~~Confidential~~

FULL INVESTIGATION REPORT

Date of Event	Location of event	ATT ref: 09514339
15/10/09	[redacted]	DCC Ref: [redacted]/F-SRI/09514339

Event Title
Temperature Excursion on furnace "C" in [redacted]

Event Type
Safety

[redacted] *Signature* *Date 9 February 2010*
ITU Representative

[redacted] *Signature* *Date 9 February 2010*
NITU Representative

[redacted] *Signature* *Date 9 February 2010*
Facility Manager

[redacted] *Signature* *Date 9 February 2010*
Approval Panel Chair

[redacted] *Signature* *Date 9 February 2010*
Lead Investigator

Severity Level: 2 Reportable to HSE/NII/MOD/EA/Security/Other Details

KEY LEARNING POINTS
Company Wide: Always consider the maintenance aspects of equipment. Do not assume an as built design is safe.
Locally:

Express ABNORMAL EVENT report reference: [redacted]/F-SRI/09514339

INVESTIGATION SUMMARY:

On 15/10/09 a [redacted] operation was taking place in furnace "C" of workstation [redacted]. There are three furnaces in [redacted] and they are lettered A, B, C. The operation involved raising [redacted] samples to [redacted] and maintaining that temperature for one week. Approximately [redacted] was in the furnace. The operation was started on 14/10/09 at approximately 09:55 hours when the furnace was loaded with the samples and switched on. At 11:45 hours on the same day the furnace was checked by the Operator and the indicated temperature was approximately [redacted] As the desired temperature had not been reached the Operator made a fine adjustment to the temperature dial. The Policeman thermocouple was set to trip at [redacted]. On 15/10/09 at 11:25 hours the Operator checked the furnace and found the indicated temperature was [redacted]. He immediately turned down the furnace set temperature dial to [redacted] and the indicated temperature immediately started to drop. The vacuum pump was not switched off at this time as this stops radiated and conducted heat leaving the outer surface of the furnace. After approximately one hour the furnace chamber temperature had reduced to [redacted] and the power was then switched off by the Operator by operating the main power switch on the control cabinet. The [redacted] Facility Manager requested that this furnace was electrically isolated and the use of

all Bay [redacted] furnaces restricted until further notice. Since this incident a cross Facility review of all active furnaces has taken place to check for similar designs and issues; none were evident.

DESCRIPTION OF EVENT:

On 15/10/09 an operation was taking place in [redacted] to heat two small samples (less than [redacted] total weight) of [redacted] to approximately [redacted] for seven days. The operation was started on 14/10/09 at approximately 09:55 hours. Nothing unusual happened during the start-up. The two samples were contained in a small aluminium tin and this was suspended from the lid of the furnace in a small metal basket fabricated from thin stainless steel wire. The operation was set up by Bay [redacted] Front Line Workers (FLW) and the actual operation was run by a Bay [redacted] Scientist. The Safety Policeman thermocouple was set to [redacted]. The Safety Policeman thermocouple is set to [redacted] as [redacted] melts at approximately [redacted]. At approximately 11:25 hours on 15/10/09 the Operator found that a temperature excursion had taken place and the furnace temperature had reached an indicated [redacted]. The operations carried out in this workstation are in support of the Trident Lifetime Assessment programme.

INVESTIGATION FINDINGS:

There are three furnaces in workstation [redacted]. The furnaces are [redacted] furnaces which can be used for [redacted] of small samples of [redacted]. Furnace A is used for [redacted] up to [redacted] but is currently non operational and has been extensively cannibalised for spare parts. Furnace B is used for [redacted] in oil at room temperature and was operational at the time of this incident. Furnace C is designed for [redacted] in oil at temperatures down to [redacted] and was operational at the time of this incident.

The furnace temperature is controlled by Eurotherm 818 temperature controllers. To achieve a furnace temperature of [redacted] the Eurotherm temperature controller has to be set to approximately [redacted]. This temperature difference is due to an inherent lag between the temperature controllers and the furnace temperature. Also included in the furnace controls is a Policeman thermocouple which should trip if a temperature excursion occurs.

