APPROACHES AND MODELING TECHNIQUES TO DETERMINE SYSTEM EFFECTIVENESS AGAINST INSIDER COLLUSION

Mark Snell, Sandia National Laboratories
Carol Scharmer, Sandia National Laboratories
Philip Gibbs, Oak Ridge National Laboratory

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525
SAND2017-12162 C

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

NNSA
National Nuclear Security Administration
Defense Nuclear Nonproliferation

Topics

- Introduction
  - Background/history
  - Evaluation methods that could be used
- Potential New Techniques
  - Descriptions
  - Examples

Background

- Historical evaluation approaches
  - For collusion: Modeled "super" insider
- Limits to historical approaches
  - Limited evaluation of preventive measures
    - Focused on people with hand-on
  - "Super" insider scenarios may lead to excessive protective measures
  - Prior technology limits

Potential New Techniques

- Adapting accepted evaluation methods to insider
  - PFMEA-based [Process Failure Modes Effects Analysis]
  - Structured Assessment Approach (SAA)

Process/Procedures Matrix Method

- Based on PFMEA process
  - – Failure Modes Effects Analysis - FMEA
  - – FMEA is a design tool used to systematically analyze postulated component failures and identify the resultant effects on system operations.
  - – PFMEA (Process FMEA) is analysis of manufacturing and assembly processes
- Instead of identifying process failure modes –

Identify potential insider actions that could facilitate a malicious act

https://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis

Process/Procedures Matrix Method

- Result is a detailed database
  - Can be sorted into selectable data sets for analysis
- Analysis can be simple or complex
  - Can examine a single preventive/protective measure
  - Can model multi faceted issues, such as collusion.

Process/Procedures Matrix Method

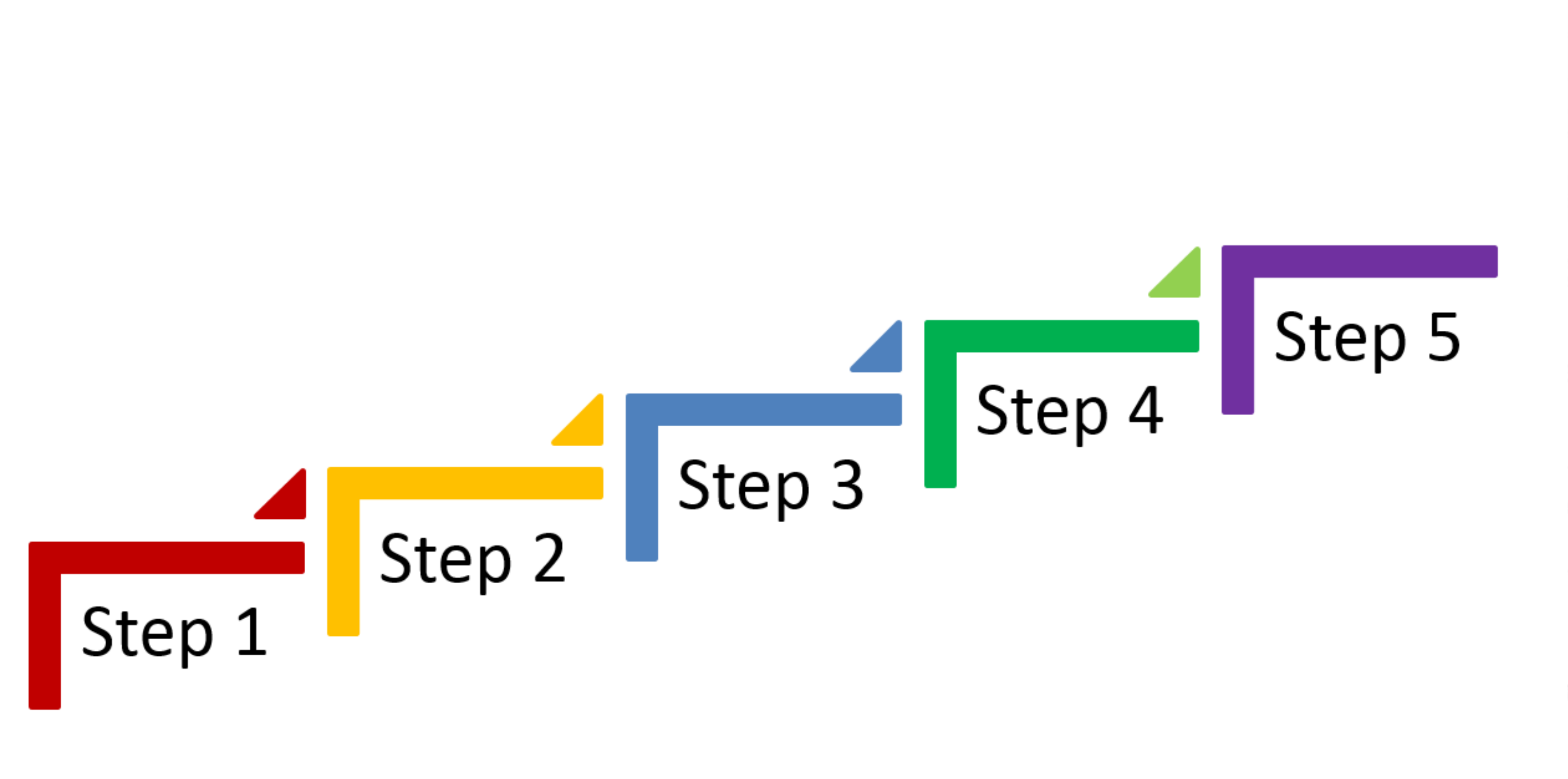
- Advantages
  - – Implemented during design – supports Security by Design
  - – Comprehensively documents the interface between operations and security
    - Defines security procedures – Documentation for Security Plan
  - – Maintain for future use/reference
  - – Results may be used to:
    - Design an insider mitigation program or
    - Identify improvements to an existing program
    - Analyze risks and impacts of changes

Process/Procedures Matrix Method

- Developing the database
  - Requires team that have detailed knowledge of operational and cross-cutting procedures
  - Based on facility operations – existing procedures
  - May immediately identify gaps in protection against insider (or outsider)

