Grantek Systems Integration

Understanding Machine Safeguarding and Lockout/Tagout

October 18th 2017

Jeff Winter, CSP, FS Eng.
Director, Safety Practice

Today's Speaker: Jeff Winter

BIO:

- TUV Certified Functional Safety Engineer (FS Eng)
- Board Certified Safety Professional (CSP)
- Industry speaker and writer
- American Society of Safety Engineers:
  - President of Three Rivers Chapter
  - Officer of Manufacturing Practice Specialty
- Z244.1 Accredited Standards Committee
- ISA Machine Safety Sub-Committee Chairman
- B11 Accredited Standards Committee
  - B11.19 Revision
  - B11.20 Revision

Today's Agenda

- Lockout/Tagout Vs. Machine Safeguarding
- Applicable Regulations and Standards
- Highlights of the new ANSI/ASSE Z244.1 Standard
- Example application of the standard
- How to move forward

Common Industry Battles

Lockout/Tagout is the regulation and the only way to keep people safe!

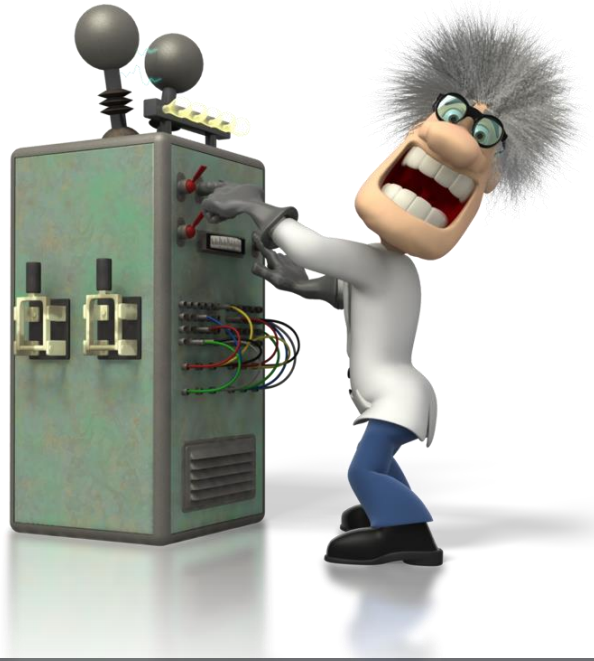
Lockout/Tagout is hindering our production!

EH&S **Operations**

What is Machine Safeguarding?

Machine safeguarding is a precautionary safety feature on equipment comprised of devices and methods designed to protect employees from hazards created by the equipment while working nearby or while operating equipment.

Simplified Goal: Keep people away



What are the requirements of Machine Safeguarding?

OSHA®

Part 1910: Occupational Safety and Health Standards

Subpart O: Machinery & Machine Guarding

- **1910.212:** General requirements for all machinery
- **1910.213:** Woodworking machinery requirements
- **1910.214:** Abrasive wheel machinery
- **1910.215:** Cooperage machinery - reserved
- **1910.216:** Mills and Calenders
- **1910.217:** Mechanical power presses
- **1910.218:** Forging machines
- **1910.219:** Mechanical power-transmission apparatus

What is Lockout/Tagout?

"Lockout/Tagout" refers to specific practices and procedures to safeguard employees from the unexpected energization or startup of machinery and equipment, or the release of hazardous energy <u>during service or maintenance activities</u>.

Simplified Goal: Remove hazardous energy

What are the requirements of Lockout/Tagout?

OSHA®

Part 1910: Occupational Safety and Health Standards

Subpart J: General Environmental Controls

1910.147: Control of Hazardous Energy

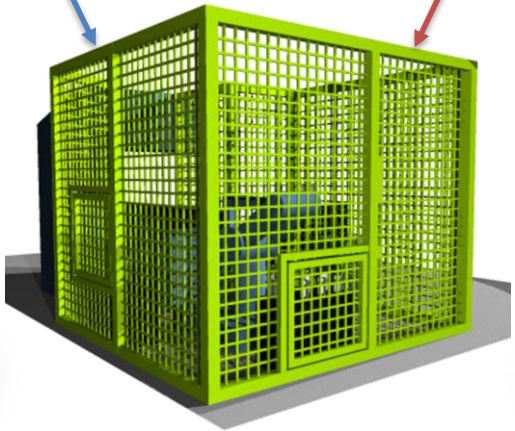
1910.147 establishes minimum performance requirements for controlling hazardous energy. The regulation specifies that employers must establish an energy-control program to ensure that employees isolate machines from their energy sources and render them inoperative before any employee services or maintains them.

