MTS SYSTEMS **TRAINING**

MTS PROJECT ENGINEERING – HAZARD & RISK ANALYSIS

Rev 1

16 Dec 2016

be certain.

Table of Contents

Purpose

- Train the Project Engineer on the responsibilities related to the Hazard & Risk Analysis (HRA) with respect to project execution and Quality Records

Scope

Training for Project Engineer's Responsibilities related to:

- Oversight/Completion of the Hazard & Risk Analysis
  - Understanding the inputs to the Hazard & Risk Analysis
  - Oversee Completion of the Hazard & Risk Analysis
  - Understanding the outputs of the Hazard & Risk Analysis
- Storing a copy of the Hazard & Risk Analysis on POND

Note: This training does not cover the completion of the Hazard & Risk Analysis

References (Processes and Templates)

- Pro29 (Product Safety Manual): \\mspdata1\quality\MASTERS\Product Safety Manual
- Engineering/Project Process: http://groups.mts.com/ProjectOps/WorkInstructions/ETO%20and%20Custom%20Process%20flow%20chart%20V5.pdf
- Hazard & Risk Analysis Process: http://groups.mts.com/ProjectSystem/ProcessHome.asp?mnuSys=ENGR&mnuShortName=EPHA
- Hazard & Risk Analysis Template (work instructions included): \\mspdata1\quality\MASTERS\Hazard_Analysis
- Projects ON Demand (POND) (process and documentation): http://groups.mts.com/ProjectSystem/ProcessHome.asp?mnuSys=ENGR&mnuShortName=EPPOND
- Hazard Analysis, Risk Assessment and Application to MTS Machinery Presentation http://groups.mts.com/ComplianceEng/PRESENTATIONS_DOCUMENTS/HAZARDS%20ANALYSIS%20AND%20RISK%20ASSESSMENTS%20july%2024%202012.pptx

Definitions

- Hazard & Risk Analysis (HRA) – an analysis that assesses the risks associated with hazards originating from MTS equipment and system designs

  Focuses on Health, Safety, and Property Risk

- Failure Mode Effects Analysis (FMEA) – an analysis that assesses the risk associated with failure of system components and subsystems as they pertain to performance and reliability

  Focuses on System Reliability and Performance Risk

- Risk Analysis - an analysis that identifies and assess factors that may jeopardize the success of a project

  Focuses on Factors that may Influence Project Success with respect to Cost, Schedule, and Fulfilling Contract Requirements

Definitions (Continued)

MTS SYSTEMS TRAINING

- Mitigation – a design feature, safety mechanism, or action that reduces the severity or likelihood of a hazard
- Verification – act of reviewing to ensure planned mitigation is present (e.g. sharp edges are rounded on drawing)
- Validation – act of performing a functional test to ensure a safety mechanism provides the expected mitigation
- Lockout/Tag-Out – safety procedure requiring hazardous energy sources be isolated and rendered inoperative prior to servicing machinery

When is the Hazard & Risk Analysis Completed?