On 15/10/09 an operation was taking place in [redacted] to heat two small samples (less than [redacted] total weight) of [redacted] to approximately [redacted] for seven days. The operation was started on 14/10/09 at approximately 09:55 hours. Nothing unusual happened during the start-up. The two samples were contained in a small aluminium tin and this was suspended from the lid of the furnace in a small metal basket fabricated from thin stainless steel wire. The operation was set up by Bay [redacted] Front Line Workers (FLW) and the actual operation was run by a Bay [redacted] Scientist. The Safety Policeman thermocouple was set to [redacted]. At 11:45 hours on the same day the furnace was checked by the Operator and the indicated temperature was [redacted]. As the desired temperature had not been reached the Operator subsequently adjusted the Eurotherm temperature controller to [redacted] by adjusting the temperature dial. The furnace was not checked again that day. On 15/10/09 at 11:25 hours the Operator checked the furnace and found the indicated temperature was [redacted]. He immediately turned down the furnace set temperature to [redacted] and the indicated temperature started to drop. The vacuum pump was not switched off at this time as this prevents radiated and conducted heat leaving the outer surface of the furnace. When the chamber temperature reduced to [redacted] the power was switched off at the main control panel by the Operator. From the computer traces it would appear that the furnace was at [redacted] for approximately 2 hours.

The [redacted] Facility Manager requested that this furnace be electrically isolated and that all Bay [redacted] furnaces be placed out of service and electrically isolated until further notice. All Out of Service Certificates in [redacted] are managed by the [redacted] Operations Control Centre.

[redacted] containment was not affected by this temperature excursion, a thorough precautionary investigation of the containment took place on 20/10/09 by Health Physics and a Bay Supervisor. The [redacted] window seals were examined as were the [redacted]. No degradation of materials or containment was evident. It cannot be determined what temperature the [redacted] reached internally. The [redacted] Control Room received no alarm from the [redacted] fire sense system. The high temperature alarm threshold is nominally of the order of 90°C but this is dependent on the fire sense cable length. Some [redacted] may alarm as low as 45°C. It can therefore be assumed that the internal [redacted] temperature did not exceed 90°C. [redacted] structural integrity as a Primary Containment boundary will withstand the thermal loading from a single [redacted] fire at maximum CCC inventory (for non bulk metal) inclusive of any additional thermal loadings from other [redacted] combustibles at normal process limits. This withstand requirement is set by SFR [redacted] cont-01 and SFR [redacted] cont-28 in Safety Functional Requirement [redacted] AS/SF/266.

A recovery procedure took place on 19 November 2009 under WAF 81450. Furnace C was dismantled and the two [redacted]s were recovered intact from the bottom of the furnace, the aluminium container which

held the samples had melted as had the stainless steel wire basket.

The furnaces in workstation [redacted] are not subject to planned maintenance. They were subject to breakdown maintenance only. Consequently none of the safety interlocks (Inner [redacted] Restraint, Policeman Thermocouple, [redacted] Guard, and [redacted] Pressure) have ever been tested. The Operating Instruction ([redacted] and [redacted] Furnaces [redacted] [redacted]/OI/R&D/81) does not specifically request that a test of the Policeman thermocouple should take place. The only requirement in the Operating Instruction is to "check that the Eurotherm over temperature sensors located in the power control cabinet have been set to a suitable temperature – the over temperature sensors protect the samples in the event of a furnace overshoot".

The Operating Instruction requires reviewing and updating. For example the temperature set points are user defined and there is no indication as to what these should be set to, there is no indication on simple tests of the safety interlocks and there are no contingency procedures, for example the procedure to follow if a temperature overshoot occurs.

It cannot be determined whether the Policeman thermocouple was functioning even though it had been set to [redacted]

The last time this furnace was operated without incident was 29th September 2009, this was evident from logbook records.

Although the Operator turned down the furnace set temperature to [redacted] when he discovered the temperature excursion, it is not clear whether this action actually caused the furnace temperature to drop as when the C&I Engineer carried out his initial investigation he found that a miniature 6 amp circuit breaker (MCB6) had tripped. This MCB protects the supply to the furnace heating coils and it is situated at the lower front of the power control cabinet. None of the staff interviewed during the investigation had touched this MCB. It cannot be determined when the MCB tripped, however it is evident that it may have tripped about the same time that the furnace temperature set point was turned down as the computer traces show the temperature overshoot was maintained to approximately the same time the furnace set temperature control was reduced to [redacted]

A technical investigation started on 14 January 2009 (Ref [redacted]REP/FDA/102). This investigation took place with power reinstated to the control system but with the furnace heating coils electrically disconnected.

The quality of the circuit drawings have caused difficulty during the technical investigation. It has proved difficult to read the drawings to determine the true layout of the circuits due to the drawings being spread over five sheets. Some inaccuracies have also become evident particularly in the power and alarm circuitry.

Initially the drawings of the alarm panel were not available. The Control and Instrumentation Operative contacted the manufacturer (CVT) and managed to obtain a set of drawings for the alarm module. On examination of the drawings it became evident that the only interlocked alarms are [redacted] pressure and [redacted] restraints. An over temperature alarm is present but it is not interlocked and will not cause the main power contactor to drop out and remove power from the heating coils.

