenomena. A final IE incident evaluation report is planned to include final machine technical analyses that address potential centrifuge design changes that are still being evaluated.

At Oak Ridge, the IE team was given a briefing on electrical systems at K-1600, and on how incidents such as happened on June 11th at Piketon were being thought through at Oak Ridge. The analysis and briefing were well done and indicate that important lessons have been learned from the February and March incidents at K-1600.

Requests for interviews with USEC personnel were responded to within the day of being issued, except for personnel on travel or otherwise absent. The IE team found USEC staff responsive to IE team questions and open in disclosing relevant information regarding the incident and operator responses. These discussions often lasted hours, allowing the IE team to probe into a step-by-step phenomenology of exactly what happened with the different event items. These discussions often led to important insights into the condition of the plant equipment before the incident, the technical details of the equipment itself and its interconnection, the state of training and preparation of the staff before the incident, the reactions of the staff during the incident, and any other factors the IE team felt were important.

XX.3. Incident Description

XX.3.1 Incident Sequence of Events

Following is a summary of the incident sequence of events based on the USEC investigation report and IE team discussions with USEC staff involved in the incident or incident investigation. Section XX.7, Technical Appendix, provides detailed summaries of the equipment and its interactions during the incident gleaned from discussions with USEC staff.

- While a routine switch-over was being done between main and alternate MCW pumps, an electrical short developed in one phase of an electrical panel providing power to the diffusion pumps of LC-1 (sole source), the MCW pumps, the UPS which powers most electrical controls, the battery room hydrogen monitor and ventilation, and the Purge

Vacuum (PV) pumps. There are alternate power paths to the latter group of equipment. The electrical short led to sputtering at the point of shorting along with falling metal fragments, which led to a larger arcing short just below that point. A circuit breaker on the electrical panel on the line side just preceding this one popped, with the target showing 16,000 amps had passed through it for a very short time.

- Available operations staff assessed the situation and determined that there was no fire and no continuing short circuit. To provide power to the panel with the short, it was possible to either replace the blown circuit breaker or to use the DG. A replacement circuit breaker was not immediately available to the staff, and they attempted to start the DG, and then to connect it to the power line with the appropriate relays. The DG's own protective circuit breakers tripped and staff waited for a power expert to arrive before continuing. The DG was started unsuccessfully four times before reconnecting and providing power.

- When the power incidents were occurring, the DCS was alarming and the on shift operators responded by sending an operator to the UPS control panel, mounted on the UPS itself outside the control room. The first step of the standard alarm response procedure is to silence the alarm. For electrical problems, the operator sent to the UPS was given the task of doing that at the UPS panel, rather than via control circuitry. The operator inadvertently shut down the UPS by hitting the emergency off switch, which is located on the same panel. The UPS controls the digital processing for the centrifuges' Machine Instrument Packages (MIPs), controls for the valve system feeding the centrifuges and one controlling the machine PV system, the MCW pump valves, the four communication systems between the MIP and the DCS (two per cascade), and other equipment and sensors.

- When the PV system loses power to its valves, they go to the fail-safe position of completely shutting off each of the centrifuges individually, both from vacuum and from feed and withdrawal. This means that in-leaks and out-gassing will lead to pressure increases in the centrifuges, which is an eventually fatal condition.

- When the MIP loses power or communication, operators lose control of the machines, and in combination with vacuum loss, this will lead to centrifuge self-destruction.

- The MIP has manual overrides, but because the communication system between the DCS and the MIP was shut down without UPS power, they could not be used.

- The operators were unable to find adequate documentation on how to restart the UPS, and this particular situation was not part of their training or procedures. This UPS has two circuit breakers located inside the system panel, accessible only by opening the UPS metal shielding. These breakers were not well documented, and only after a more experienced expert arrived was this problem overcome and UPS power restored.

- By the time the UPS power was restored, four machines had already crashed. One of these machines suffered a breach.

- When the UPS was reactivated, the servers providing the communications between the DCS and the MIPs went into restart mode. Two of these are older systems which must go into idle status, which requires manual control from DCS to make them operational. There was no training or procedures for this action, and it had to wait until another expert arrived and was able to locate the software controls needed to change them into operational mode. The other two, for the newer cascade (LC-3), can be set to start either in operational mode or in idle mode. Only one had been set properly to start in operational mode; one had not. This meant that three of the four communication channels were unusable immediately after UPS restart. During the time it took for a DCS expert to arrive and correct the mode settings of these three controllers, two more machines had crashed. It is not clear that if the restarts had taken place much faster, that either or both of these machines could have been saved, but the possibility exists they could have.
- After the UPS was on and the DCS was able to communicate with the MIPs, the remaining centrifuges were brought into stable condition. Approximately 10 of them had experienced temperatures beyond design limits.

XX.3.2 IE Verification of Incident Timeline

For each of the steps involved in the incident event timeline, the IE team interviewed personnel involved in the incident and its investigation, and closely compared the information to the USEC event sequence spreadsheet. Only after a thorough understanding of the details of each piece of equipment involved, perhaps viewing it or its components, and a thorough understanding of the actions of the individuals involved, did the IE team verify the above sequence of events. During the meetings, there were often differing explanations arising early in the investigation, and the IE team worked with USEC personnel and other sources to eliminate any possibilities that were outside the sequence of events being developed.

The IE team listened to the investigative reports discussed daily between USEC staff located at the various sites, but formed their own conclusions based on reasonable physical phenomena and the discussions with involved employees. The IE team did not find any discrepancies between a 'physics or engineering' understanding of the equipment and centrifuges involved and the events listed in the sequence of events.

XX.3.3 Impact on the Centrifuges

The previously completed USEC Oak Ridge centrifuge FMEA stopped at internally caused failure modes and did not treat failure modes generated by external effects, such as loss of power. For this reason, there was no prediction by Oak Ridge of the possibility of a breach. Furthermore, it took a disassembly of the breached machine to reveal what had happened. No breach events had happened since 1977, and USEC had not developed any prior mechanisms as to how a breach might take place or even considered the possibility that one might occur. Thus, when a breach occurred, there was no basis to immediately generate possible mechanisms for the breach, and some initial visual observations of the machine in question

were misinterpreted, as there was simply no concept of breach mechanisms that would allow these observations to be correctly interpreted.

Photographs of the disassembled machine internal components revealed the details of what had caused the breach. This is now being reviewed by Oak Ridge for the purpose of determining both interim fixes to prevent a recurrence during LC operations, and long term design fixes. The IE team will review these fixes when they are available.

The IE team also reviewed the photographs and data associated with the surviving machine which had received the greatest heating, and there was no indication of internal damage or weakening of any component. USEC did not subject this machine to destructive testing to determine if any non-visible weakening had occurred, and the temperatures that were recorded when DCS power was restored, which should have been the highest experienced, were not close to the lowest temperature where damage would be expected. The IE concurs with the reasonable assumption that these 10 machines were not damaged, but there remains the possibility that a hidden and unexpected mode of temperature damage has occurred. The machines will be monitored to confirm they operate within known parameters.