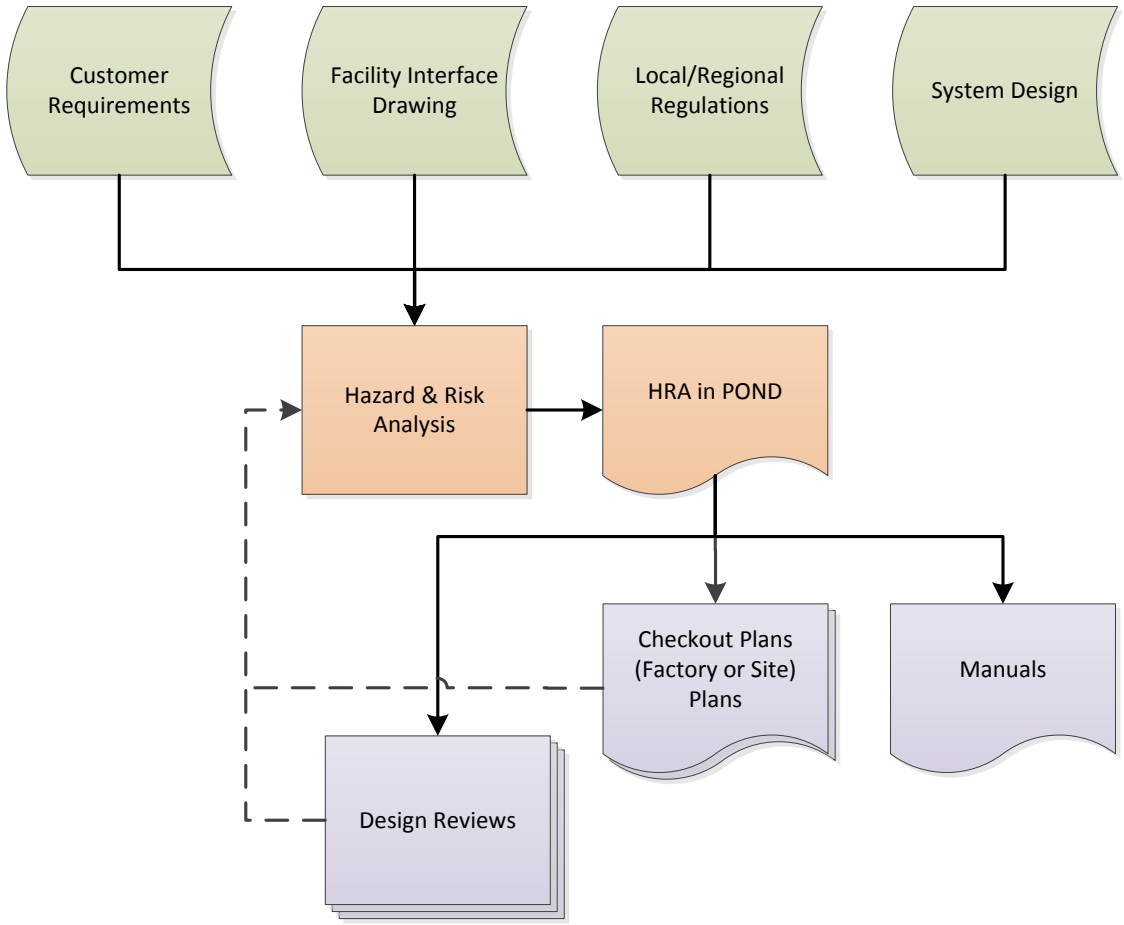
The Hazard & Risk Analysis is a living document throughout the lifecycle of a project. The majority of activity occurs during:

1. Presale Design Phase (as required to understand system requirements)
2. Project Development/Design Phase

Hazard & Risk Analysis shall be updated:

- When risk mitigations are verified or validated (i.e. following Design Reviews, Manual Reviews, Checkout, and Installation as applicable)
- If any mitigation elements are not verifiable or validatable
- If changes to the system design or its external interfaces occurs after the Design Reviews, Checkout, or Site Acceptance have been completed
- As corrective actions require

Inputs & Outputs of the Hazard & Risk Analysis



INPUTS

HAZARD & RISK ANALYSIS

OUTPUTS

Brief Intro to the MTS Hazard & Risk Analysis

Manual/Training Mitigations

Safe Guarding/Mechanism Mitigations

Design Mitigations

Verification/Validation (i.e. what was done to verify or validate the mitigations were implemented and/or effective)

Risk with Mitigations Implemented

Hazard Analysis Title:	(ENTER A TITLE NAME; e.g. product name, project title) *(not a customer name)*
Most Recent Revision Date:	(ENTER MOST RECENT REVIEW DATE; per the Attendance Record)
Intended Use	(ENTER INTENDED USE)

Assume initial risk without any HW/SW safety measures applied.