Process/Procedures Matrix Method

- 5 step process
  - – Correspond to the first five steps of the PFMEA



Process/Procedures Matrix Method

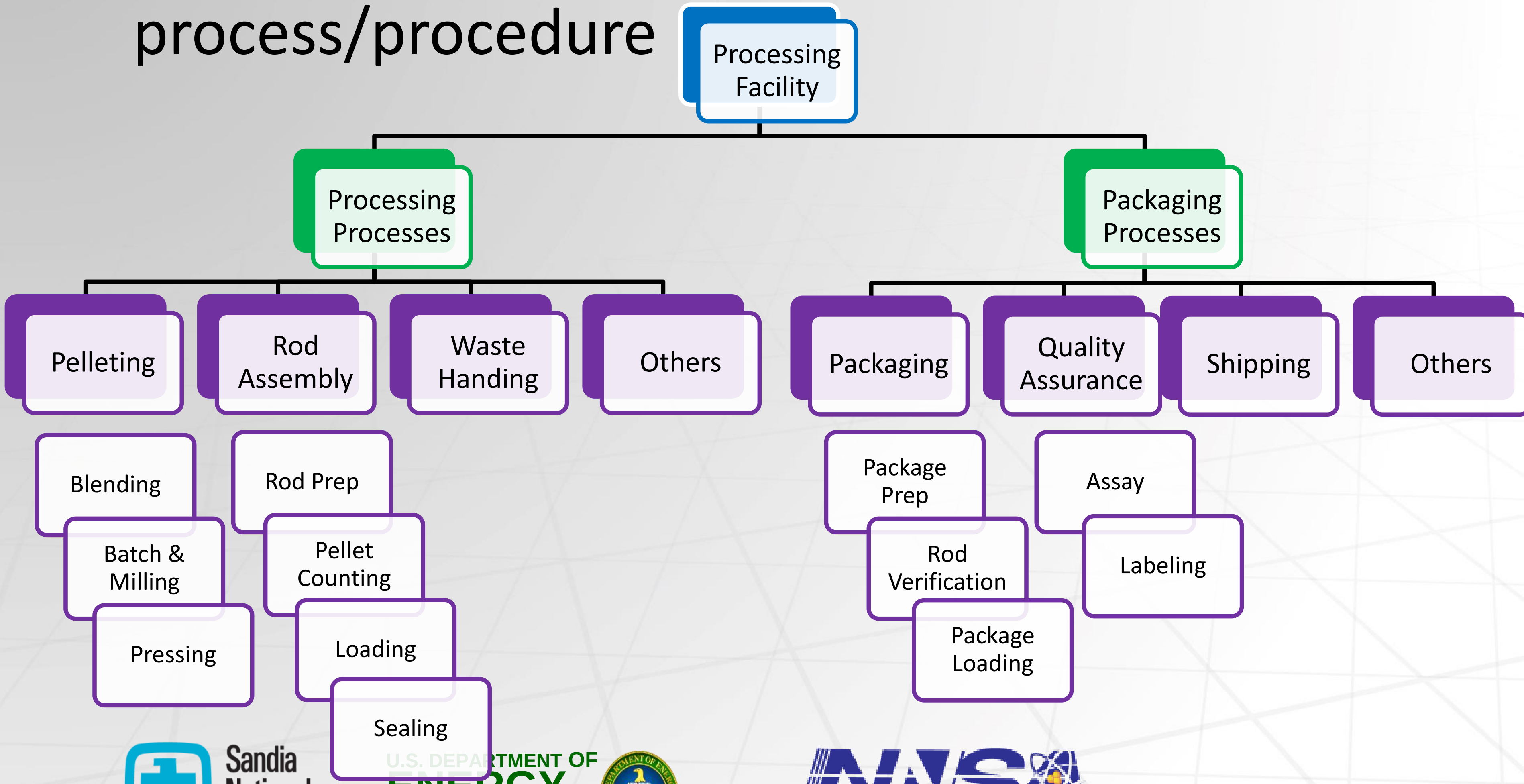
- PFMEA process
  - Failure Modes Effects Analysis - FMEA
  - FMEA is a design tool used to systematically analyze postulated component failures and identify the resultant effects on system operations.
  - PFMEA (Process) is analysis of manufacturing and assembly processes
  - Requires team that have detailed knowledge of operational and cross-cutting procedures
  -

Cross-Cutting Procedures

- Importance of identifying Cross-cutting Procedures
  - Cross-cutting procedures are the same or similar processes that apply to multiple operations.
  - Specific to security these would encompass procedures that implement preventive and protective measures. For example, access control measures include :
    - Two-person rule
    - Segregation
    - Compartmentalization
  - Cross-cutting procedures should be consistently applied

Step 1

- Organize the facility operations by process/procedure



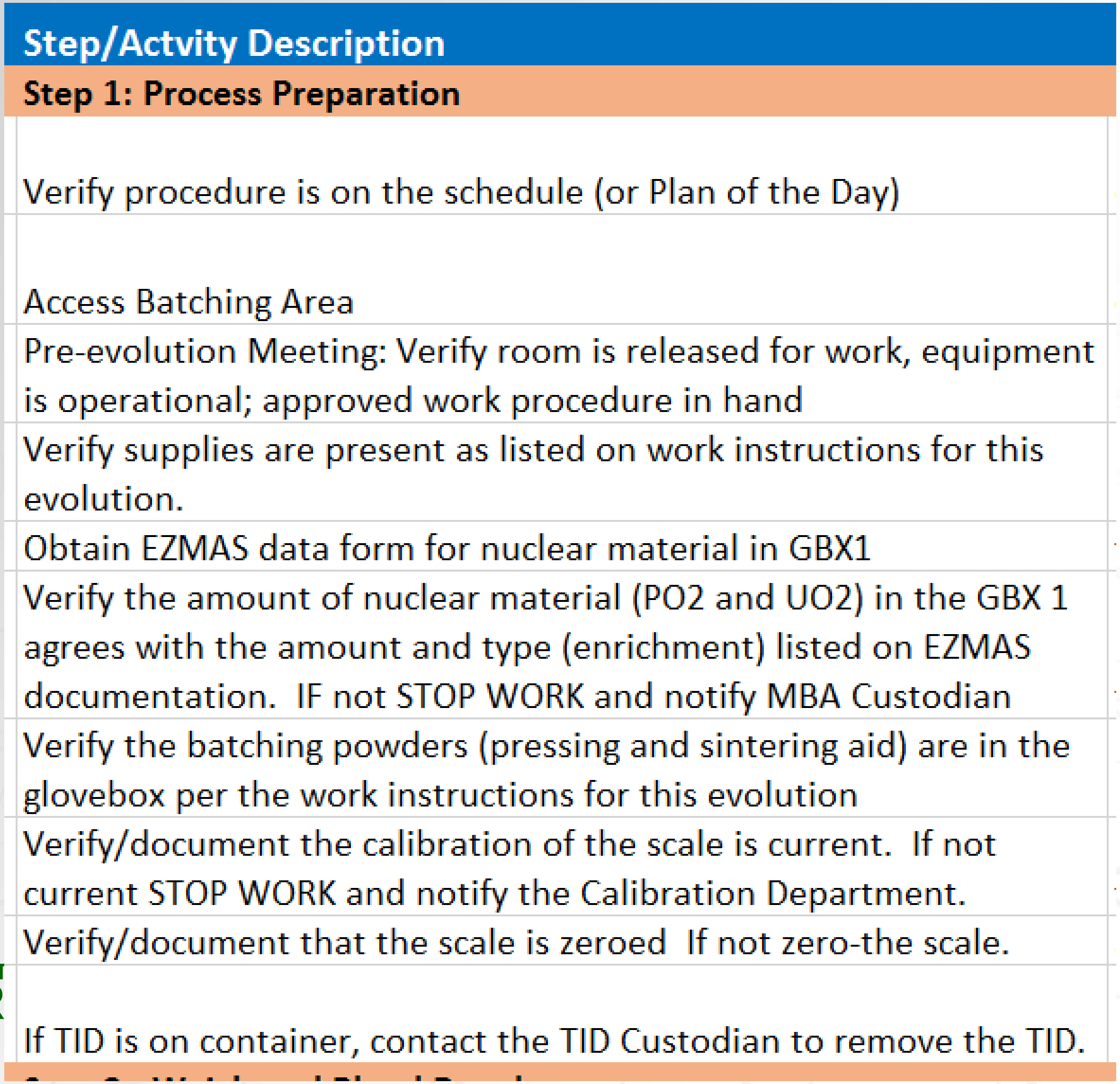
- Processing Facility
  - Processing Processes
    - Pelleting
      - Blending
      - Batch & Milling
      - Pressing
    - Rod Assembly
      - Rod Prep
      - Pellet Counting
      - Loading
      - Sealing
    - Waste Handing
    - Others
  - Packaging Processes
    - Packaging
      - Package Prep
      - Rod Verification
      - Package Loading
    - Quality Assurance
      - Assay
      - Labeling
    - Shipping
    - Others