The examination of the machine which suffered the breach led to a physically reasonable understanding of the mode of collapse as well as the cause of the breach. The IE team concludes that the breach was not instigated by any internal failure or design flaw in the centrifuge, but arose from external power failure. Furthermore, all six machines which crashed did so because of this power failure. The details of how they failed internally differ somewhat, and that is the subject of further investigation. It also is not clear, among the machines of the older cascade (LC-1), why the two that failed were the ones which did, and not another one. This will likely be explained by the detailed modeling of the machine failure mechanisms. Likewise, the evaluation of potential machine design changes to eliminate or mitigate these problems remains to be completed.

The IE team is concerned that other external causes may lead to a breach or another serious unexpected centrifuge crash result. The IE team discussed in detail the possibilities of different external sources of machine crash, such as lack of cooling water, or circuit problems in the MIP or other electronics, as well as loss of power or vacuum, or some of these in combination. Despite these not having been included in the centrifuge failure mode analysis, the USEC technology engineering and management staff have thought through these possibilities and have experienced crashes of sufficiently diverse origin that staff understands and can explain what could happen in the cases that the IE team was able to pose. At this time, the IE team does not feel that there are further unknown accident types remaining to be experienced, but further examination and documentation of these understandings would add to the confidence level of this statement.

XX.3.4 Peripheral Phenomena Occurring During the Incident

When the power to the MCW digital controller was cut off, the valves connecting th e MCW to the centrifuges went into fail-safe mode. However, the fail-safe mode had been installed in inverted fashion, so the cooling water was cut off and the pump deadheaded. The valves in question come from the manufacturer with cutoff as the fail-safe mode, although a simple change in installation allows this to be changed to a fail-open mode. Quite clearly, a power failure scenario for the MCW digital controller had not been included in a test program, and this QC lapse has implications for both the LCs and for the commercial plant. Additional training for maintenance and construction personnel will be necessary to ensure proper installation and valve lineups. QC personnel should inspect installation at designated hold points for the initial phases of construction until reasonable confidence is attained that proper installation has occurred.

The loss of MCW cooling added to the burden of problems going on during the incid ent, and if pump water was not eventually restored, components in the centrifuges would have overheated from lack of cooling. Furthermore, the diffusion pumps depend on water, so they would have failed to work after some time. USEC was not, at the time of the investi gation, aware of just how much time is available to fix a cooling water problem before machines would be endangered, but it is believed to be longer than tens of minutes. The shut valves were manually bypassed before 20 minutes had passed, restoring cooling water, and no damage is known to have occurred to the pumps or centrifuges from this mishap.

The cut-off pump, being deadheaded, created a great deal of noise, which led to an investigation of its condition. There are bypass valves that go around the automated valve, and these were used to restore cooling water. If the DCS, communications servers, and MIPs were all working at the time of a water problem, there would be alarms at the control room that would lead to the discovery of this problem and its solution. If the problem was not solvable for some reason, the machines would be brought to a safe operating condition. This is not likely to be a failure mode which would cause multiple centrifuge failures, but it bears further investigation in the FMEA and in the IE review of it.

Specifically, the early detection of installation errors in support systems should be part of any QC program, such as the Nuclear Quality Assurance Level 1 (NQA-1) used by USEC. This problem should be addressed in the USEC Lessons Learned report.

XX.4. Incident Response

XX.4.1 USEC Related Actions before the Incident

The root cause of the incident, the shorting of a stab connector to a busbar in the Electrical Motor Control Center (EMCC) electrical panel, might have been prevented if industry-standard Preventive Maintenance (PM) had been performed. There was good reason to use a less-thorough substitute PM since the panel was expected to be removed and discarded when the LCs were removed, with LC operation duration expected only to be a year or so beyond the industry-standard time for a PM. Furthermore, these connectors do not wear out, having a

clearly predictable time when they need to be replaced, such as a tire with 30,000 miles on it. Thus the industry-standard is only a guideline. The IE does not fault USEC for this decision, however, it proved to be quite unfortunate in being the incident root cause.

Similarly, the DG was known to have startup problems for some number of months, but they were not sufficiently investigated to prevent the problems that occurred on June 11th. Again, it is understandable how a generator that was scheduled to be removed when the LCs were removed would have an analysis of its problems delayed, but again, it proved to be unfortunate in its contribution to the incident results.

The lack of procedures for UPS and DCS communication server restarts indicates a too heavy reliance on the expectation that these systems were highly reliable and did not need restart procedures. Again, this proved to be an unfortunate oversight.

The lack of testing of the MCW fail-safe mode should not have happened. The lack of back-up power for the diffusion pumps may be a design flaw dating back to the GCEP era, but it was not flagged during the re-installation of operating LCs as a potential problem. This may be because there were no circuit diagrams showing this sole source situation that would have made the situation obvious to USEC management.

One by one, these problems can be explained by the environment, such as shortage of funds and personnel during the demobilization period, but the number of them is surprising. It also is not clear how many other problems with LC equipment and procedures may exist that were not involved in this incident. The existence of this many problems indicate a lack of a nuclear plant "atmosphere" or "culture", in which testing is obsessive and finding 'faults' by personnel is rewarded if it leads to a stronger environment. Multiple discussions with USEC management indicate they desire to have such an atmosphere, and this incident came as a shock to them, revealing that this atmosphere did not exist to the extent they desired. This is a repairable situation, but DOE LPO should ensure that the desired atmosphere prevails before the commercial plant is built.

XX.4.2 USEC Response During and After Incident

USEC staff on-site during the incident and those brought in after being summoned by the initial team displayed a calm and controlled response to the problems, which led to the remaining machines being rescued from destruction. This resourcefulness in the face of unpredicted event sequences is one of the most desirable attributes that an operating team can have. USEC has done an excellent job in finding and retaining the quality of operating personnel that was demonstrated here.

This aspect cannot be sufficiently emphasized. If the operating team had not responded so well, most or all of the machines would have been lost, as they were all on the path to the same unpredicted failure mode that captured six of them. This incident analysis would certainly have a different character if all machines had been lost.

After the incident, USEC designated and formed an investigation team with participation by both Piketon and Oak Ridge USEC employees. The IE team used REASON software to

determine and isolate the root causes of the problem, and this use was, in the view of the IE team, successful. The investigation was conducted in an orderly manner, with plans for analysis and calculations, machine disassembly, data collection, and so on planned in advance of any actions being taken. The IE team feels that the classified video connection between the two organizations was quite useful; USEC has responded well to the comments in the original IE Report about lack of coordination between the two facility locations. This event clearly demonstrated that this problem has been successfully eliminated and the opposite situation, excellent communication, prevails and appeared invaluable during this investigation.

The IE team monitored the USEC investigation by attending the daily status meetings and through frequent discussion with USEC Piketon management staff. The investigation was conducted in exemplary fashion, was well planned, and did not consume excess time that was visible to the IE team. The IE team was careful not to make any demands on employee time that would interfere with the ongoing investigation.

USEC developed a two-stage plan for resuming operations, and this was applied separately to K-1600 and Piketon. Because of the breach incident, K-1600 had been similarly shut down until the investigation had determined the cause and understood the phenomena. Phase one involves slow speed operations and phase two, full speed.

XX.5. Restoration of Operational Status

USEC plans to resume LC machine operations using a two-phased approach. Phase 1 is the resumption of centrifuge operations to establish a machine rotational speed below the threshold that will cause a breach in any known situation. Phase 2 is restoration of full-speed machine operations but requires completion of the investigation analysis and implementation of any needed risk mitigation actions.