							RISK REDUCTION If the Initial Risk Level = Medium / High / Critical, then must do 1			*Verification & Validation*		
HAZARD TYPE / GROUP	PART OF MACHINE	HAZARD ORIGIN	SYSTEM STATE / MODE	POTENTIAL CONSEQUENCE(S)	CAUSE(S) *(TRIGGERS CONSEQUENCE)*	INITIAL RISK LEVEL	1 DESIGN OUT THE HAZARD *(INHERENTLY SAFE)*	2 HW/SW CONTROL MEANS *(SAFEGUARDING / COMPLEMENTARY)*	3 PAPER & DOCUMENTATION *(TRAINING / INSTRUCTIONS)*	VERIFICATION: IDENTIFY WHAT WAS DONE TO REDUCE INITIAL RISK (or customer action)	VALIDATION: IDENTIFY SAFETY FUNCTIONAL TEST DONE TO CONFIRM REDUCTION OF INITIAL RISK	FINAL RISK LEVEL
Mechanical Hazards	Accumulator	High pressure	Maintenance	Impact, injection	Failure to depressurized before servicing	2B	N/A	Drain valve and pressure gauge added.	Procedure for safe draining added to the user manual. Add warning label to accumulator.	Edge was rounded in drawings; labels verified.	N/A	2E
	Accumulator	High pressure	Operation	Impact, injection	Ruptured accumulator, pressure exceeds capacity	2B	Supplier designed accumulator with sufficient safety factor above max system pressure; critical to safety feature on print	Add relief valve	Add procedure to manual to periodically test relief valve	Critical to safety feature from supplier (check certificate), manual procedure updated.	Factory testing on relief valve	2E
	Load frame	Falling object	Packaging / Handling	Crushing	Heavy object; unwieldly	1C	N/A	Lifting eyes on cross-head; critical to safety feature	Safe lifting procedure in manual. Add warning label for lifting.	Critical to safety feature (check certificate); labels verified.	N/A	1E
Electrical Hazards	Drive cabinet	Live parts	Maintenance	Shock, burn	Exposed live parts	1C	N/A	Disconnect switch added on cabinet door. Barrier on live part.	Add warning label for shock, add procedure for use in manual.	Labels verified, manual updated.	Power interupt during factory test.	1E

Hazard Identification

Initial Risk Assessment

Mitigations

Verifications/Validations

Project Engineering Responsibilities

1. Ensures Hazard & Risk Analysis is completed
2. Ensures Hazard & Risk Analysis is stored in POND
3. Ensures Hazards “mitigated by design” are reviewed during the design reviews
4. Ensures Manuals are reviewed/updated for ETO/Custom projects
5. Communicates Assembly/System Hazards to assembly/checkout team prior to respective activities
6. Ensures safety measures are verified/validated during checkout or site acceptance (i.e. clearly outlined in checkout plan, clearly outlined in site acceptance plan, etc.)
7. Ensures installation program provides for safe installation of the system in the customer facility, including customer training per the manual [1]

1 Field Service Engineer can also perform this per FS-AD-3113

Ensuring the Hazard & Risk Analysis Completion

MTS SYSTEMS TRAINING

- The Systems Engineer owns the Hazard & Risk Analysis and is responsible for completion
- The Project Engineer makes sure it gets done
- Ensure the latest Hazard & Risk Analysis Template is used: \\mspdata1\quality\MASTERS\Hazard_Analysis
- Ensure that any “nonstandard” or “ETO” features are consider

Note: “Systems Engineer” is a role and the responsibility of Hazard Analysis ownership may fall on other members of the project team (i.e. the PE might assume the role of System Engineer on some projects, the Lead Mechanical/Electrical Engineer might assume the role of Systems Engineer on some projects)

Ensuring the Hazard & Risk Analysis is Completion: Leveraging Existing Hazard & Risk Analyses