Step 2

- Document each process/procedure step-by-step
- Characterize the step: review and identify
  - Who performs the step
  - Where the step is performed
  - Equipment needed for the step
  - Containment
- This step is iterative for all facility processes and procedures

Procedure Steps

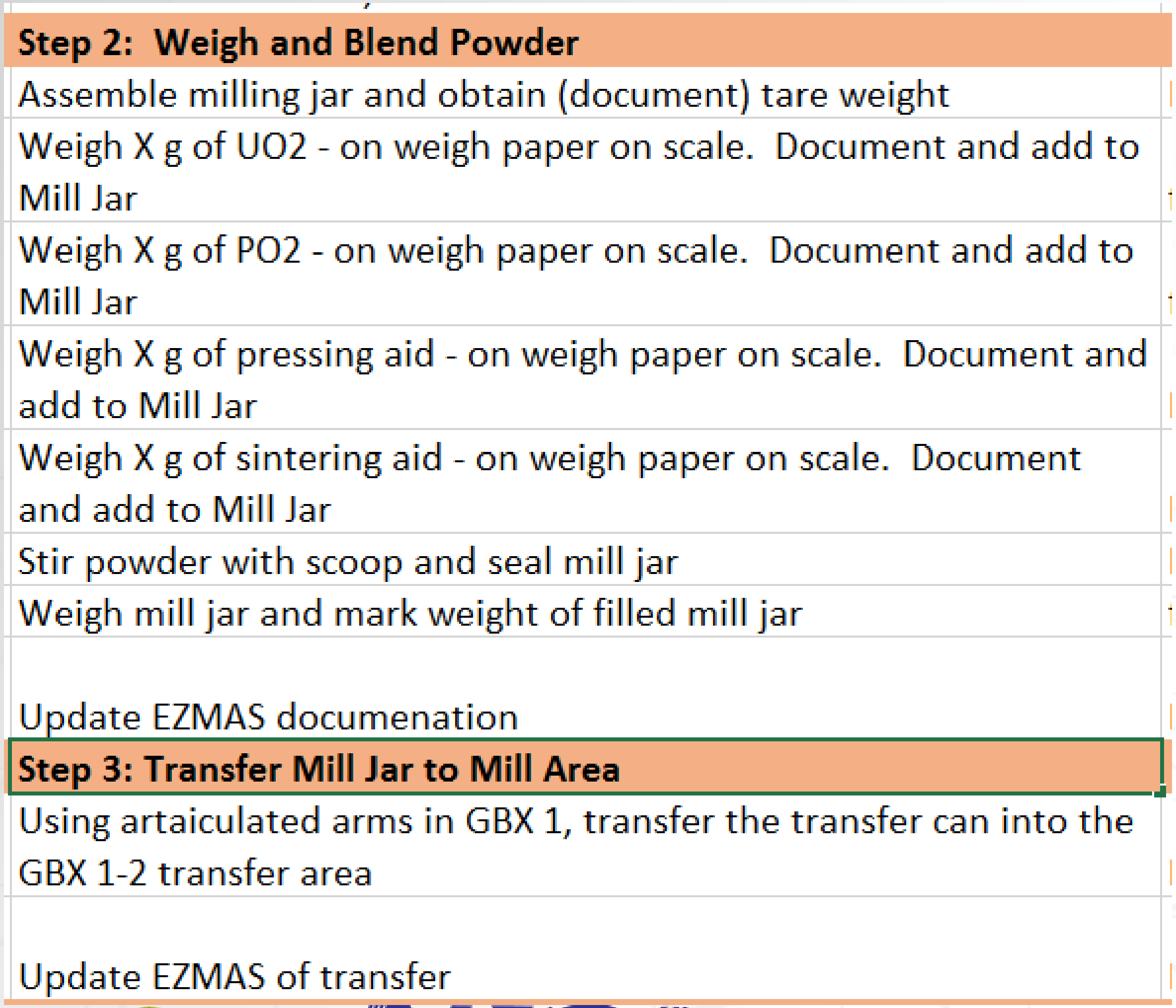
- Process Prep:



Step/Actvity Description
Step 1: Process Preparation
Verify procedure is on the schedule (or Plan of the Day)
Access Batching Area
Pre-evolution Meeting: Verify room is released for work, equipment is operational; approved work procedure in hand
Verify supplies are present as listed on work instructions for this evolution.
Obtain EZMAS data form for nuclear material in GBX1
Verify the amount of nuclear material (PO2 and UO2) in the GBX 1 agrees with the amount and type (enrichment) listed on EZMAS documentation. IF not STOP WORK and notify MBA Custodian
Verify the batching powders (pressing and sintering aid) are in the glovebox per the work instructions for this evolution
Verify/document the calibration of the scale is current. If not current STOP WORK and notify the Calibration Department.
Verify/document that the scale is zeroed If not zero-the scale.
If TID is on container, contact the TID Custodian to remove the TID.

Procedure Steps, cont.