IE staff attended a briefing given by USEC Piketon operations staff to the ACP Director on the Readiness Assessment package prepared to support Phase 1 resumption of centrifuge operations. A high-level review of the assessment package by IE staff suggested a comprehensive approach had been taken by USEC to prepare the facility for resumption of machine operation which was started that same day (June 29, 2011). The IE team discussed with Oak Ridge management the calculations that justified slow speed operations and understood the decision having no reservations.

Phase 2 requires completion of investigation analysis and implementation of any needed risk mitigation actions. There are ongoing dynamic analyses being performed on machine failure mechanisms to verify 'failure mode' sequences, i.e., which parts did what and went where during the time from crash initiation to crash conclusion. Presently these sequences are still uncertain due to a lack of machine operational data during the incident due to the unavailability of the DCS during the incident. Dynamic modeling is being used to understand these mechanisms under the off-normal operation conditions encountered during the incident.

USEC also applied the two-phased plan for resuming operations to the K-1600 facility. Because of the breach incident, K-1600 had been similarly shut down until the investigation had determined the cause and understood the phenomena.

XX.6. Lessons Learned

USEC's final investigation report was considered as having insufficient detail on lessons learned and how these would be implemented in the subsequent LC operations and ACP. Following are IE judgments on lessons learned that require consideration by USEC.

- Incident resolution and machine damage mitigation relied on knowledgeable and experienced operators to provide solutions to failure events that moved beyond procedures and training, with CONOPS and test program issues also evident. USEC needs to institutionalize this key operator knowledge and experience through procedures and staff training. USEC staff's response to this incident should be used as a training example of how staff should respond to catastrophic incidents in an organized, calm, and diligent manner to resolve unknown issues and seek solutions to those that have been diagnosed.

- System redundancy in the ACP design that is expected to eliminate or reduce the possibility of multi-centrifuge incidents can be rendered ineffective if systems are inadequately tested. USEC needs to ensure sufficient system testing of redundant systems is performed and implement instructions and training for all staff that encourages a 'no hesitation' mindset of staff in using the web or internet based Corrective Action Tracking System (CATSWEB) process to report possible testing lapses which might lead to the beginning of an incident or could exacerbate an abnormal situation.

- Multiple problems relating to the support systems during the incident resulted from a lack of attention to abnormal system operations, and an unwise reliance on the availability of multiple backups for most systems. USEC needs to address failure modes involving backup systems through conduct of a formal BOP – human performance FMEA or Failure Modes, Effects, and Criticality Analysis (FMECA). The ACP BOP is clarified as including all the non-machine systems, structures, and components in facilities such as Feed and Withdrawal (FW), Recycle and Assembly (RA), Process Area (PA), etc. The ACP Engineering, Procurement, and Construction (EPC) contractor also needs to re-evaluate the ACP electrical configuration design. The LCs provide an opportunity to pilot incident prevention activities before ACP build-out of the new cascades and trains is underway (i.e., conduct LC BOP – human performance FMEA).

- Loss of power failure modes experienced during the incident were unexpected based on previous GCEP operating experience. USEC needs to properly consider these failure modes during conduct of a formal ACP BOP – human performance FMEA or FMECA and perform follow-up staff training drills related to potential loss of power incidents to verify proper facility response to loss of normal power, including backup diesel power startup and power to bus timing and critical power loads carried by UPS system as

required. BOP is used here to include anything other than the centrifuges themselves. These drills need to be conducted with tested and trained operations personnel. The K-1600 facility loss of power drill program presented to IE staff appeared to be a good example of proactive operations training that was 'tested' during recent offsite power outages due to electrical storms (April to May 2011).

- Machine breach was not instigated by any internal failure or design flaw in the centrifuge, but arose from external power failure. USEC needs to expand the centrifuge FMEA to include externally caused failures, and not simply concentrate on providing redundant controls so there will be no externally caused failures, but also focus on examining what would happen if redundancy failed for some reason.

XX.7. Impacts

The IE should provide an independent assessment of USEC's calculation of costs and schedule delays resulting from the June 11th incident. These values have been calculated and presented to the DOE Under Secretary, Office of Science and Technology, but these preliminary values are no longer accurate because of changes in restart time.

XX.7.1 Cost

The IE is not yet able to assess cost impacts due to BOP and potential machine design changes since USEC analyses to provide the basis for these changes are still outstanding. These analyses are expected to be completed shortly.

The IE roughly estimates that a BOP / Human Performance FMEA or FMECA will cost between $3 Million to $5 Million. Cost impacts for machine design changes are pending final technical engineering analyses of failure mechanisms that are ongoing. Costs associated for BOP changes that will preclude failure modes experienced during the incident and others that could impact machine operation requires completion of the FMEA and integrated baseline.

XX.7.2 Schedule

The IE is not yet able to assess schedule impacts due to BOP and potential machine design changes since USEC analyses to provide the basis for these changes are still outstanding. These analyses are nearly completed, but final details are pending design change confirmation.

The BOP / Human Performance FMEA or FMECA work is estimated to require 4 to 6 months. The integrated baseline development schedule appears to be delayed 3 to 5 months past the November 2011 date. The delay caused by the findings of the BOP/Human Performance FMEA on baseline development will depend on how extensive the mitigation actions are.

XX.8. Conclusions and Recommendations

XX.8.1 Conclusions

The incident evaluation concentrated on the problems found with equipment and procedures that relate to the incident. The following conclusions need to be viewed in this context.

- The recent IER noted that USEC had demonstrated technical competency in performing centrifuge design work, in planning for and managing machine build-out, and in attracting and maintaining a talented and motivated staff, but had financial considerations judged as a 'very significant' risk. The IE does not retract its IER conclusions based on this incident. USEC staff's response to this incident reflects USEC's ability to respond to catastrophic incidents in an organized, calm, and diligent manner to resolve unknown issues and seek solutions to those that have been diagnosed. USEC's ability to satisfactorily diagnose the unknowns associated with this incident is a good indicator of their ability to respond to any incidents which occur during commercial operation. However, the multiple human factor and support equipment problems which combined to create this incident raise QC questions for the LC, which also must be addressed for the commercial plant.

- BOP system failures initiated the incident which was subsequently exacerbated by a critical operator error which caused the machines to move into off-normal machine operating conditions that were not remedied in time to prevent some machine crashes; this off-normal operating environment was not considered in the original machine failure modes analysis.

- Incident response by operators showed that some required measures to remedy the BOP system failures were not covered by procedures and operator training. Other CONOPS and test program issues were evident. The IE team acknowledges how the actions of experienced and knowledgeable operations and maintenance staff called to the scene by on-shift operations staff provided solutions for the problems at hand that were key in limiting machine crash extent by restoring critical systems. However, incident extent could have been significantly greater in terms of machine crashes if these same individuals had not been available. Remedies for BOP system failures need to be developed that do not include off-site staff to the extent possible, with these operator 'tribal lore' solutions implemented in procedures.