MTS SYSTEMS TRAINING

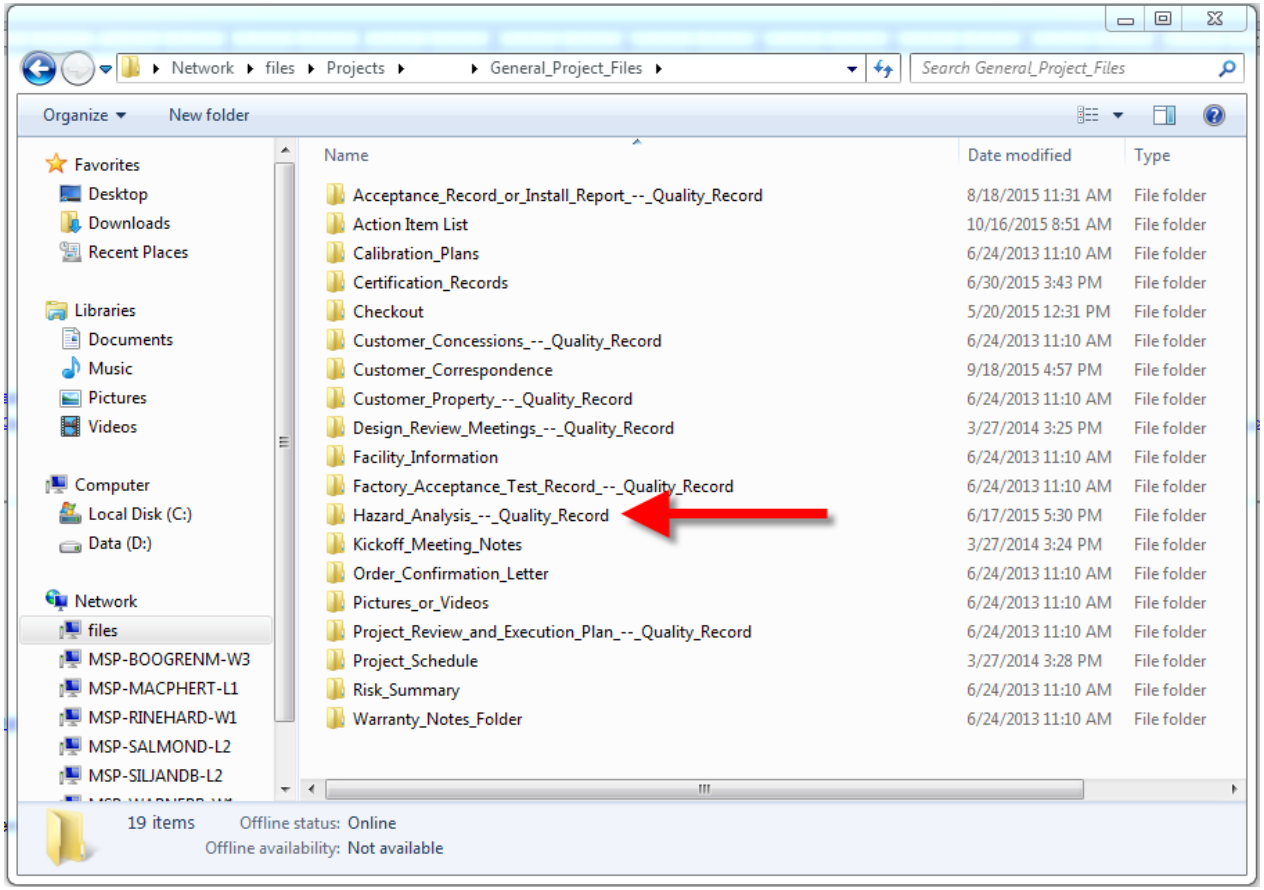
"Standard" and "ETO" projects can, and should, leverage previous Hazard & Risk Analysis :

- Hazard & Risk Analyses should exist for products/systems that have previously been delivered
- Previous Hazard & Risk Analyses will need to be reviewed against the current project to identify if there any differences with respect Hazards (i.e. does the new system really have the same hazards as the old system)
  - Special consideration should be taken when:
    - The customer has unique safety requirements
    - Nonstandard, ETO, or Special features will be delivered

Note: If utilizing an existing or legacy HRA, it is important to note that it may not be consistent with current HRA template and information may need to be transferred to the new format.