- Weighing and Blending
- Transferring



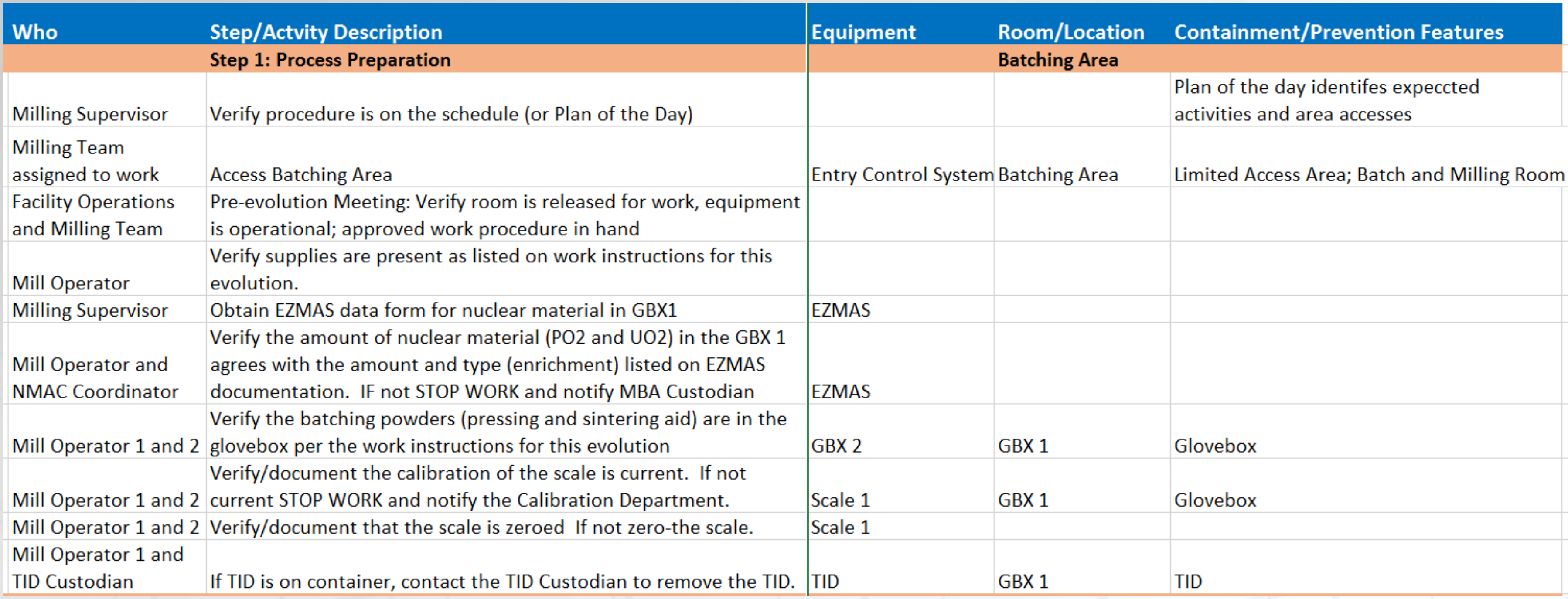
Step 2: Weigh and Blend Powder
Assemble milling jar and obtain (document) tare weight
Weigh X g of UO2 - on weigh paper on scale. Document and add to Mill Jar
Weigh X g of PO2 - on weigh paper on scale. Document and add to Mill Jar
Weigh X g of pressing aid - on weigh paper on scale. Document and add to Mill Jar
Weigh X g of sintering aid - on weigh paper on scale. Document and add to Mill Jar
Stir powder with scoop and seal mill jar
Weigh mill jar and mark weight of filled mill jar
Update EZMAS documenation
Step 3: Transfer Mill Jar to Mill Area
Using artaiculated arms in GBX 1, transfer the transfer can into the GBX 1-2 transfer area
Update EZMAS of transfer

Step 2

- Document each process/procedure step-by-step
- Characterize the step: review and identify
  - Who performs the step
  - Where the step is performed
  - Equipment needed for the step
  - Containment
- This step is iterative for all facility processes and procedures

Characterize

- Process Preparation:



Who	Step/Actvity Description	Equipment	Room/Location	Containment/Prevention Features
	Step 1: Process Preparation		Batching Area	
Milling Supervisor	Verify procedure is on the schedule (or Plan of the Day)			Plan of the day identifes expeccted activities and area accesses
Milling Team assigned to work	Access Batching Area	Entry Control System	Batching Area	Limited Access Area; Batch and Milling Room
Facility Operations and Milling Team	Pre-evolution Meeting: Verify room is released for work, equipment is operational; approved work procedure in hand			
Mill Operator	Verify supplies are present as listed on work instructions for this evolution.			
Milling Supervisor	Obtain EZMAS data form for nuclear material in GBX1	EZMAS		
Mill Operator and NMAC Coordinator	Verify the amount of nuclear material (PO2 and UO2) in the GBX 1 agrees with the amount and type (enrichment) listed on EZMAS documentation. IF not STOP WORK and notify MBA Custodian	EZMAS		
Mill Operator 1 and 2	Verify the batching powders (pressing and sintering aid) are in the glovebox per the work instructions for this evolution	GBX 2	GBX 1	Glovebox
Mill Operator 1 and 2	Verify/document the calibration of the scale is current. If not current STOP WORK and notify the Calibration Department.	Scale 1	GBX 1	Glovebox
Mill Operator 1 and 2	Verify/document that the scale is zeroed If not zero-the scale.	Scale 1		
Mill Operator 1 and TID Custodian	If TID is on container, contact the TID Custodian to remove the TID.	TID	GBX 1	TID

Step 2

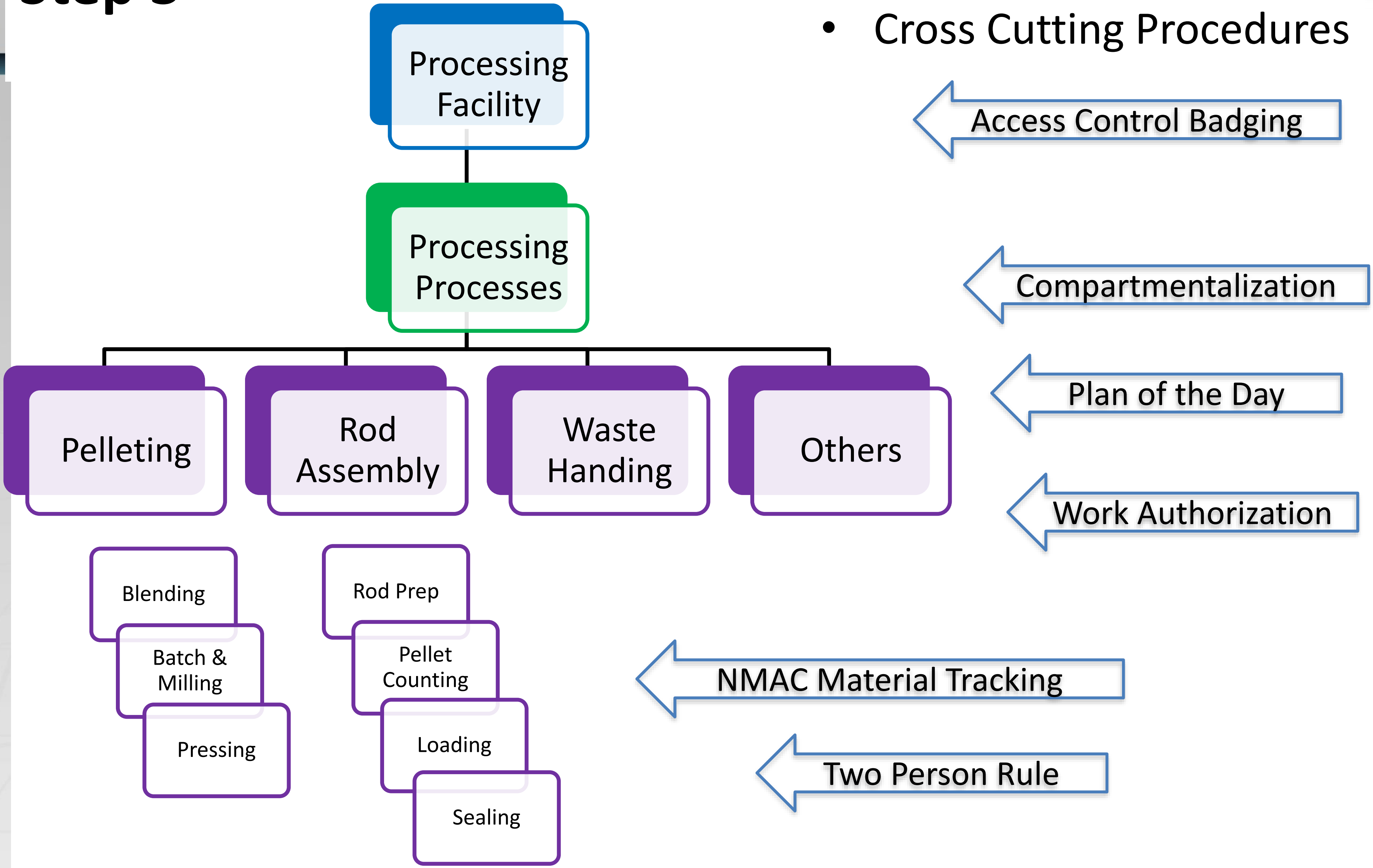
- Document each process/procedure step-by-step
- Characterize the step: review and identify
  - Who performs the step
  - Where the step is performed
  - Equipment needed for the step
  - Containment
- This step is iterative for all facility processes and procedures