Lockout/Tagout Vs. Machine Safeguarding

Lockout/Tagout

Protects employees during service and maintenance tasks

Default: Lockout by removing energy



Machine Safeguarding

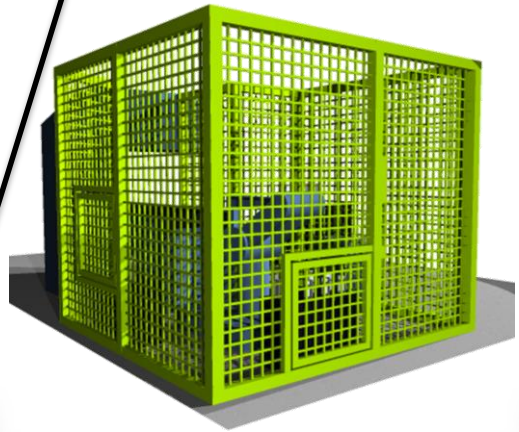
Protects all employees from general hazards, especially during normal operation

Default: Protect Operator by keeping away

Minor Servicing Exception

Lockout/Tagout

Exception to paragraph (a)(2)(ii): Minor tool changes and adjustments, and other minor servicing activities, which take place during normal production operations, are not covered by this standard if they are routine, repetitive, and integral to the use of the equipment for production, provided that the work is performed using alternative measures which provide effective protection (See Subpart O of this Part).



Machine Safeguarding

Two main goals of Machine Safeguarding:

- Identify hazards and evaluate risk (ideally based off their tasks)
- Appropriately apply control measures to protect against the hazards and reduce risks to acceptable levels

How does OSHA enforce 1910.147?

CPL 02-00-147:

- Inclusion of guidance on the minor servicing exception, specific energy control procedures, periodic inspections, and unexpected energization;
- Inclusion of information and guidance on *Alternative Methods to Lockout/Tagout (LOTO)*

How do employers demonstrate compliance?

“Assessment” standards make sure you identify and remediate hazards appropriately. (e.g. ANSI B11.0, ISO 12100, etc.)

“product” standards give you confidence that safety devices and technology are fail safe and designed correctly. (e.g. ISO and IEC Type B2 Standards)

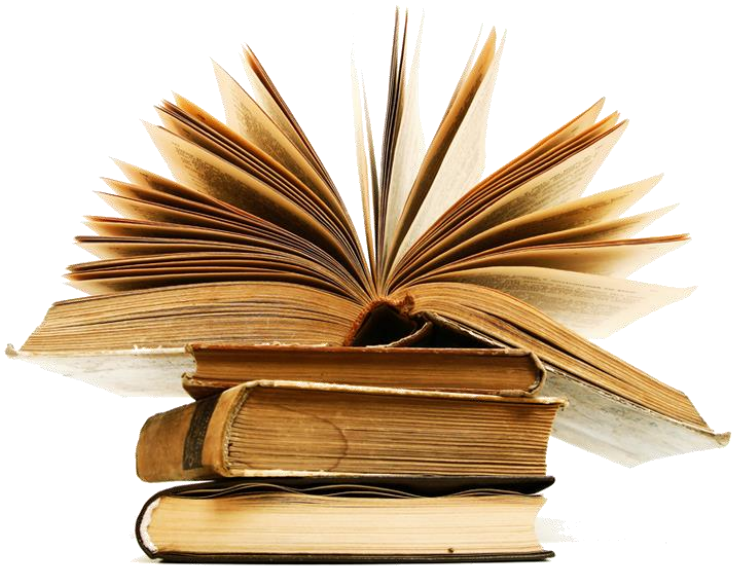
“Application” standards ensures safety devices and technology are applied, installed, and used properly. (e.g. ANSI B11.19, or ISO C-Type Standards)

“Performance” standards ensure each all safety systems (devices connected together) are designed to still work in the event of a failure. (e.g. ISO 13849-1, etc.)