Store Hazard & Risk Analysis on POND

» Hazard & Risk Analysis shall be stored in POND



Note: It is not acceptable to hyperlink to a Hazard Analysis. If an existing Hazard Analysis is to be used as is, a copy must be stored in POND to maintain revision fidelity.

Ensure “Design Mitigations” are Reviewed

- The Systems Engineer Role shall facilitate design reviews ensuring that mitigations that “Design Out the Hazard” are reviewed for adequacy
- Following a Design Review, the Hazard & Risk Analysis Verification column shall be populated for any verified mitigation

Design Mitigations

Verification

Hazard Analysis Title:	(ENTER A TITLE NAME; e.g. product name, project title) *(not a customer name)*
Most Recent Revision Date:	(ENTER MOST RECENT REVIEW DATE; per the Attendance Record)
Intended Use	(ENTER INTENDED USE)

Assum initial risk without ny HW/SW safety m sures applied.

							RISK REDUCTION *If the Initial Risk Level is Medium / High / Critical, then must do 1-3.*			Verification & Validation		
HAZARD TYPE / GROUP	PART OF MACHINE	HAZARD ORIGIN	SYSTEM STATE / MODE	POTENTIAL CONSEQUENCE(S)	CAUSE(S) *(TRIGGERS CONSEQUENCE)*	INITIAL RISK LEVEL	1 DESIGN OUT THE HAZARD *(INHERENTLY SAFE)*	2 HW/SW CONTROL MEANS *(SAFEGUARDING / COMPLEMENTARY)*	3 PAPER & DOCUMENTATION *(TRAINING / INSTRUCTIONS)*	VERIFICATION: IDENTIFY WHAT WAS DONE TO REDUCE INITIAL RISK (or customer action)	VALIDATION: IDENTIFY SAFETY FUNCTIONAL TEST DONE TO CONFIRM REDUCTION OF INITIAL RISK	FINAL RISK LEVEL
Mechanical Hazards	Accumulator	High pressure	Maintenance	Impact, injection	Failure to depressurized before servicing	2B	N/A	Drain valve and pressure gauge added.	Procedure for safe draining added to the user manual. Add warning label to accumulator.	Edge was rounded in drawings; labels verified.	N/A	2E
	Accumulator	High pressure	Operation	Impact, injection	Ruptured accumulator, pressure exceeds capacity	2B	Supplier designed accumulator with sufficient safety factor above max system pressure; critical to safety feature on print	Add relief valve	Add procedure to manual to periodically test relief valve	Critical to safety feature from supplier (check certificate), manual procedure updated.	Factory testing on relief valve	2E
	Load frame	Falling object	Packaging / Handling	Crushing	Heavy object; unwieldy	1C	N/A	Lifting eyes on cross-head; critical to safety feature	Safe lifting procedure in manual. Add warning label for lifting.	Critical to safety feature (check certificate); labels verified.	N/A	1E

Ensure Manual Review

- The Systems Engineer Role shall review the Product Manuals:
  - Ensuring hazards are properly stated with reference to the Hazard & Risk Analysis
- The “Paper & Documentation” column shall be reviewed against the manuals during a manual review
- Following a Manual Review, the Hazard & Risk Analysis Verification column shall be populated for any verified mitigation

Paper & Documentation **Verification**

Hazard Analysis Title:	(ENTER A TITLE NAME; e.g. product name, project title) *(not a customer name)*
Most Recent Revision Date:	(ENTER MOST RECENT REVIEW DATE; per the Attendance Record)
Intended Use	(ENTER INTENDED USE)

Assume initial risk without any HW/SW safety measures applied.