Step 3

- Identify all cross-cutting processes and procedures
  - For the process as a whole
  - For each step in the procedure
  - For example:
    - Implementation of security measures
      - Preventive and protective measures against the insider
    - Implementation of safety measures
    - Interface with external entities
    - Work authorization
    - Access control / Badging
- Don’t forget to review steps in the cross-cutting procedures also
  - The cross cutting procedures are facility procedures, too

Step 3

- Cross Cutting Procedures



Processing Facility

Processing Processes

Pelleting

Rod Assembly

Waste Handing

Others

Blending

Batch & Milling

Pressing

Rod Prep

Pellet Counting

Loading

Sealing

Access Control Badging

Compartmentalization

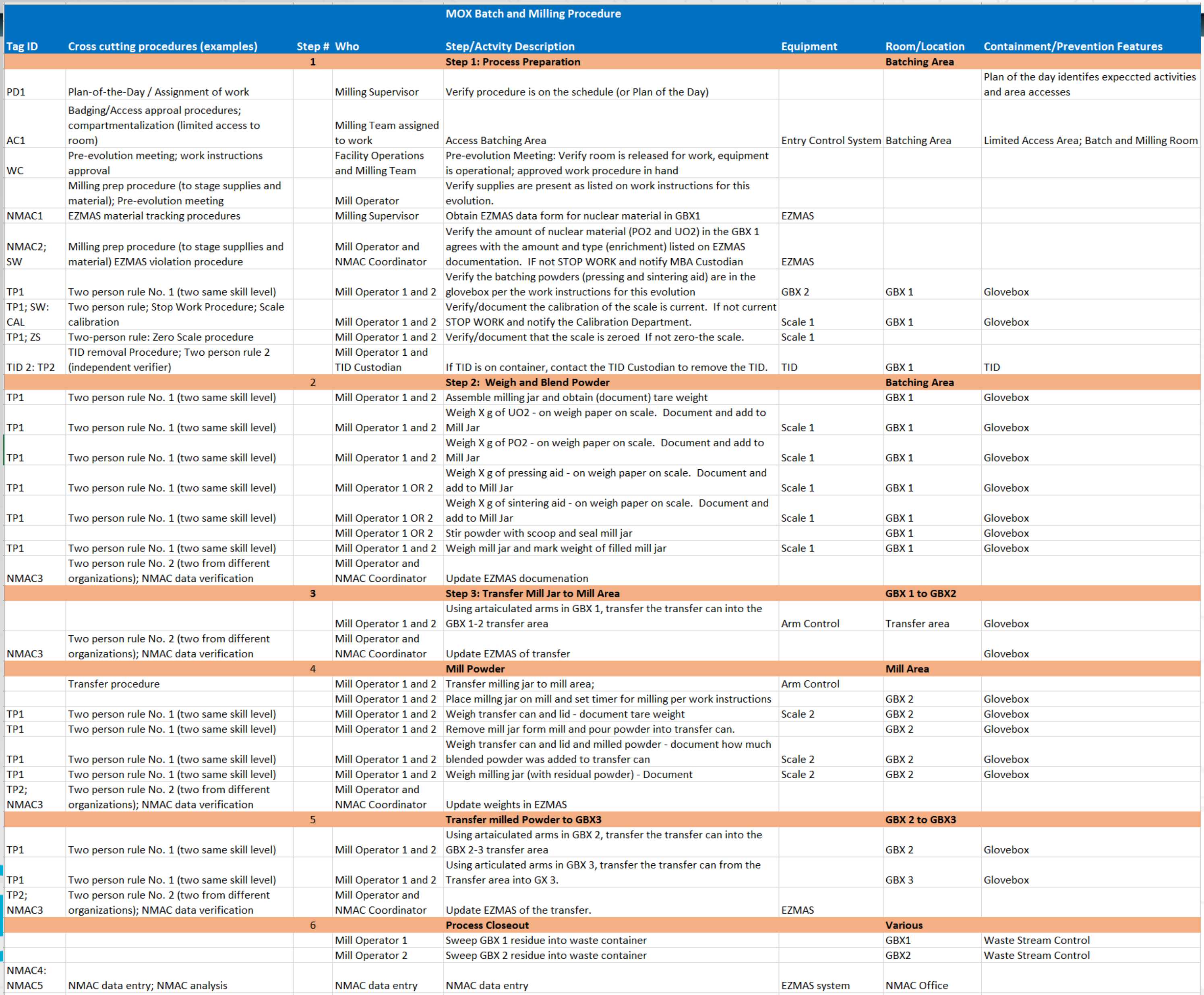
Plan of the Day

Work Authorization

NMAC Material Tracking

Two Person Rule

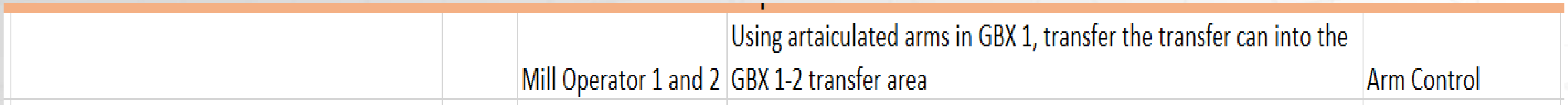
Database for One Procedure



				MOX Batch and Milling Procedure			
Tag ID	Cross cutting procedures (examples)	Step #	Who	Step/Actvity Description	Equipment	Room/Location	Containment/Prevention Features
		1		**Step 1: Process Preparation**		**Batching Area**	
PD1	Plan-of-the-Day / Assignment of work		Milling Supervisor	Verify procedure is on the schedule (or Plan of the Day)			Plan of the day identifes expeccted activities and area accesses
AC1	Badging/Access approal procedures; compartmentalization (limited access to room)		Milling Team assigned to work	Access Batching Area	Entry Control System	Batching Area	Limited Access Area; Batch and Milling Room
WC	Pre-evolution meeting; work instructions approval		Facility Operations and Milling Team	Pre-evolution Meeting: Verify room is released for work, equipment is operational; approved work procedure in hand			
	Milling prep procedure (to stage supplies and material); Pre-evolution meeting		Mill Operator	Verify supplies are present as listed on work instructions for this evolution.			
NMAC1	EZMAS material tracking procedures		Milling Supervisor	Obtain EZMAS data form for nuclear material in GBX1	EZMAS		
NMAC2; SW	Milling prep procedure (to stage suppllies and material) EZMAS violation procedure		Mill Operator and NMAC Coordinator	Verify the amount of nuclear material (PO2 and UO2) in the GBX 1 agrees with the amount and type (enrichment) listed on EZMAS documentation. If not STOP WORK and notify MBA Custodian	EZMAS		
TP1	Two person rule No. 1 (two same skill level)		Mill Operator 1 and 2	Verify the batching powders (pressing and sintering aid) are in the glovebox per the work instructions for this evolution	GBX 2	GBX 1	Glovebox
TP1; SW: CAL	Two person rule; Stop Work Procedure; Scale calibration		Mill Operator 1 and 2	Verify/document the calibration of the scale is current. If not current STOP WORK and notify the Calibration Department.	Scale 1	GBX 1	Glovebox
TP1; ZS	Two-person rule: Zero Scale procedure		Mill Operator 1 and 2	Verify/document that the scale is zeroed If not zero-the scale.	Scale 1		
TID 2: TP2	TID removal Procedure; Two person rule 2 (independent verifier)		Mill Operator 1 and TID Custodian	If TID is on container, contact the TID Custodian to remove the TID.	TID	GBX 1	TID
		2		**Step 2: Weigh and Blend Powder**		**Batching Area**	
TP1	Two person rule No. 1 (two same skill level)		Mill Operator 1 and 2	Assemble milling jar and obtain (document) tare weight		GBX 1	Glovebox
TP1	Two person rule No. 1 (two same skill level)		Mill Operator 1 and 2	Weigh X g of UO2 - on weigh paper on scale. Document and add to Mill Jar	Scale 1	GBX 1	Glovebox