- Initiating factors for the incident were equivalent for machines that crashed, but exact timing and description of 'failure mode' sequences, i.e., which parts did what and went where during the time from crash initiation to crash conclusion, is still somewhat uncertain due to a lack of machine operational data during the incident due to the unavailability of the DCS during the incident. The examination of the machine which suffered the breach led to a physically reasonable understanding of the mode of collapse as well as the cause of the breach. The IE team concludes that the breach was not instigated by any internal failure or design flaw in the centrifuge, but was made

possible by the internal design. All six machines which crashed did so from the same external power failure.

- The investigative process developed multiple hypotheses about many of the details of the incident. Most of these details have now been ironed out. IE staff judgment is that most uncertainty about the crashes has been resolved, but there remains a small amount of uncertainty on why certain machines crashed and others did not, with correlation to available operational data not fully established by the TER. USEC has on-going studies to attempt to provide more clarity, and they will respond to this and other IE suggestions on improving the document. USEC also is reviewing past incidents regarding certain design features involved in the recent machine crashes.

- The IE team reviewed photographs and data associated with a surviving machine which received the greatest heating, and there was no indication of internal damage or weakening of any component. USEC did not subject this machine to destructive testing to determine if any non-visible weakening had occurred, and the temperatures that were recorded when DCS power was restored, which should have been the highest experienced, were not close to the lowest temperature where damage would be expected. The IE concurs with the reasonable assumption that these 10 machines were not damaged, but there remains the possibility that a hidden and unexpected mode of temperature damage has occurred. The machines will be monitored to confirm they operate within known parameters.

- The previous machine incidents in February and March 2011 experienced at K-1600 dispelled USEC management's unwarranted belief that their staff training at Oak Ridge would eliminate the possibility of human performance errors causing centrifuge losses. In the IE's opinion, USEC responded well to this situation. Further IE review will confirm this.

- The IE team warned in the previous incident report contained in the IER that possible problems with multi-centrifuge plant-generated accidents should be analyzed, but did not change their recommendations based on this possibility. Now that one has happened, the IE team has evaluated USEC's response and capability to reduce this type of occurrence, and concludes that their staff should be able to do this. The recent incident dispelled USEC management's belief that GCEP-planned redundancy would prevent multi-centrifuge crashes. So far, USEC management has responded well to this challenging incident and the investigation thereof, and should be allowed to continue their path forward, while continuing IE monitoring. IE monitoring may need to be increased in the area of QC, especially in the initial phases of installation.

XX.8.2 Recommendations

The occurrence of machine crashes is expected and is taken into account in estimating availability. However, it is individual machine crashes that enter into this formulation, not multiple crashes arising from external sources in the plant itself. Following the two machine crashes in K-1600 in February and March of this year, the IE became concerned about similar incidents, but relating to multiple machines, that could occur in Piketon and made the recommendation that this be investigated with a failure modes analysis. This analysis had not been started at the time of this new incident. It obviously needs to be done.

It was the belief of Piketon management that the existence of redundancy in their plant design would eliminate or reduce the possibility of multi-centrifuge incidents. However, redundancy is only one part of a system for reducing accidents. Testing and preparation is the other part. Untested redundant systems or inadequately tested redundant systems are not redundant; they are simply hardware located in the plant. It is the IE's belief that steps need to be taken at Piketon to better prepare for equipment faults that could avalanche into multi-centrifuge destruction. Specifically:

1. USEC should take advantage of the opportunity afforded by ongoing LC-1 and LC-3 operations to pilot their incident prevention activities, rather than waiting until the build-out of the new cascades and trains is underway, including performing a BOP – Human Performance FMEA for the LC as a precursor to performing an ACP BOP – Human Performance FMEA or FMECA. The ACP BOP includes all the non-machine systems, structures, and components in facilities such as FW, RA, PA, etc. The precursor LC FMEA should be conducted with the same format and rigor used in the centrifuge failure modes analysis conducted by USEC Oak Ridge staff. The failure mode analysis done for centrifuges should be expanded to address externally caused failures, and should not simply concentrate on providing redundant controls so there will be no externally caused failures. IE staff believe that risk No. 1B, "*Poor Conduct of Operations and Conduct of Maintenance Practices and Procedures Resulted in Excessive Human Errors Causing Recent Machine Failures*" previously identified in the IER should be raised to "Significant" with risk mitigation focused upon USEC completion of noted FMEA work.

2. ACP reliability and availability estimates should be revised consistent with the FMEA(s) results. The FMEA results need to lead to commercial plant design inputs (requirements) that, when implemented through the design into the physical plant, enhance the overall plant reliability and availability. USEC machine dynamic analyses regarding failure mechanisms are still ongoing and prevent IE conclusions on performance impacts of potential machine design changes at this time.

3. A Lessons Learned document that addresses the details of the June 11th incident and derives lessons learned from them is still required with a broad extent of condition analysis. This Lessons Learned document should be used as an important predecessor document for the FMEA work.

4. USEC should take advantage of the opportunity afforded by the LCs to pilot their incident prevention activities, rather than waiting until the build-out of the new cascades and trains is underway. Because there is so much at stake, financially, in availability, it would be desirable to have a 'nuclear plant' culture at Piketon, in which everything is tested, failure modes are continually explored, personnel are trained in abnormal situations as well as normal ones, procedures are continually reviewed for improvements, and people are held responsible for prevention as opposed to only response. This culture is not something that can be switched on when the build-out starts. It is something that has to be developed and grown over time.

5. USEC should designate an individual who is responsible for maintaining availability. This is not the same as someone who is responsible for calculating availability, but instead is a line person with authority to designate testing, preventive maintenance, procedure writing or re-writing, training, spare parts or tool availability, ergonomics that are appropriate to maintaining availability, and so on, and ensure that it is done. This can be a new hire or an existing person, but this responsibility should be high on the job description for this person, and sufficient authority given to this position to ensure that availability sufficient to repay all loans is maintained. K-1600 had personnel changes made following their second incident. The IE team has met with the new person responsible for ensuring that operator caused crashes do not occur at K-1600 and were impressed with his attention to detail.

6. The BOP – Human Performance FMEA should be conducted with the same format and rigor that the centrifuge FMEA was conducted at Oak Ridge. The IE reviewed both the analysis process and the results and considered the process as sufficiently and competently performed. This process involves having Integrated Product Teams (IPTs) set up for each component; for example, vacuum systems, electrical systems, communications, DCS, and so on, for the plant. These teams should include both Oak Ridge and Piketon personnel in all cases. It is felt that Oak Ridge personnel will bring fresh eyes to look at possible failure modes in Piketon and the process will benefit, in Piketon as it did in Oak Ridge, from having both communities involved.

7. The centrifuge FMEA should be expanded to include externally caused failures, and should not simply concentrate on providing redundant controls so there will be no externally caused failures, but also focus on examining what would happen if redundancy failed for some reason. The details of how machine failure proceeds and the sequence of failure mechanisms are the important items. It is necessary for many reasons why the type of failure that occurred on June 11th should not happen again; nor should there be any other 'surprises' when a machine crashes.

XX.8.3 Possible Conditions for the Loan Guarantee

Following are possible conditions for loan guarantee recommended for consideration by DOE LPO.