							RISK REDUCTION *If the Initial Risk Level is Medium / High / Critical, then must do 1-3.*			*Verification & Validation*		
HAZARD TYPE / GROUP	PART OF MACHINE	HAZARD ORIGIN	SYSTEM STATE / MODE	POTENTIAL CONSEQUENCE(S)	CAUSE(S) *(TRIGGERS CONSEQUENCE)*	INITIAL RISK LEVEL	1 DESIGN OUT THE HAZARD *(INHERENTLY SAFE)*	2 HW/SW CONTROL MEANS *(SAFEGUARDING / COMPLEMENTARY)*	3 PAPER & DOCUMENTATION *(TRAINING / INSTRUCTIONS)*	VERIFICATION: IDENTIFY WHAT WAS DONE TO REDUCE INITIAL RISK (or customer action)	VALIDATION: IDENTIFY SAFETY FUNCTIONAL TEST DONE TO CONFIRM REDUCTION OF INITIAL RISK	FINAL RISK LEVEL
Mechanical Hazards	Accumulator	High pressure	Maintenance	Impact, injection	Failure to depressurized before servicing	2B	N/A	Drain valve and pressure gauge added.	Procedure for safe draining added to the user manual. Add warning label to accumulator.	Edge was rounded in drawings; labels verified.	N/A	2E
	Accumulator	High pressure	Operation	Impact, injection	Ruptured accumulator, pressure exceeds capacity	2B	Supplier designed accumulator with sufficient safety factor above max system pressure; critical to safety feature on print	Add relief valve	Add procedure to manual to periodically test relief valve	Critical to safety feature from supplier (check certificate), manual procedure updated.	Factory testing on relief valve	2E
	Load frame	Falling object	Packaging / Handling	Crushing	Heavy object; unwieldly	1C	N/A	Lifting eyes on cross-head; critical to safety feature	Safe lifting procedure in manual. Add warning label for lifting.	Critical to safety feature (check certificate); labels verified.	N/A	1E

Ensure "Design Mitigations" and Manuals are Reviewed: Leveraging Existing HRA

- When leveraging existing Hazard & Risk Analysis, any "Design Mitigations" that were verified on a previous project and left unchanged do not need to be reverified
- When leveraging existing Hazard & Risk Analysis, any "Manual Mitigations" that were verified on a previous project and left unchanged do not need to be reverified

Design Mitigations **Paper & Documentation** **Verification**

Hazard Analysis Title:	(ENTER A TITLE NAME; e.g. product name, project title) *(not a customer name)*
Most Recent Revision Date:	(ENTER MOST RECENT REVIEW DATE; per the Attendance Record)
Intended Use	(ENTER INTENDED USE)

Assum[illegible] initial risk without[illegible] HW/SW safety m[illegible]sures applied.

								RISK REDUCTION *If the Initial Risk Level is Medium / High / Critical, then must do 1-3.*			Verification & Validation		
HAZARD TYPE / GROUP	PART OF MACHINE	HAZARD ORIGIN	SYSTEM STATE / MODE	POTENTIAL CONSEQUENCE(S)	CAUSE(S) *(TRIGGERS CONSEQUENCE)*	INITIAL RISK LEVEL		1 DESIGN OUT THE HAZARD *(INHERENTLY SAFE)*	2 HW/SW CONTROL MEANS *(SAFEGUARDING / COMPLEMENTARY)*	3 PAPER & DOCUMENTATION *(TRAINING / INSTRUCTIONS)*	VERIFICATION: IDENTIFY WHAT WAS DONE TO REDUCE INITIAL RISK (or customer action)	VALIDATION: IDENTIFY SAFETY FUNCTIONAL TEST DONE TO CONFIRM REDUCTION OF INITIAL RISK	FINAL RISK LEVEL
Mechanical Hazards	Accumulator	High pressure	Maintenance	Impact, injection	Failure to depressurized before servicing	2B		N/A	Drain valve and pressure gauge added.	Procedure for safe draining added to the user manual. Add warning label to accumulator.	Edge was rounded in drawings; labels verified.	N/A	2E
	Accumulator	High pressure	Operation	Impact, injection	Ruptured accumulator, pressure exceeds capacity	2B		Supplier designed accumulator with sufficient safety factor above max system pressure; critical to safety feature on print	Add relief valve	Add procedure to manual to periodically test relief valve	Critical to safety feature from supplier (check certificate), manual procedure updated.	Factory testing on relief valve	2E
	Load frame	Falling object	Packaging / Handling	Crushing	Heavy object; unwieldy	1C		N/A	Lifting eyes on cross-head; critical to safety feature	Safe lifting procedure in manual. Add warning label for lifting.	Critical to safety feature (check certificate); labels verified.	N/A	1E