The relay taken from furnace C was inspected and it was observed that on the normally open contact the metal pad had completely been eroded and deposited on the common contact indicating that the contacts had indeed stuck together at some point (See picture below).

The conclusions from the Technical Investigation are that (a) the control system is working correctly and (b) the contacts on Furnace C relay have at some point been stuck together making the output to the heater uncontrollable.

It is now evident therefore that a "single point of failure" exists in the power supply to the furnace heating coils, this being the contacts of Furnace C Relay. If the contacts of this relay do not open, a voltage will be applied to the furnace coils that cannot be interrupted. Due to the circuit design an over temperature alarm cannot cut the power to the furnace heating coils if the contacts of Furnace C relay remain closed.

There is no evidence that any operational instructions were violated although it is noted that the Operating Instruction is weak in key areas.

The recently completed HAZAN ([redacted]PRS/C1/AP/11) contains a Hazard Category 1 Shortfall on this system. Design Basis Analysis has identified that there are no engineered safety measures to support or perform a DB2 Class safety function with respect to protecting the Operator from a contaminated burn hazard arising from a range of plant faults and Operator errors. Plant faults include process control failure leading to an over temperature excursion and incorrect display of temperature data. Operator error includes incorrect setting of temperature set points and inadvertent unloading of a sample while the furnace is still at temperature.

In addition to the above shortfall, the HAZAN identifies that there are engineering deficiencies associated with the application of over temperature protection and the [redacted] guard interlock in that both facilities are implemented via the process controller. Hence these systems cannot be claimed as part of the DBA analysis. Furthermore, there are a number of claims made within the DBA analysis that require substantiation (and which cannot be inferred from other, existing substantiation, mainly relating to the Zone 1 containment boundary).

This equipment cannot be used again until this shortfall (which comprises 8 separate actions) has been cleared.

This investigation has also concluded that a single point of failure exists in the furnace heater control circuit. Therefore this furnace cannot be used until additional interlocks have been incorporated in the heater supply. The electrical supply wiring to the furnace is below current standards, it is thinner than currently required for the voltage it carries and should therefore be replaced.

As a result of this incident, a review has been undertaken of the active furnaces available for use within the Facility. This review drew heavily upon the Engineering Substantiation work which was recently completed to support the Facilities Periodic Review of Safety. As part of this review it has been confirmed that the remaining furnaces in use across the [redacted] Facility are subject to regular periodic maintenance. The substantiation work has also reviewed the adequacy of the control systems against that expected against modern standards. Where shortfalls have been identified, arrangements have been made and implemented via the [redacted] ALARP panel to make relevant improvements to the affected furnaces.

CONCLUSION and CAUSE ANALYSIS

This equipment has been operated for many years without significant incident. Engineering weaknesses exist in this equipment and the incident was exacerbated by a lack of planned maintenance. This equipment had been identified for rekit which will involve replacement of the control unit. Once the new design has been finalised it will be subject to Engineering Substantiation review. The furnaces in workstation [redacted] will remain out of service until this has taken place.

Since this incident, a review has been undertaken of the active furnaces available for use within the Facility. The remaining furnaces in use across the [redacted] Facility are subject to regular periodic maintenance. The adequacy of the control systems has been checked against that expected against modern standards. Where shortfalls have been identified, arrangements have been made and implemented via the [redacted] ALARP panel to make relevant improvements to the affected furnaces.

Immediate Cause: 4.2 Inadequate or defective design. Single point of failure (Relay 13) in power supply to furnace heater coils.

Underlying Cause: 1.1 Defective or failed part – Contacts of relay welded together, consequently power to furnace coils could not be interrupted.

Underlying Cause: 1.7.2 Inadequate Preventative Maintenance – Furnaces not subject to Planned Periodic Maintenance and test.

State Number of attached non-conformance 303s
QA303's:
None. The currently installed electronics will be replaced during the planned rekit activity. The category 1 PRS shortfall on this equipment requires that five actions be cleared before this shortfall is downgraded to a category 2. Completion of these actions would have highlighted the engineering weaknesses and the lack of periodic maintenance had this incident not occurred.

Lessons Learnt:
Always consider the maintenance aspects.

Distribution via ATT office:

Assurance Director	Relevant Director of Management Unit		Relevant Facility Manager
HoHS	Relevant HoAS	MOD IPT	HSy (if appropriate)
All Internal Regulators	ITU Office	NITU (SA)	Further as requested

PROTECTIVE MARKING
UNCLASSIFIED