To support Conditional Loan Approval:

1) USEC performs a BOP - Human Performance FMEA for LC facility that is verified by the IE; analysis should determine all single-point failures (e.g., non-functioning equipment that could lead to the destruction of more than one machine) for LC operation and means (e.g., redundancy, procedures, and spares) to address each. The LC FMEA would serve as a pilot for the commercial plant FMEA or FMECA, taking into account the lessons learned from the recent incident as a starting point.

2) USEC provides a revised estimate of plant availability that incorporates improved estimates of BOP and machine availability in consideration of the recent incident events and the results from performing a BOP - Human Performance FMEA for the LC facility.

3) USEC completes forensics of remaining failed machines and those with heat stress to complete dataset and documents results as part of the investigation report verified by the IE. This does not imply disassembly of all machines but investigation sufficient to provide confirming information for conclusions.

4) USEC provides detailed cost and schedule impacts resulting from the incident that are verified as sufficient by IE review.

5) USEC obtains U.S. Nuclear Regulatory Commission (NRC) approval for resolution of the portion of the event that impacted any Items Relied On For Safety (IROFS) (e.g., battery room hydrogen monitor and fan) as needed to support return to full speed machine operations of LCs to the extent necessary.

6) USEC completes final incident report that includes:

    a. Lessons learned and how implemented (current section in USEC investigation report is judged as insufficient by the IE).

    b. Root cause analysis (documented in the final TER) that includes results of dynamic analyses of machine failure mode mechanisms and timing resulting from externally imposed off-normal operations.

    c. Machine design changes resulting from incident

    d. Phased plan for restart of LCs with basis for reestablishing machine full speed operations.

    e. Resolution of any NRC issues.

f. Describe the Commercial plant modifications needed for components, procedures, training, operator QC protocols, etc., that will need to be incorporated formally into the design, operations, maintenance, and training for the commercial plant.

7) USEC prepares a comprehensive "Lessons Learned" document based on the incident that is reviewed by DOE and confirmed by the IE team.

To support Loan Closure:

1) USEC executes machine build-out schedule and operation within LC-3 sufficient to support demonstration of reliability of Ac100 machine (based on prevailing Critical Design Review [CDR] design) and accomplishes demonstration of 20 machine-years (M-Yrs) of operation on gas with failure rates within limits. Any machine design changes resulting from the recent incident requires IE review and verification regarding this demonstration.

2) USEC obtains independent review of BOP root cause analysis (IE also will provide an independent review). An independent reviewer would provide a high confidence level that the analysis was sufficient to determining root causes.

3) USEC performs a BOP - Human Performance FMEA or FMECA for the ACP that is verified by the IE; analysis should determine all single-point failures (e.g., non-functioning equipment that could lead to the destruction of more than one machine) for machine cascade operation and means (e.g., redundancy) to address each (this was referred to as confirming commercial plant redundancy). The recent machine crash incidents all included human performance issues along with BOP system failures that externally impacted machine operation. These calculations need to be brought to the same level of confidence as machine intrinsic availability, as BOP and human performance issues have an impact on overall availability and Separative Work Unit (SWU) production.

4) USEC performs a revised centrifuge FMEA verified by the IE that considers externally caused crashes, where the motive is not to predict the crash – inevitable – but to understand if any unexpected phenomena can arise that would lead to a plant shutdown.

5) USEC integrates cost and schedule impacts from recent incident into integrated baseline that is verified by the IE. USEC has only performed rough calculations of cost and schedule impacts due to BOP and potential machine design changes to date. More detailed estimates are required to provide sufficient confidence in assessing the impacts.

6) USEC completes a CDR of machine design changes to prevent breach during failure including any necessary performance testing, and this is verified by the IE. The CDR is the required machine design Configuration Change Control (CCC) process. Subsequent

changes will require processing through USEC's Change Review Board (CRB), then through a Configuration Control Board (CCB).

7) USEC establishes a staff position with sufficient authority and responsibility to ensure ACP availability is met with implementation of any required corrective actions. The IE believes this position will provide a single point of authority to ensure ACP changes properly consider plant availability critical to achieving success and loan repayment.

B) USEC implements instructions and training for all staff that encourages a 'no hesitation' mindset of staff in using the CATSWEB process to report possible testing lapses which might lead to the beginning of an incident or could exacerbate an abnormal situation. The CATSWEB process has been reviewed in detail by the IE and is well done; it needs to be extended to cover testing gaps. For example, the DG has unique self-preservation circuitry and the UPS has unique capacitive load requirements; these had not been tested together as the testing for the DG was completed before the arrival of the UPS. Gaps such as this should be reportable by any staff aware of it.

XX.8.4 IE Actions to Complete the Incident Evaluation

Another IE review should be scheduled when USEC Oak Ridge staff is ready to present their final technical analyses. USEC Oak Ridge staff are still a few weeks away from completing analysis of 'failure mode mechanisms' (e.g., using dynamic modeling) so IE staff are not yet able to fully judge the impact of potential machine design changes on machine reliability and performance, although some expected performance impacts were generally discussed and noted as minimal.

It is necessary to establish the vulnerability of the loan payback to a multi-centrifuge incident that involves a plant shutdown. It is clear that it is a normal operating situation to have occasional machine failures and even some crashes, and these are worked into the maintenance schedule. This has even been incorporated into the simulation of installation to determine that a reasonable failure rate will not impede build-out at the desired maximum rate.

However, there is no contingency for multi-centrifuge problems taking out substantial numbers of centrifuges. It is necessary to use the financial modeling tools to determine what would happen if an incident occurs and 'N' machines are knocked out, and the plant shut down for 'T' days. Sufficient analysis needs to be done to determine what the effects on loan payback are if, for example, a cascade is blown out and causes a 60 day shutdown. The financial models could show that cascades can be lost without a financial catastrophe occurring. They may show that it is necessary to lose a whole train, or a half-building, for the loan to be in jeopardy. This modeling may be done using the simple model built to support the IER and the USEC financial model itself.

This modeling should provide an understanding of the vulnerability of loan repayment to the situation where there is a grave oversight and a combination of events happen, similar to what happened on June 11th. The models should take into account that the demand for enrichment

has been negatively impacted by the March 2011 Fukushima nuclear accident. This accident would translate into lower demand, and therefore a lower SWU price.

The IE should provide an independent assessment of USEC's calculation of delays and costs resulting from the June 11th incident. These values were roughly calculated and presented to DOE Under Secretary, Office of Science and Technology. USEC needs to complete the cost and schedule impact analysis with IE verification.

The IE should review the design changes developed to cope with the breach problem by monitoring the CDR process and reviewing the analysis on behalf of and in conjunction with DOE.

The IE should monitor the FMEA work done at Piketon and Oak Ridge to ascertain for DOE that there is little likelihood left of a multi-cascade problem, or at least one in which a large number of centrifuges in the commercial plant could be damaged.

XX.8.5 Risk Issues and Recommended Mitigation Actions

IE staff believe that IER risk No. 1B, "*Poor Conduct of Operations and Conduct of Maintenance Practices and Procedures Resulted in Excessive Human Errors Causing Recent Machine Failures*" should be raised to "Significant" with risk mitigation focused upon USEC completion of noted FMEA work including BOP – Human Performance FMEA for the LC as a precursor to performing an ACP FMEA; along with an updated centrifuge FMEA that is expanded to include externally caused failures, not simply focused on providing redundant controls so there will be no externally caused failures, but also focused on examining what would happen if redundancy failed for some reason. The IER risk Table Error! ***No text of specified style in document.-1*** showing risk No. 1B is included for completeness.

