Application of Design Basis Accident Analysis (DBAA) at Sellafield, United Kingdom

James Rendell
DBAA – the Basics

• Initiating Event

“A fault condition arising from a failure of item or person which, if combined with any necessary detrimental circumstances, and in the absence of correct functioning of safety measures, would give rise to consequences.”

• Basket Safety Measures
DBAA – the Basics

Potential Consequences to Worker (mSv)

Initiating Event Frequency (per year)
DBAA – the Basics

DBAA

PSA

ALARP
Example Fault: Initiating Event is Difficult to Define
Mechanical Handling Accident in the Fuel Handling Plant (FHP)

Simplified Process Overview

- Irradiated AGR fuel elements arrive at FHP in a skip within a flask.
- The skip is transferred into a container, whose lid is locked.
- The container is dispatched to the pond where fuel is stored until ready for dismantling.
- Containers are removed from the pond and elements are removed from containers for dismantling.
- Fuel pins from three elements are put in each can.
- Cans are put in skip compartments before containers are locked and returned to pond.
- Currently, containers are only double stacked but need to assess triple stacking.
Example fault: Initiating Event is Difficult to Define
Mechanical Handling Accident in FHP
Example Fault: Initiating Event is Difficult to Define

Mechanical Handling Accident in FHP

Operator error when inputting data into the Skip Handler Machine.

Maloperation of Skip Handler Machine (SHM) Software.

OR

Collision of fuel container with triple stacked ACR fuel container.

Failure of SHM mast tilt interlock.

This triple-stacked container is adjacent to at least 1 double-stacked container, and motion of the SHM is towards this direction.

Criticality in the storage pond resulting in dose to an operator at pond surface.

Collision continues with sufficient maintained force to dislodge the triple-stacked container.

Critical fuel arrangement is piled up to the height of a triple stack.

Fuel pins fall out of container onto the top of a double stack and form an unsafe geometry.

Impact is sufficiently severe and lid falls off quickly enough under water to allow sufficient fuel pins to be projected out of their cans.

Failure of operator to lock fuel container lid.

Triple-stacked AGR fuel container is toppled from stack onto an adjacent double-high stack.

Collision continues with sufficient force to dislodge the triple-stacked container.

Failure of SHM mast tilt interlock.

This triple-stacked container is adjacent to at least 1 double-stacked container, and motion of the SHM is towards this direction.

Criticality in the storage pond resulting in dose to an operator at pond surface.

Collision of fuel container with triple stacked ACR fuel container.

Failure of operator to lock fuel container lid.

Maloperation of Skip Handler Machine (SHM) Software.

OR

Collision of fuel container with triple stacked ACR fuel container.

Failure of SHM mast tilt interlock.

This triple-stacked container is adjacent to at least 1 double-stacked container, and motion of the SHM is towards this direction.

Criticality in the storage pond resulting in dose to an operator at pond surface.

Collision continues with sufficient maintained force to dislodge the triple-stacked container.

Critical fuel arrangement is piled up to the height of a triple stack.

Fuel pins fall out of container onto the top of a double stack and form an unsafe geometry.

Impact is sufficiently severe and lid falls off quickly enough under water to allow sufficient fuel pins to be projected out of their cans.

Failure of operator to lock fuel container lid.

Triple-stacked AGR fuel container is toppled from stack onto an adjacent double-high stack.

Collision continues with sufficient force to dislodge the triple-stacked container.

Failure of SHM mast tilt interlock.

This triple-stacked container is adjacent to at least 1 double-stacked container, and motion of the SHM is towards this direction.

Criticality in the storage pond resulting in dose to an operator at pond surface.

Collision of fuel container with triple stacked ACR fuel container.

Failure of operator to lock fuel container lid.

Maloperation of Skip Handler Machine (SHM) Software.

OR

Collision of fuel container with triple stacked ACR fuel container.

Failure of SHM mast tilt interlock.

This triple-stacked container is adjacent to at least 1 double-stacked container, and motion of the SHM is towards this direction.

Criticality in the storage pond resulting in dose to an operator at pond surface.

Collision continues with sufficient maintained force to dislodge the triple-stacked container.

Critical fuel arrangement is piled up to the height of a triple stack.

Fuel pins fall out of container onto the top of a double stack and form an unsafe geometry.

Impact is sufficiently severe and lid falls off quickly enough under water to allow sufficient fuel pins to be projected out of their cans.

Failure of operator to lock fuel container lid.

Triple-stacked AGR fuel container is toppled from stack onto an adjacent double-high stack.

Collision continues with sufficient force to dislodge the triple-stacked container.

Failure of SHM mast tilt interlock.

This triple-stacked container is adjacent to at least 1 double-stacked container, and motion of the SHM is towards this direction.

Criticality in the storage pond resulting in dose to an operator at pond surface.
Example Fault: Initiating Event is Difficult to Define
Mechanical Handling Accident in FHP

- Event: Maloperation of Skip Handler Machine (SHM) Software.
- Effect: Collision of fuel container with triple stacked AGR fuel container.

Failure of SHM mast tilt interlock.

Collision continues with sufficient maintained force to dislodge the triple-stacked container.

Triple-stacked AGR fuel container is toppled from stack onto an adjacent double-high stack.

Impact is sufficiently severe and lid falls off quickly enough under water to allow sufficient fuel pins to be projected out of their cans.

Operator error when inputting data into the Skip Handler Machine.
Summary

• Where DB2 faults are designated, more safety designations tend to be required to meet the requirements of DBAA than to meet those of the Double Contingency Principle.

• Take care when defining initiating events: don’t take credit for protective measures.

• DBAA should not be considered in isolation, but it is a useful technique to demonstrate defence-in-depth and that operations are ALARP.