TP1	Two person rule No. 1 (two same skill level)		Mill Operator 1 and 2	Weigh X g of PO2 - on weigh paper on scale. Document and add to Mill Jar	Scale 1	GBX 1	Glovebox
TP1	Two person rule No. 1 (two same skill level)		Mill Operator 1 OR 2	Weigh X g of pressing aid - on weigh paper on scale. Document and add to Mill Jar	Scale 1	GBX 1	Glovebox
TP1	Two person rule No. 1 (two same skill level)		Mill Operator 1 OR 2	Weigh X g of sintering aid - on weigh paper on scale. Document and add to Mill Jar	Scale 1	GBX 1	Glovebox
			Mill Operator 1 OR 2	Stir powder with scoop and seal mill jar		GBX 1	Glovebox
TP1	Two person rule No. 1 (two same skill level)		Mill Operator 1 and 2	Weigh mill jar and mark weight of filled mill jar	Scale 1	GBX 1	Glovebox
NMAC3	Two person rule No. 2 (two from different organizations); NMAC data verification		Mill Operator and NMAC Coordinator	Update EZMAS documenation			
		3		**Step 3: Transfer Mill Jar to Mill Area**		**GBX 1 to GBX2**	
			Mill Operator 1 and 2	Using artaiculated arms in GBX 1, transfer the transfer can into the GBX 1-2 transfer area	Arm Control	Transfer area	Glovebox
NMAC3	Two person rule No. 2 (two from different organizations); NMAC data verification		Mill Operator and NMAC Coordinator	Update EZMAS of transfer			Glovebox
		4		**Mill Powder**		**Mill Area**	
	Transfer procedure		Mill Operator 1 and 2	Transfer milling jar to mill area;	Arm Control		
			Mill Operator 1 and 2	Place millng jar on mill and set timer for milling per work instructions		GBX 2	Glovebox
TP1	Two person rule No. 1 (two same skill level)		Mill Operator 1 and 2	Weigh transfer can and lid - document tare weight	Scale 2	GBX 2	Glovebox
TP1	Two person rule No. 1 (two same skill level)		Mill Operator 1 and 2	Remove mill jar form mill and pour powder into transfer can.		GBX 2	Glovebox
TP1	Two person rule No. 1 (two same skill level)		Mill Operator 1 and 2	Weigh transfer can and lid and milled powder - document how much blended powder was added to transfer can	Scale 2	GBX 2	Glovebox
TP1	Two person rule No. 1 (two same skill level)		Mill Operator 1 and 2	Weigh milling jar (with residual powder) - Document	Scale 2	GBX 2	Glovebox
TP2; NMAC3	Two person rule No. 2 (two from different organizations); NMAC data verification		Mill Operator and NMAC Coordinator	Update weights in EZMAS			
		5		**Transfer milled Powder to GBX3**		**GBX 2 to GBX3**	
TP1	Two person rule No. 1 (two same skill level)		Mill Operator 1 and 2	Using artaiculated arms in GBX 2, transfer the transfer can into the GBX 2-3 transfer area		GBX 2	Glovebox
TP1	Two person rule No. 1 (two same skill level)		Mill Operator 1 and 2	Using articulated arms in GBX 3, transfer the transfer can from the Transfer area into GX 3.		GBX 3	Glovebox
TP2; NMAC3	Two person rule No. 2 (two from different organizations); NMAC data verification		Mill Operator and NMAC Coordinator	Update EZMAS of the transfer.	EZMAS		
		6		**Process Closeout**		**Various**	
			Mill Operator 1	Sweep GBX 1 residue into waste container		GBX1	Waste Stream Control
			Mill Operator 2	Sweep GBX 2 residue into waste container		GBX2	Waste Stream Control
NMAC4: NMAC5	NMAC data entry; NMAC analysis		NMAC data entry	NMAC data entry	EZMAS system	NMAC Office	

Step 3 Result

- Database of protective measures identified – or not
- May identify gaps
  - Empty fields may identify missing procedures
  - Procedures that are inconsistently or ineffectively applied across operational processes