Table Error! No text of specified style in document.-1 - Summary of Concerns/Risks

Item	Concern/Risk	Original Risk Level	Updated Risk Level	Notes On Update	Potential Mitigations	Section
18	Poor Conduct of Operations and Conduct of Maintenance Practices and Procedures Resulted in Excessive Human Errors Causing Recent Machine Failures	Moderate	Significant	USEC recently experienced two machine failures at the K-1600 centrifuge demonstration test facility resulting from an operator procedural error and an incorrect valve installation by maintenance staff. There are significant differences in procedures governing centrifuge machine operation and maintenance procedures between the K-1600 test facility in Oak Ridge TN and the ACP facility in Piketon OH that should preclude similar events (e.g., ACP operator training is nuclear facility oriented as governed by NRC; ACP operations and maintenance procedures are more comprehensive; ACP will have steady state production operation) that mitigate the risk level for these types of events. The IE notes that NRC review for license purposes does not include review of all issues that could impact loan servicing, although there are overlaps. USEC has not performed Failure Modes and Effects Analysis (FMEA) for human errors or other non-technical errors as was done for technical failure modes to identify critical ACP operations and maintenance procedures that could lead to machine failure. The IE regards FMEA as a superior means of identifying failure modes and mitigation actions and further regards the adoption of FMEA for machine design following the first IE report as an important factor in achieving the current level of machine reliability. *Continued below*	• Perform human error FMEA to identify critical ACP operations and maintenance procedures that could lead to machine failure and implement risk mitigation actions to prevent or preclude such failures (e.g., use two-man rule check of critical machine operation procedure steps; automation of machine operation steps with software interlocks to prevent missing key procedure steps; implement nuclear facility type machine startup procedures that require signoff when procedure steps are started and completed; implement sensors and interlocks as required to prevent machine failure and machine-to-machine propagation due to valve failures. • IE should conduct a thorough review of the ACP operations and maintenance procedures to ensure USEC has properly evaluated human error failure modes in operation and maintenance planning.	(Sec 4 Tech, Sec 6 Operations and Maintenance [O&M])

Item	Concern/Risk	Original Risk Level	Updated Risk Level	Notes On Update	Potential Mitigations	Section
18 (continued)	Poor Conduct of Operations and Conduct of Maintenance Practices and Procedures Resulted in Excessive Human Errors Causing Recent Machine Failures	Moderate	Significant	*(continued)* USEC stated that it had estimated the number of machine failures related to Human Performance Errors and Balance of Plant equipment based on Lead Cascade experience and showed that expected number of machine failures in the plant related to human error is small and therefore should not rise to the level of a concern. The IE believes estimates of human failure rate completed before a major build out of centrifuges are useful, but not sufficient to demonstrate that human error is an insignificant problem. USEC has not made any convincing arguments that failure mode analysis should not be done for any major category of errors that could have machine damage as a consequence. The IE will consider the VTM operation strategy as part of the solution to this IE recommendation. The IE believes the current level of uncertainty at Piketon regarding the potential for machine damage from human error represents a risk. The IE has received no evidence that rules out the potential for analogous failures at Pikelon. The IE intends to conduct more thorough review of these procedures to ensure USEC has properly evaluated human error failure modes in operation and maintenance planning.		

XX.9. Technical Appendix

Following technical sections were developed with more details of the equipment and its interactions during the incident as part of the investigation evaluation. They are included here for completeness. No section is included for the centrifuge itself for classification reasons. These detailed summaries are based on discussions between IE staff and USEC operations and maintenance staff to confirm reports within the USEC Investigation Report.

XX.9.1 Electrical Fault

To verify the root cause analysis of the electrical portion of the incident, the IE team observed the electrical substation where the fault occurred as it was being disassembled, reviewed electrical circuit diagrams, interviewed various staff, including the Piketon electrical program leader, viewed electrical ampere-measuring equipment of the type used to diagnose the lead cause analysis, and formulated a detailed cause-and-effect sequence of the event. No discrepancies with USEC's views were noted.

The initial short occurred in the circuit that powers the MCW pumps as well as some vacuum pumps and building equipment. The short was initiated by arcing on one phase of the power line feeding this equipment. The original arcing occurred at a 'stab', which is a U-shaped prong that fits over a busbar. This phenomenon is a well-known problem in the industry, and there are industry standards for preventing it. The usual cause of this is from temperature cycling: As a contact is used and then de-energized, a temperature cycle will occur which causes a slight deformation of the contact members, which may lead to less contact area. This leads to higher current per area through the contact area, leading to higher temperatures, more deformation, and eventually a reduction of the contact area to such a small amount that the copper at the contact point melts, separating the contacts. Then, arcing will occur, which will serve to melt or vaporize more of the copper.

In the substation under question, the arcing occurred about 15 cm over a point where the substation metal, which was grounded, held the busbars in place with insulation in between. The melted metal fell, leading to a short between the busbar and ground, which ionized air in the vicinity, leading to arcing and shorting of all three of the electrical phases. It was quite obvious from the panel where the damage was.

Industry standard PM calls for this type of substation to be inspected at five-year intervals, with temperature measurements made of the contacts to determine if one or more of the contacts is at a higher temperature, indicating some deformation has started. If it had, the contacts would be replaced. This substation had been refurbished in 2005, and was due for PM in 2010, but the PM was deferred for two reasons. One was that the LC was only due to be run for one more year and then the substation would be retired. The other was that the initial two years of the period saw little use of the power, as the initial cascade was not installed. It did see use in the testing of various components and some minor BOP loads. In the IE's opinion, it was a reasonable decision to postpone the PM, but the consequences were significant.

Other possible root-causes, other than thermal cycling of the stab, were investigated. One suggested was a problem with the MCW pump, as that was the action that called up on the power that initiated the event. Scenarios involving the MCW pump were talked through and dismissed, based on the action of the various ampere measuring equipment and circuit breakers that are installed. The circuit breaker leading from the substation to the MCW pump did not fire, and if that pump had been drawing too much power during its start-up phase, it would have been caught. The MCW pump current, moving through the substation, did lead to the initial melting at the stab, but this melting can be done with either the start-up pump power or the running pump power, providing the contact area has been sufficiently reduced. Each circuit breaker in the substation has an electronic monitoring component, which measures current and trips on any one of three conditions: high instantaneous load (time being the physical time necessary to open the circuit), high short-term load, corresponding to starting transients, and high long-term load, corresponding to a load operating for longer than the settable transient time at higher than rated load levels. The action of the ampere measuring equipment on the circuit breaker covering the fault area was to detect an instantaneous high-load, as opposed to a longer, less-high load, indicating some direct short rather than an overload situation.

Some conclusions can be made:

1. The root cause of the entire incident was the failure of a busbar contact in a way well-known to the industry; all physical evidence points to this; the evidence was witnessed by the IE.
2. The circuit protection functioned as expected and appears to have been well-designed in the GCEP era – the damage to the busbars was much less than it could have been had the circuit breaker not been very fast-acting.
3. The design of the circuitry was such that the diesel power backup fed through the same busbar which shorted out and eliminated main power.