Communicate Hazards to Assembly & Checkout

- The Project Engineer shall adequately communicate assembly and/or system hazards to the Assembly and Checkout personnel
- Specific awareness should be directed to:
  - HW/SW Control Means mitigations as these will not have been validated at the start of assembly/checkout
  - Paper & Documentation mitigations as these mitigations involve hazards that will potentially be present before, during, and after assembly/checkout

HW/SW Control **Paper & Documentation**

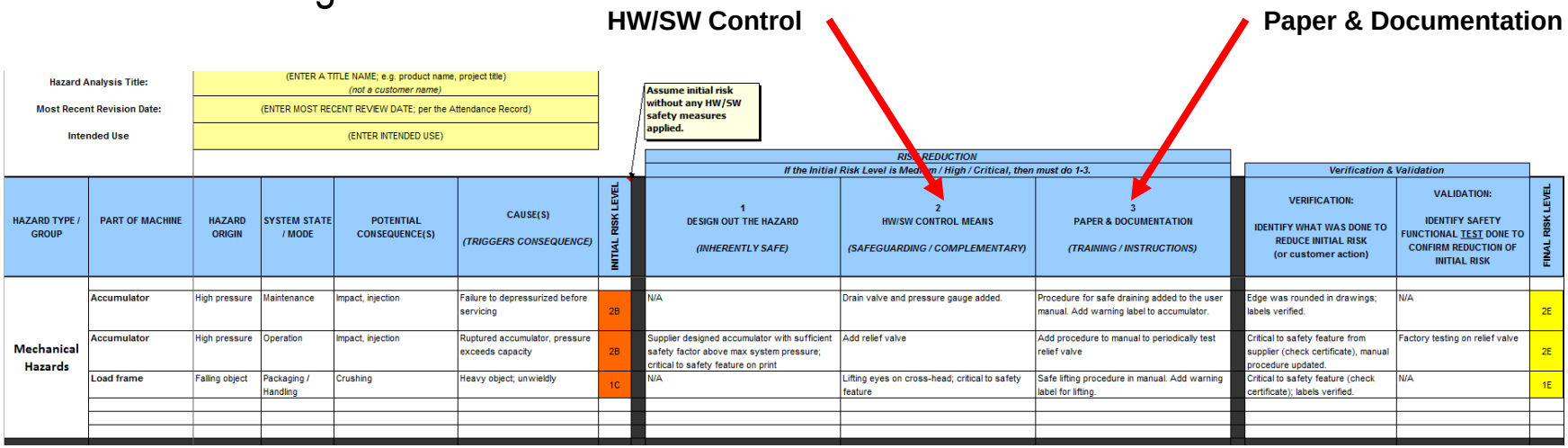
Hazard Analysis Title:	(ENTER A TITLE NAME; e.g. product name, project title) *(not a customer name)*
Most Recent Revision Date:	(ENTER MOST RECENT REVIEW DATE; per the Attendance Record)
Intended Use	(ENTER INTENDED USE)

Assume initial risk without any HW/SW safety measures applied.