“Validation” standards make sure ALL the pieces were put together properly to ultimately reduce the risk. (e.g. ISO 13849-2)

ANSI/ASSE Z244.1 History

- First publication 1982, reaffirmed in 1992
- Revised in 2003, reaffirmed in 2008 and 2014
- 2003 revision included major modifications were around “How to meet 1910.147 regulation.”
- 2016 revision had a 70% increase in participation from a variety of industries
- 2016 revision published in December of 2016



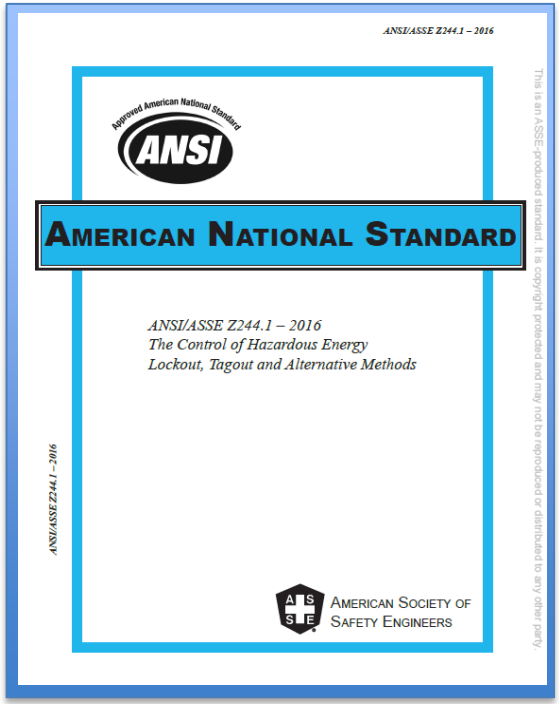
ANSI/ASSE Z244.1 Basics

2016 revision presents distinct requirements for controlling hazardous energy through 3 different approaches:

- Lockout (Primary approach)
- Tagout
- Alternative Methods

ANSI/ASSE Z244.1 Contents

1) Scope and Purpose
2) References
3) Definitions
4) **Responsibilities**
5) **Design of Machinery/Equipment for the Control of Hazardous Energy**
6) **Hazardous Energy Program**
7) **Control of Hazardous Energy**
8) **Alternative Methods of Hazardous Energy Control**
9) Annexes


ANSI/ASSE Z244.1 – 2016

Approved American National Standard

ANSI

AMERICAN NATIONAL STANDARD

ANSI/ASSE Z244.1 – 2016
The Control of Hazardous Energy
Lockout, Tagout and Alternative Methods

AMERICAN SOCIETY OF SAFETY ENGINEERS

Section 4 - Responsibilities

Notable changes in 2016 revision:

- All suppliers are now required to meet the design requirements (Section 5)
- Users (employers) now required to obtain equipment that complies with section 5.
- Users (employers) are responsible for upgrading non-compliant equipment to be compliant with section 5.

Actions to Consider

- Require Suppliers and OEMS to follow Z244.1 as part of corporate specifications to ensure all future equipment fits into your program.

Section 5 – Design Requirements

Notable changes in 2016 revision:

- Risk assessments are now required during the design phase of a project
- Documentation requirements
  - Procedures for use of energy isolating devices
  - Instructions for tasks requiring partial energization
  - Instructions for servicing and maintenance tasks
  - Instructions for releasing or controlling stored energy
- Use of warnings (e.g. labels, placards, etc.)
- Control Integration now commensurate with the risk
- Requirements for tamper resistance

Actions to Consider

- Evaluate what requirements are currently specified to suppliers. Do they easily support your current Lockout/Tagout program or conflict? Don't know?

Section 6 – Hazardous Energy Control Program

Notable changes in 2016 revision:

- Greater detail in the development of a hazardous energy control program, including the elements in each section.
- Addition of a change management program.
- New decision process for the selection of Lockout, Tagout, and Alternative Methods.