Some recommendations can be made:

1. A failure modes analysis appears not to have been done for the LC BOP and doing so might provide important clues for the completion of the failure modes analysis for the commercial plant – doing at least a first level of this analysis should be accomplished to eliminate other incidents of the magnitude of this one.
2. If not already done, PM should be done for all electrical and other subsystem components for the LC to ensure that the LC will be able to accumulate the number of machine hours required to establish the reliability of the commercial plant centrifuge design.

XX.9.2 Inverted Controls on MCW Pump Discharge Valves

When the UPS was turned off, besides de-powering the DCS, it also de-powered the MCW pump valve electrical controls, a Programmable Logic Controller (PLC) which manipulates valves on the discharge side of the pump. The MCW pump provides cooling water to the centrifuge drives, the diffusion pumps, the purge pumps, and the evacuation pumps. When water is discharged under pressure from the MCW pump, it is split into two flows, one of which flows through the heat exchanger and the other bypasses the heat exchanger. The PLC adjusts the division of flow between that entering the heat exchanger and not entering it so that the output temperature is within specified bounds.

When the PLC lost power, power was interrupted to the solenoids controlling these valves, and they reverted to being fully extended, which, at the time of the incident, closed both valves. In normal operations, the two valves operate in opposite directions. When these valves were installed for the LCs, USEC did not pay attention to the power-off setting of the valves, but concentrated on ensuring they tested properly in normal operating conditions.

With no power, there was no cooling water due to these valves. Thus, the diffusion pumps (for both cascades) lost effectiveness, as the cooling water serves to condense the circulating oil that removes gas molecules that enter the pump. The diffusion pump does not damage itself without cooling water. The centrifuge drives, in a no-control-power scenario, continue at the last commanded drive speed. The cooling water serves to keep the lubricant cool. If there is no cooling water, the bearings will heat up and friction will increase. It is not clear what the first item to fail would be if no cooling water is present. This damage mechanism is in competition with that caused by the loss of vacuum pumps, which serve to add drag to a machine which is not capable of coping with speed changes.

Furthermore, the PV pumps and the evacuation pumps receive cooling water. These pumps are similar in design and operation, differing principally in size. The cooling water serves to cool the lubricating oil, which cools the motor in the pumps. If the oil temperature rises beyond a threshold, the internal PLC, which is powered by pump power, turns off the motor, ensuring survival of the pump. There also is an alarm signal sent to DCS.

When the UPS lost power, the discharge valves went into closed position, and the pump was deadheaded. It began to cavitate and create noise, which was noticed by the operators who were in the vicinity of the UPS. Some members of the operational staff attended to the pump, which was the only MCW pump operating at that time. At the onset of the events, the second MCW pump was being turned on, but when the electrical fault occurred, it was returned to a power-off condition.

The closed valves are proportional valves operated by the PLC, and there is a bypass line with a manually operated valve. The operators, once they realized what was happening, opened both bypass valves, restarting the flow of cooling water to the machine drives and the multiple pumps that require it.

Some conclusions can be made:

1. The valve manufacturer supplies valves that have a fail-close setting, and it is necessary to make a modification to the valve for a fail-open setting. The GCEP team did not make these changes, most likely as an oversight. The settings were not checked during the restart operations. Loss of cooling water represents a further possible failure mode. If the PLC had failed instead of the UPS being powered down, and no one was in the vicinity of the MCW pump to hear it react to being deadheaded, it may be possible that the pump could have damaged itself after running in this situation for an extended period.
2. It is not clear that there is adequate knowledge of the time window for MCW pump failure, PLC failure, valve failure or other phenomena relating to the loss of cooling water, during which the components which receive that power would damage themselves or other equipment.

Some recommendations can be made:

1. The LC support equipment, including all components that could create damage, should be checked to see if the programmed diagnostics to reveal this to the operating staff are available during normal and abnormal operating condition. It also should be verified that adequate time is available to respond, that mechanisms exist to respond with, that procedures are available to lead the operating staff through the responses, and that training on the procedures is done to familiarize the staff with these contingencies.
2. USEC might consider expanding the scenarios they use in training staff to include any situations found in the analysis of cooling water related incidents.

XX.9.3 Diesel Generator Use during the Event

There is one DG that is installed to provide backup power to the two LCs. This generator is designed to automatically come on when the main power disappears. It can be used manually to deal with situations with partial power failures, such as occurred on June 11th.

When the electrical short occurred, and one of the substations had its circuit breaker tripped, there was a short, temporarily, preventing power from being applied to the loads that are fed from this substation. As long as the short was in place, it would make no difference whether diesel power was applied or main power was re-connected; no feed of power to those loads would be possible. USEC personnel attempted to use the DG to supply power to that substation, and over time their efforts succeeded. It is not clear if there was a residual fault in that substation which was eliminated by the re-application of power, or if the fault had cleared itself in the initial flash and the DG could not be applied due to faults within the circuitry connecting the generator with the substation.

Experiments following the event determined a cause for the failure to connect the generator with the substation: a voltage measuring sensor at the output voltage of the generator was

sensing the fall in voltage when a load was applied, and when the voltage drop reached a threshold (92 percent of nominal for a fraction of a second), it would trip a relay, dropping the load at the generator. It was found that this relay would trip for even small loads being applied. If there was a residual fault, even with only a moderate current drain, or if one of the breakers that had been manually tripped to remove all loads from the substation was still on, the relay still would disconnect the generator. The typical drop in voltage was close to threshold, meaning that the firing of the relay was intermittent; it depends on external conditions, such as the presence of external power. USEC has resolved this problem following the incident by adding circuit modifications that do not let this relay trip until the low voltage condition has persisted for seconds, which is much longer than any observed drop in voltage.

There are multiple other protective circuits in the DG output circuit that serve to prevent damage. The DG has been tested multiple times.

During the testing, a substation was used for load testing but not the one that failed. Instead the one providing main power to the UPS was used. It was found that the UPS, with its very large capacitive impedance caused by its input filters, impose a large voltage drop on the generator; it would not have been possible to use the DG to restart the UPS had the fault been in the substation providing main power to the UPS rather than bypass power. This also was remedied by the delay circuit modification. This problem was not detected at time of installation of the DG because the UPS was not installed until after the time when the DG was being tested.

Some conclusions can be made:

1. The DG was insufficiently tested for the roles it was expected to serve, specifically to restore main power and to restore power during a partial power failure.
2. There does not seem to be any way that the existence of a residual fault in the damaged substation can be determined. Whether DG circuit problems or a residual fault prevented the restoration of power will remain unknown.
3. The DG was able to be made capable of serving its purposes by a minor change in the circuitry used to monitor its output.

Some recommendations can be made:

1. Even though the LC is only a stepping-stone to the commercial plant, a significant amount of operational knowledge can be learned by examining its possible failure modes and extracting lessons learned for the commercial plant.
2. USEC might consider devoting a small fraction of personnel resources to exploring whether or not the backup systems will operate in abnormal environments.