							RISK REDUCTION *If the Initial Risk Level is Medium / High / Critical, then must do 1-3.*			Verification & Validation		
HAZARD TYPE / GROUP	PART OF MACHINE	HAZARD ORIGIN	SYSTEM STATE / MODE	POTENTIAL CONSEQUENCE(S)	CAUSE(S) *(TRIGGERS CONSEQUENCE)*	INITIAL RISK LEVEL	1 DESIGN OUT THE HAZARD *(INHERENTLY SAFE)*	2 HW/SW CONTROL MEANS *(SAFEGUARDING / COMPLEMENTARY)*	3 PAPER & DOCUMENTATION *(TRAINING / INSTRUCTIONS)*	VERIFICATION: IDENTIFY WHAT WAS DONE TO REDUCE INITIAL RISK (or customer action)	VALIDATION: IDENTIFY SAFETY FUNCTIONAL TEST DONE TO CONFIRM REDUCTION OF INITIAL RISK	FINAL RISK LEVEL
Mechanical Hazards	Accumulator	High pressure	Maintenance	Impact, injection	Failure to depressurized before servicing	2B	N/A	Drain valve and pressure gauge added.	Procedure for safe draining added to the user manual. Add warning label to accumulator.	Edge was rounded in drawings; labels verified.	N/A	2E
	Accumulator	High pressure	Operation	Impact, injection	Ruptured accumulator, pressure exceeds capacity	2B	Supplier designed accumulator with sufficient safety factor above max system pressure; critical to safety feature on print	Add relief valve	Add procedure to manual to periodically test relief valve	Critical to safety feature from supplier (check certificate), manual procedure updated.	Factory testing on relief valve	2E
	Load frame	Falling object	Packaging / Handling	Crushing	Heavy object; unwieldly	1C	N/A	Lifting eyes on cross-head; critical to safety feature	Safe lifting procedure in manual. Add warning label for lifting.	Critical to safety feature (check certificate); labels verified.	N/A	1E

Flow HRA Results to Checkout

- The Project Engineer shall work with the Hazard Analysis owner to identify verifications and validations that should take place during checkout
  - Examples:
    - Verify Accumulator Certificates
    - Test Pressure Relief Valves
    - Hazard Labels are Present
- Preferred method of flow down is through the Checkout Plan. If a checkout plan is not utilized, the Hazard & Risk Analysis shall be updated for any verified or validated mitigations



Communicate Install/Commissioning Hazards

- If the Project Engineer is managing the installation/commissioning (not utilizing the Service Organization), the Project Engineer shall:
  - Inform/Train the installation/commissioning team of potential hazards which will result, at a minimum, in awareness of the following topics:
    - Weights & Lifting Procedures
    - System Operation & Maintenance (via Manuals)
    - Lockout/Tagout
  - Provide capable oversight of all installation and commissioning activities to ensure the safety of observers and bystanders
  - Provide, at a minimum, training to the customer that outlines the Hazards related to operation and maintenance of the system

IMPORTANT

MTS SYSTEMS TRAINING

All Hazard & Risk Analysis Mitigations should be verified and/or validated prior to presenting the system to the customer for Acceptance

- If all mitigations cannot be verified prior to acceptance, then:
  - MTS shall inform the customer of the Hazard and the potential consequences
  - the customer shall acknowledge they understand the hazard and accept the risk associated with operation with the unmitigated hazard(s)

How do we get there?

- With help from Systems Engineering
- Projects will be audited, internal to PE organization
- Compliance:
  - All *S2 level projects (order entered after 22 Dec 2015) with an assigned systems engineering group team member shall be compliant
    and
    all existing projects with an assigned systems engineering group team member that ship after March 2016 shall be compliant
  - PE Managers will assign goals for product focused PEs of ETO projects

Associated Quality Records

- Hazard & Risk Analysis Report
- Design Review Minutes
- Checkout Plan

Revision Training Requirements

- New PE
  - Formal - Full training
  - Awareness - Full best practices
- Existing PE / Revision
  - Awareness - Email Distribution of any changes
  - Formal – Annual Online Training

Revision History and Approval

Rev	Change	Author	Effective Date
-	Original	T. MacPherson	22 Dec 2015
1	Update for FY17, change to annual online training	T. Kimball	12 Dec 2016

Name / Function	Signature	Date