Actions to Consider

- How mature is your current Lockout/Tagout program? Does it even include the option for alternative methods?

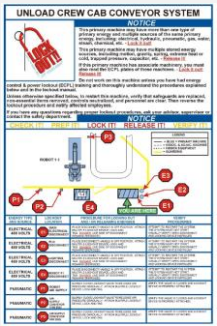
Section 7 – Control of Hazardous Energy

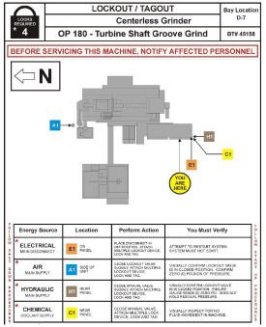
Notable changes in 2016 revision:

- Added elements needed in the development of procedures
- Verification of isolation has added emphasis on testing
- Expanded procedures for user-directed Lockout/Tagout device removal

Actions to Consider

- Do your Lockout/Tagout procedures include all appropriate elements to be best practice? (and compliant)





Section 8 – Alternative Methods

Notable changes in 2016 revision:

- Before Alternative Methods can be used:
  - Practicability/justification analysis
  - A risk assessment
  - Hazard control hierarchy evaluation
  - Evaluation of selected alternative method
- Alternative Methods must be designed by qualified individuals

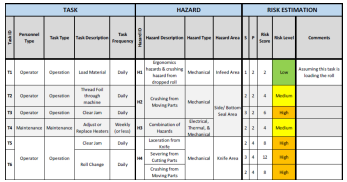
Actions to Consider

- Do you check if your suppliers and/or designers are certified in functional safety?

Potential Situations to use Alternative Methods

- Hazardous energy must be present because is required to perform the task
- Lockout or Tagout is not feasible or practicable
- When a documented risk assessment shows the task can be performed with acceptable risk
- When inherent hazards (e.g. thermal, radiation, etc.) are unable to be controlled using Lockout or Tagout
- When energy is required to maintain equipment in a safe state
- When repetitive cycling of an energy isolation device compromise the safety function

Identified as part of a Risk Assessment



TASK					HAZARD				RISK ESTIMATION				
Number	Personnel Type	Task Type	Task Description	Task Frequency	Number	Hazard Description	Hazard Type	Hazard Area	S	F	Risk Score	Risk Level	Comments
T1	Operator	Operation	Load Material	Daily	H1	Ergonomics Hazards & crushing hazard from dropped roll	Mechanical	Infeed Area	1	2	2	Low	Assuming this task is loading the roll
T2	Operator	Operation	Thread Foil through machine	Daily	H2	Crushing From Moving Parts	Mechanical	Daily/ Bottom Seal Area	2	2	4	Medium	
T3	Operator	Operation	Clear Jam	Daily					3	2	6	High	
T4	Maintenance	Maintenance	Adjust or Replace Heaters	Weekly (or less)	H3	Combination of Hazards	Electrical, Thermal, & Mechanical		2	2	4	Medium	
T5	Operator	Operation	Clear Jam	Daily	H4	Laceration from Knife	Mechanical	Knife Area	2	4	8	High	
T6			Roll Change	Daily		Severing from Cutting Parts			3	4	12	High	
						Crushing From Moving Parts			2	4	8	High	