XX.9.4 Response to UPS Loss of Power

In the process of responding to alarms for the electrical fault, an operator went to the UPS to respond to alarms from it. This is part of the standard procedure. The operator inadvertently pressed the Emergency Power Off switch, which turned off the UPS completely, and isolated it from both input and output. This should not have been done, as the switch is only for UPS safety, and there was no known threat to the UPS at that time.

Operators immediately recognized the problem and retrieved the vendor's manual for the UPS. Because of the electrical fault, there was no bypass power to the UPS, but there was still main power. However, the vendor's manual does not have any procedure for restarting the UPS when there is no bypass power available. If there is bypass power, there are two routes inside the UPS to bring that power to the output, but there is no connection within the UPS to use main power directly in a bypass mode. There were no procedures written by USEC on restart of the UPS; they intended to rely on the vendor's manual.

Lacking any information on how to restart the UPS with no bypass power, the operators attempted to restart it by trying various sequence of switches, using the circuit diagram in the vendor's manual, and portions of the existing startup sequence. This took approximately 45 minutes. The operators were concerned about the possibility that a trial-and-error approach would damage the UPS and make the existing situation even worse. They believed that attempting to start it from battery only was more dangerous to the UPS than trying to start it using main power, and attempted to overcome automatic trips in the UPS circuitry which interfered with some of these attempts. There is a sequence of manual throws of circuit breakers that allowed UPS output power to be restored.

Some conclusions can be made:

1. For some reason, no one at Piketon seems to have evaluated the possibility that UPS power would be down in abnormal situations. For normal situations, the UPS vendor's manual would have sufficed to restore operations. However, there was little or no training with restarting UPS in either normal or abnormal situations, and the vendor's manual is somewhat unclear about where various switches and bypasses are located, as well as being fairly complex.
2. The UPS and some circuitry surrounding it are a single point failure, and if the UPS were to be destroyed, there is no option left for saving any of the running machines. No machines can be controlled without UPS, and they could only be spun down by turning their power off, which would likely destroy them.

Some recommendations can be made:

1. The LC and support equipment should be checked to see if there are any other single points of failure. USEC believes that backups for all systems exist in the commercial plant design, but this should be verified.

2. New procedures have been written to deal with the situation on UPS restart, but there is no plan to test these in abnormal situations. USEC should consider if there is some way of testing this without great cost or loss of operational time.

XX.9.5 DCS Operations

The DCS serves as the controller of the cascade piping system and the individual centrifuges. It also serves as the interface between both the various controllers that work valves or other devices as well as the sensors taking readings and the operators in the control room.

The DCS consists of two pairs of servers for each cascade. The pairs are redundant, being identical – one works while the other monitors and records data without sending control signals. One of the two pairs interfaces with the valve system for the cascade and the other pair interfaces with the centrifuge controls. There are at least three relevant power sources: one for DCS, which was not taken down during the incident, one for the machine drive power, which was also not taken down during the incident, and the UPS-provided power network, which includes the MIP, much of the Ethernet communication system between the DCS and the cascade systems and individual machines, the PV controller, the MCW controller, and the battery room fan (a component identified as an IROFS).

DCS displays to the operators include machine-specific displays, piping-specific displays, and electrical system-specific displays. The first two allow operators to make manual control changes or to override some automatic control, but the third only provides monitoring information.

When the problem began, DCS showed problems with the electrical network, which had been subject to a short circuit. Operators followed procedure and stationed one operator at the UPS cabinet to manually make any settings necessary; this is a procedure choice designed to eliminate any communications problems between the DCS controller for the UPS and the UPS itself. Instead of using DCS screens to manipulate the UPS settings and quiet alarms arising from it recognizing that the backup power had disappeared and was being started and stopped from attempts to substitute diesel power, an operator was stationed at the UPS cabinet, manipulating the buttons available there. That operator inadvertently killed the UPS with the emergency off button.

With no power to the PV system controllers, the machines were automatically isolated by the automatic response of the Secondary Isolation System (SIS) to a lack of controller power. Isolation means both that feed and withdrawal connections were closed, but also PV valves are closed. Machines outgas at all times. This would mean that pressure in all of the machines would increase, some that had run a long time, very slowly and others, faster.

With no power to the MIP system, the Machine Drive Unit (MDU) would continue to maintain the last commanded speed. Eventually, increasing pressure would overcome this and lead to failure by one of several possible modes.

When UPS power came back, the two controllers that govern connection between the MIPs of the two cascades and the DCS rebooted. They have the capability to 'warm boot', which

means they would re-start immediately. The LC-3 system did this properly, but the LC-1 system did not – it had been set to go to 'idle boot', in other words, it turned on and waited for a command from DCS to begin operating and order the MIPs under its control to resume commanded operations.

The PV controller systems are older, and can only come back to 'idle boot', and waited for commands from DCS. Thus, the system initially stayed in isolation, meaning that those two machines continued to experience higher drag, and destroyed themselves. The PV controllers and LC-1 MIP system were brought out of idle state in sufficient time to preserve all other machines.

Three emergency options are known that could have rescued these machines, however, these options require control of the machines for sufficient periods of time. Time was lacking.

The operators have the option for turning the three systems from 'idle' to operating status, but their training did not cover this, and the controls were buried deep in typically unused menu areas. Thus, they had to wait until an analyst was on site who understood the restart options within DCS for both a MIP controller and a PV controller. The two machines closest to crashing did so, but the rest were prevented from crashing.

Operators do not gain experience in making a transition from idle state to operating state when machines are added to a cascade, as the PV systems start when the first machine is added to the cascade and remain started continuously from that time, and the MIP system for a new machine is automatically started up when it is connected.

Some conclusions can be made:

1. USEC management has stated that operators are drilled in various scenarios so that they can respond well under any circumstances. Clearly the scope of those circumstances did not cover the situation which actually occurred.
2. USEC operators understood when they were beyond their depth of knowledge, and had the contact resources available to them to be able to summon assistance.

Some recommendations can be made:

1. An independent party, perhaps a team from Oak Ridge, should be used to re-evaluate the scope actually needed for the procedures to be used at Piketon's control room. Piketon is re-looking at this and has made progress here, but a set of fresh eyes would be useful in avoiding another recurrence of Murphy's law.
2. The operators at Piketon give the impression of being quite capable, and therefore, competent to deal with more depth of control, at least in emergency situations, that they had been allowed to access before the accident. Control of communications servers were reserved for analysts. It is fortunate that a knowledgeable analyst was available rapidly to perform the necessary actions. Changes have been made to grant them this single capability. A good look should be taken to see if there are other

capabilities that should be added to the operators' repertoire – analyst help may not always be available.

The IE team concluded that this complex incident was not instigated by any design flaw, manufacturing shortcoming, or installation error in the machines, but were instead caused by preventable human error compounding a support equipment malfunction. These errors can and should be remedied without significant delay or risk to the program.

The IE team recommends that a thorough FMEA for the plant, for human operator error, for other human error, and for software flaws be completed and documented at Piketon, and that this be reviewed by the IE team to ensure that no failure modes exist that could place the completion of the validation of machine reliability in question. These failure modes should not be restricted only to normal operating conditions, but should cover situations similar to those which initiated this incident. Until such time as this issue has been addressed, it represents a risk to the program. (See IER Section 2.2, Risk Item No. 18; see also table shown in Section XX.8.5)