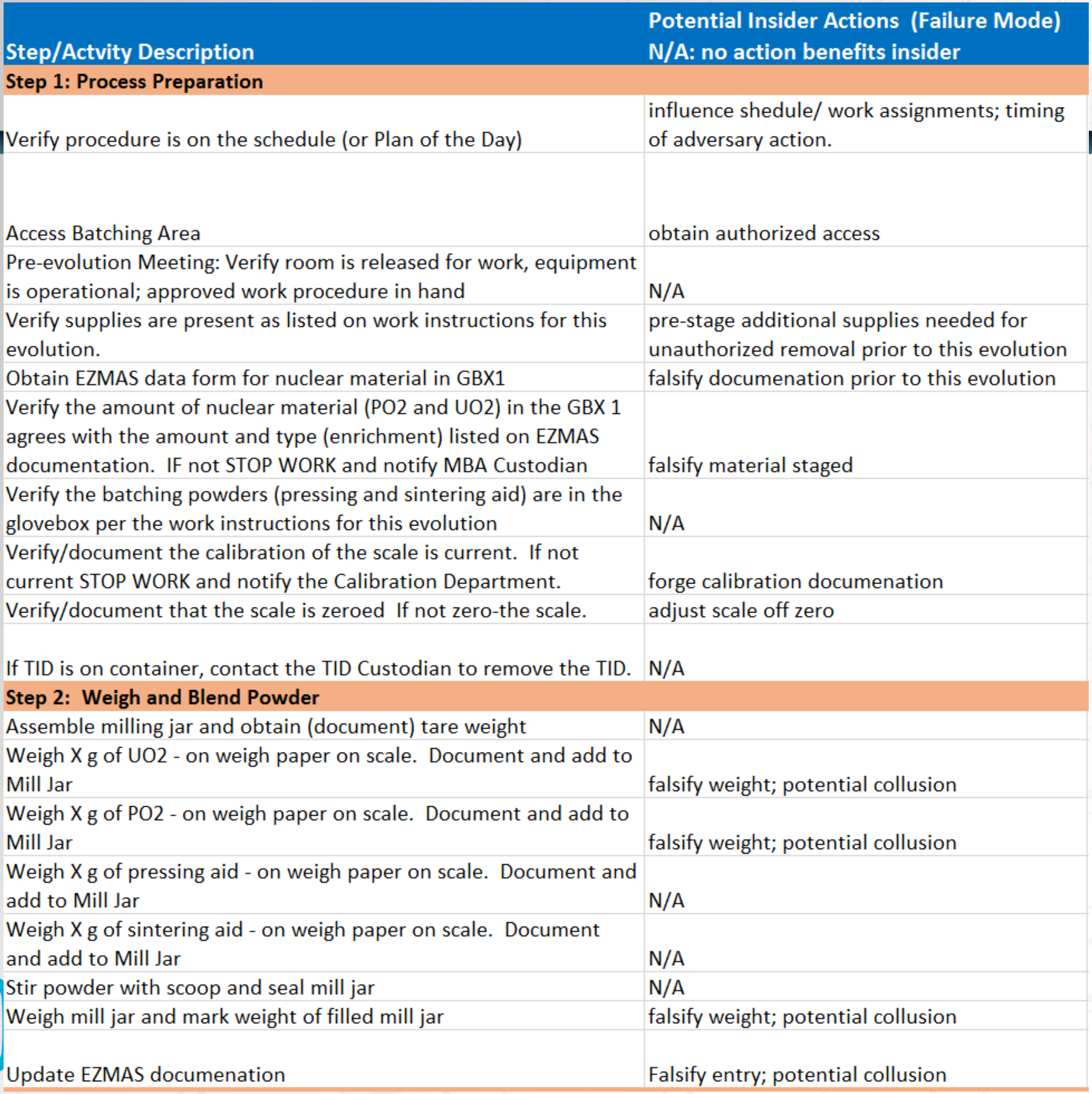


		Mill Operator 1 and 2	Using artaiculated arms in GBX 1, transfer the transfer can into the GBX 1-2 transfer area	Arm Control

Step 4

- Identify the insider actions or steps that could be taken at each step in the procedure
  - Include actions for insider collusion

Note: this data is intentionally adversary and scenario independent



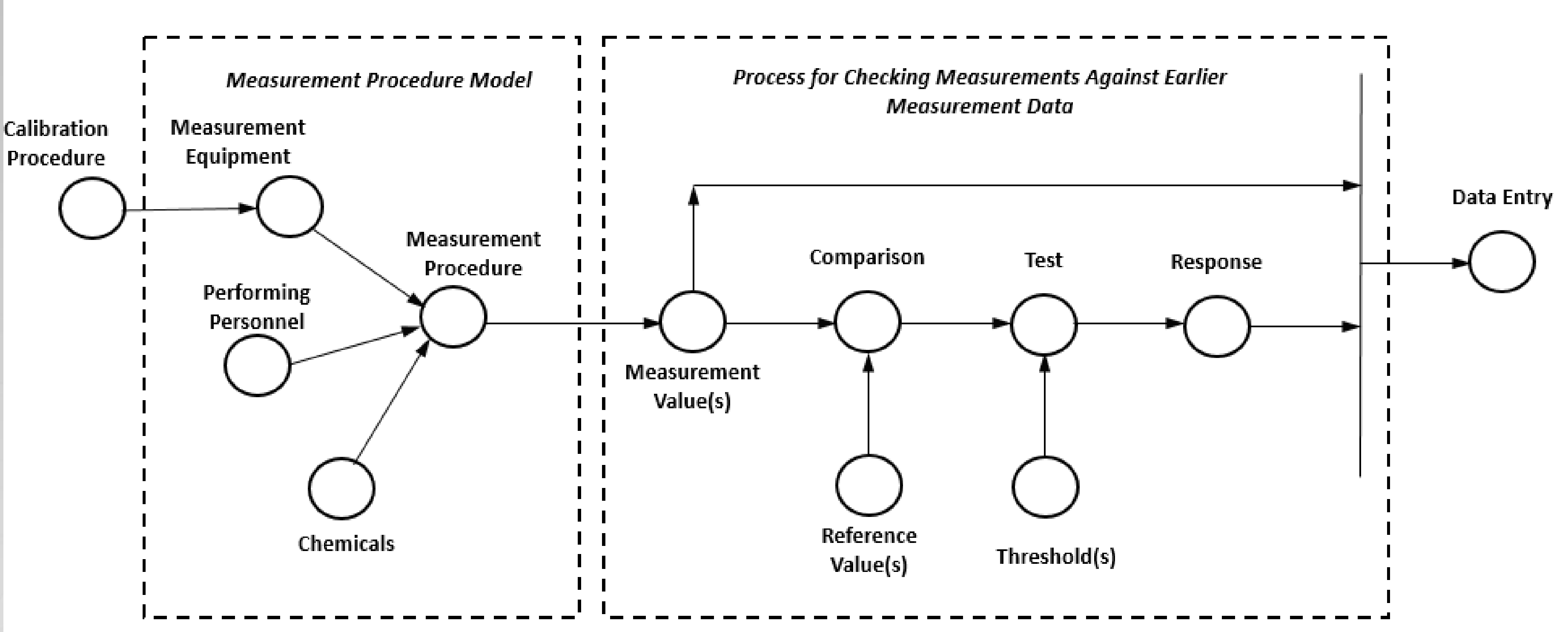
Step/Actvity Description	Potential Insider Actions (Failure Mode) N/A: no action benefits insider
Step 1: Process Preparation	
Verify procedure is on the schedule (or Plan of the Day)	influence shedule/ work assignments; timing of adversary action.
Access Batching Area	obtain authorized access
Pre-evolution Meeting: Verify room is released for work, equipment is operational; approved work procedure in hand	N/A
Verify supplies are present as listed on work instructions for this evolution.	pre-stage additional supplies needed for unauthorized removal prior to this evolution
Obtain EZMAS data form for nuclear material in GBX1	falsify documenation prior to this evolution
Verify the amount of nuclear material (PO2 and UO2) in the GBX 1 agrees with the amount and type (enrichment) listed on EZMAS documentation. IF not STOP WORK and notify MBA Custodian	falsify material staged
Verify the batching powders (pressing and sintering aid) are in the glovebox per the work instructions for this evolution	N/A
Verify/document the calibration of the scale is current. If not current STOP WORK and notify the Calibration Department.	forge calibration documenation
Verify/document that the scale is zeroed If not zero-the scale.	adjust scale off zero
If TID is on container, contact the TID Custodian to remove the TID.	N/A
Step 2: Weigh and Blend Powder	
Assemble milling jar and obtain (document) tare weight	N/A
Weigh X g of UO2 - on weigh paper on scale. Document and add to Mill Jar	falsify weight; potential collusion
Weigh X g of PO2 - on weigh paper on scale. Document and add to Mill Jar	falsify weight; potential collusion
Weigh X g of pressing aid - on weigh paper on scale. Document and add to Mill Jar	N/A
Weigh X g of sintering aid - on weigh paper on scale. Document and add to Mill Jar	N/A
Stir powder with scoop and seal mill jar	N/A
Weigh mill jar and mark weight of filled mill jar	falsify weight; potential collusion
Update EZMAS documenation	Falsify entry; potential collusion