Annexes – Industry Best Practices

LOCK/TAG/VERIFY PERIODIC INSPECTION			
Date:	Area:		
Inspector(s):			
[ ] [ ] Contractor	Crew/Team/Shift:		
Equipment:			
Task:			
Lockout Task ID:	Lockout Task Date:		
Authorized Employees: (Maintenance/Production who works on the equipment)			
1.	Job Position:		
2.	Job Position:		
3.	Job Position:		
4.	Job Position:		
Affected Employees: (Operators who work with the equipment)			
1.	Job Position:		
2.	Job Position:		
3.	Job Position:		
4.	Job Position:		
Energy-Isolating Device (Check all that apply):			
Electrical – Disconnect – Lock	Hydraulic – Stored Energy – Lock		
Electrical – Breaker Switch – Switch Device	Pneumatic – Ball valve.		
Electrical – PLC – Lock	Process – Line - Break in Line. Block in Line.		
Mobile Equipment – Battery – Key Control	Mechanical – Mobile Equipment – Blocking device		
1. Was the location (affected personnel) notified of work to be performed?	Y	N	NA
2. Have authorized employee's responsibilities been reviewed with them?	Y	N	NA
3. Does a written Lockout Task Procedure exist for the task?	Y	N	NA
4. If "Yes," was it followed?	Y	N	NA
5. If "No" explain how it was determined what to lock out.	Y	N	NA
6. Do authorized employees know where to find the Lockout Procedure?	Y	N	NA
7. Is all necessary hardware available to operators? (locks/tags/lockboxes/)	Y	N	NA
8. For equipment with a single isolation device: Was the isolation device properly identified?	Y	N	NA

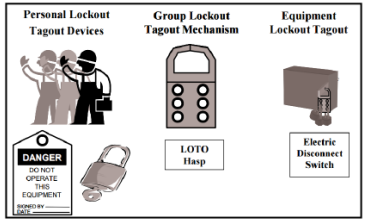
Example LOTO Inspection Form

Annex L-1 Sample Alternative Methods Practicability/Justification Evaluation

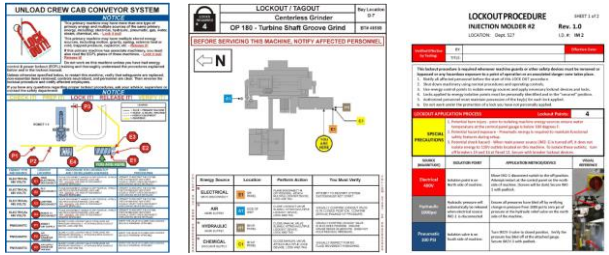
Alternative Method (Lockout) – Three Step Process (1) Justification Analysis (2) Risk Assessment (3) Alternative Procedure (from clauses 8.1, 8.,2.1.3)

PLANT:		DEPT:	**Extrusion**	METHOD REFERENCE:	**JSP #010-#016; LOTO 002**	NUMBER:	
TASK:	**Tool Cleaning/Polishing/Adjustments; Tool Changes; Clearing Discard Chute/Shear; Pit Entry for Tool Recovery**	NEW ☐	EXISTING ☐	MODIFIED ☐			
TASK DATA: Define the task characteristics (frequency of occurrence, personnel exposed; use history, current key safeguard, perceived risk)							
30-40 times/8 hour shift; press operator; task history (20+ years); trapped circuit key control system; serious level risk							
LOCKOUT IMPACTS: What is the impact of applying conventional lockout? (for example - process interruption, electrical device wear, employee additional risk, task interference, power needed for task completion, etc.)							
Each pump (4) shutdown requires a startup delay (5 minutes) to protect the pumps from fast cycling. Note: All press container/ram production tasks would require each pump to be cycled an additional 30 times/shift. Cycling disconnects multiple times causes excessive wear, potential failure and increased risk of arc flash.							
POTENTIAL OPTIONS: What can be done to avoid using power or reducing employee exposure? (task elimination, engineering/design changes; remote task completion; exposure reduction; product change, etc.)							
Improved press settings (crush)-recipe control data to minimize aluminum buildup. Increased nitrogen flow to improve surface condition, ensure billet lubrication system functioning properly							
OPTION PRACTICABILITY: What obstacles exist that prevent using potential options listed above? (Limiting factors for task power elimination; previous unsuccessful changes; inherent hazard/thermal, etc.)							
Inherent formation of some aluminum buildup on die/container face dictates cleaning necessity; customer demand and scheduling drives tooling changes							