Step 5

- Analyze the information
- Define scope of analysis for single or multiple "facets of interest."

  For example, examine:
  - Individual processes to determine robustness of security
  - Similar groups of processes to determine consistent application of cross-cutting procedures
    - Example, material movement procedures or two person rule
  - Cross-cutting procedures with respect to the Security Plan objectives
- Results of analyses can also provide input for other analysis methods

Examples of Structured Assessment Approach (SAA) Models

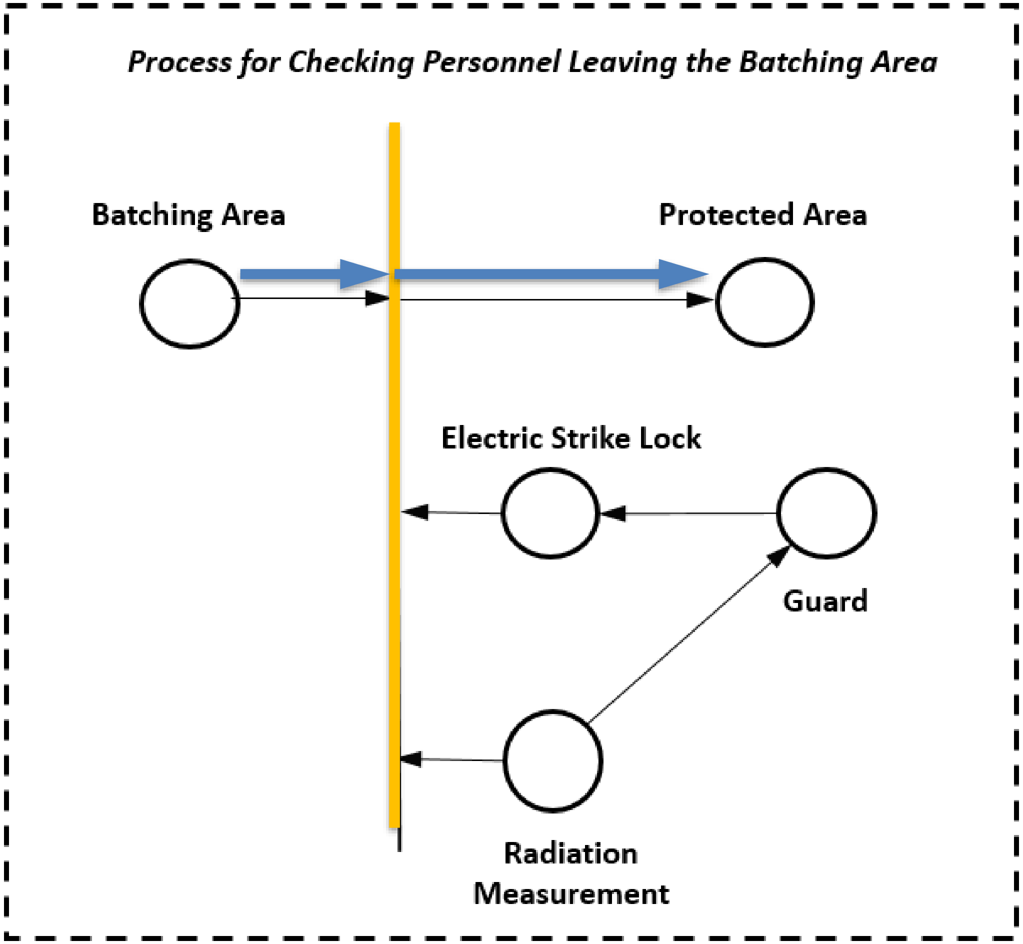


Represents a process for taking a measurement, comparing it against an earlier measurement and, if the two agree, entering it into an accounting system

Examples of Structured Assessment Approach (SAA) Models (Continued)

Represents a process where

1. A person exiting the Batching Area is swept by a guard with a radiation detector
2. The guard then determines whether to open the door by releasing the lock to let him/her exit


Process for Checking Personnel Leaving the Batching Area

Relationship with the IAEA NUSAM* Insider Effectiveness Model

PFMEA and SAA techniques align with an insider effectiveness model developed as part of NUSAM:

$$P_E = 1 – (1\text{-}P_{DS}\{SP\}) \text{ x } (1\text{-}P_{EA}|_{SP}),$$

where:

- *SP* is a set of protracted actions that occur before the abrupt attack and
- $P_{EA}|_{SP}$ is the effectiveness of the PP and NMAC systems during the abrupt attack given that the set of actions, *SP*, have been completed previously.

*****_Nuclear Security Assessment Methodologies Coordinated Research Project_

Summary and Conclusions

- The PFMEA model results in a multidimensional database
  - Generated from facility operational processes and procedures
  - Can help the analyst identify where in a process an insider attacks may be more successful
    - Including identifying opportunities for insider collusion
  - Identify additional protective and preventive measures that may be implemented or more consistently applied.
- The SAA models provides for an analysis of the implementation of multiple protection systems
  - Also identified from the facility operational processes and procedures