Example Alternative Methods Justification



Example Group Lockout Program

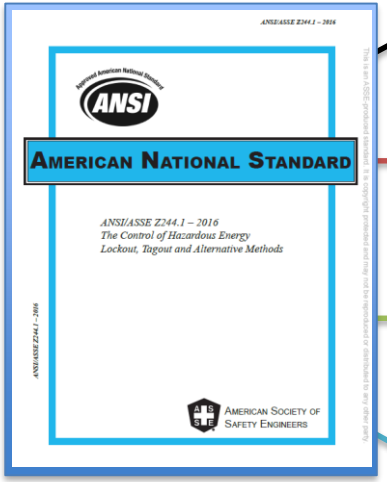


Example LOTO Procedures

Actions to Consider

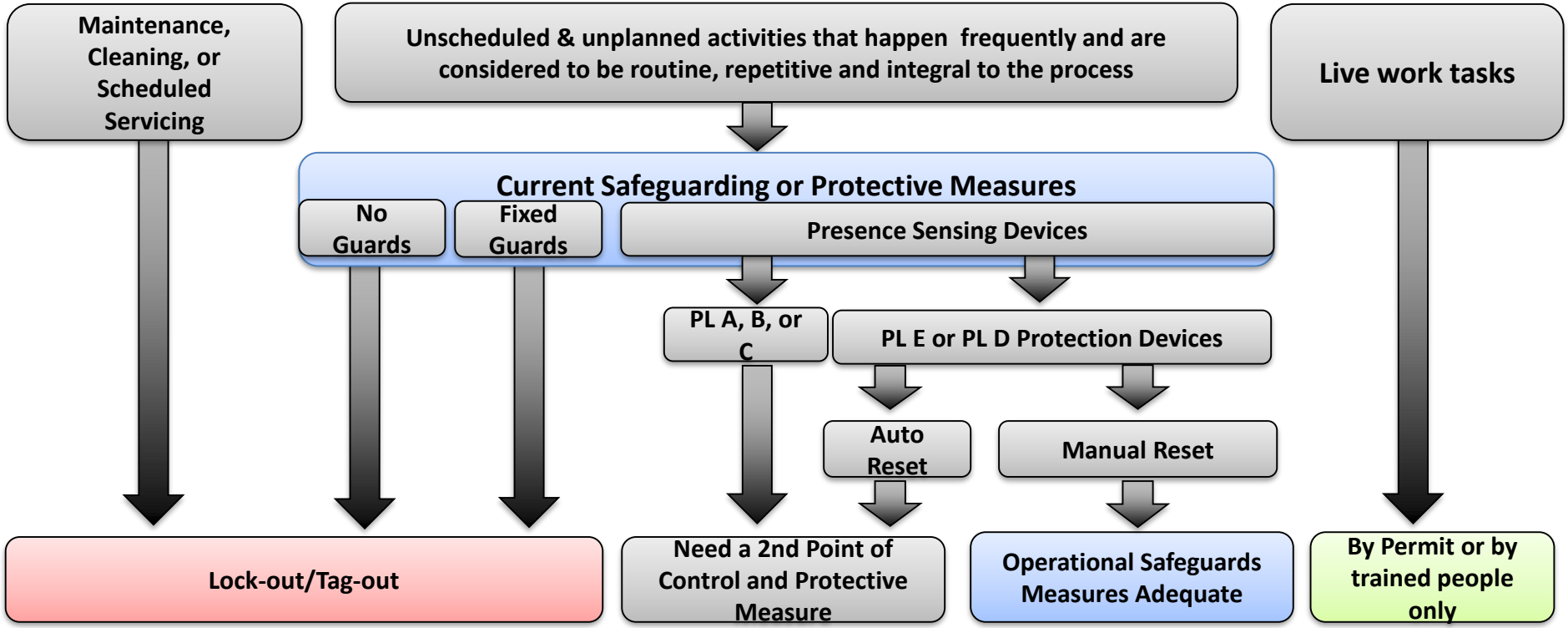
- Are any of the suggestions in the Annex worth turning into requirements for your company (either through your program or your specifications)?
- How do your current templates compare to the examples? Do they capture the same information?

Building a Program with Z244.1

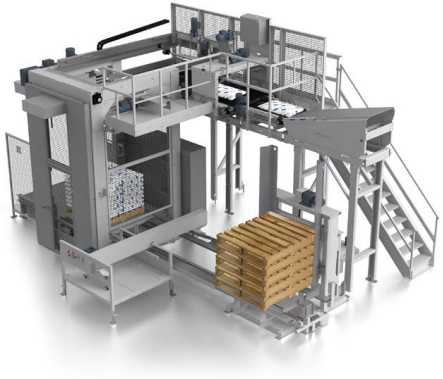


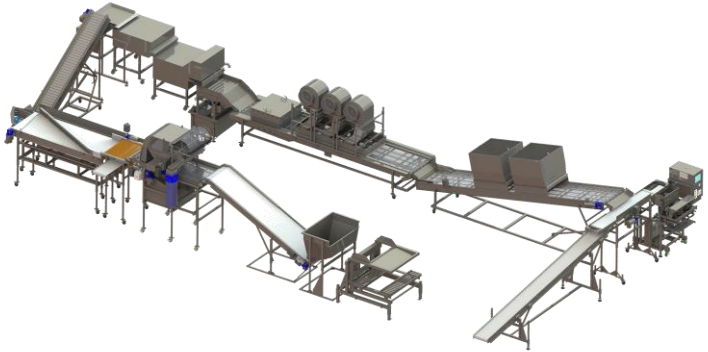
- **Lockout/Tagout Program**
  - Alternative Methods Justification
  - Task Based Risk Assessment Process
- **Machine Safeguarding Program**
  - Task Based Risk Assessment Process
  - Inspection and Testing of Safeguards
  - Training & Awareness
- **Safety Specifications**
  - Acceptable Methods of Safeguarding
  - Documentation Requirements
  - Design & Functional Requirements
  - Verification & Validation Requirements
- **Project Management Processes**
  - Verification & Validation Requirements
  - Deviations & Exceptions Management
  - Stage Gates and Approvals

Example Approach for applying a method



Example Application of Z244.1





STEP 1: Risk Assessment

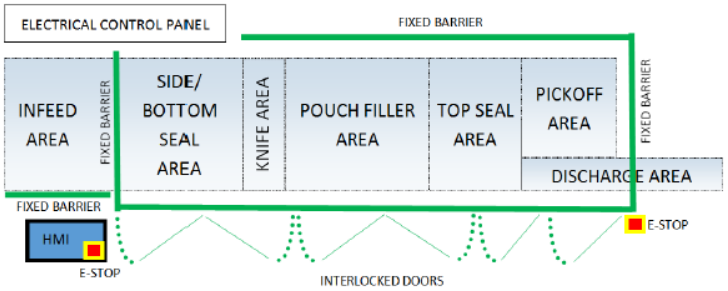
Item ID	Area	Hazard / Failure Mode	Severity of Harm	Exposure to Hazard	Possibility of Avoidance	Probability of Occurrence	Risk Level
RA.1.1	Upper Level Case Infeed & Diverter Area	**Upper Infeed Diverter Conveyor** Mechanical hazards: entanglement, crush	S4	F2	A2	O2	9
RA.2.1		**Upper Infeed Roller Conveyor** Mechanical hazards: entanglement	S3	F2	A2	O3	6
RA.3.1		**Upper Infeed Conveyor Stops** Mechanical hazards: impact	S3	F2	A2	O2	5
RA.4.1		**Upper Box Turners** Mechanical hazards: crush, impact	S3	F2	A1	O3	5
RA.5.1	Layer Forming Area	**Upper Pusher Bar** Mechanical hazards: crush, impact, entanglement	S4	F2	A1	O2	8
RA.6.1		**Upper Apron** Mechanical hazards: crush, impact, entanglement	S3	F2	A1	O2	4

Hazard Based Risk Assessment

TASK					HAZARD				RISK ESTIMATION				
Task ID	Personnel Type	Task Type	Task Description	Task Frequency	Hazard ID	Hazard Description	Hazard Type	Hazard Area	S	P	Risk Score	Risk Level	Comments
T1	Operator	Operation	Load Material	Daily	H1	Ergonomics hazards & crushing hazard from dropped roll	Mechanical	Infeed Area	1	2	2	Low	Assuming this task is loading the roll
T2	Operator	Operation	Thread Foil through machine	Daily	H2	Crushing from Moving Parts	Mechanical	Side/ Bottom Seal Area	2	2	4	Medium	
T3	Operator	Operation	Clear Jam	Daily					3	2	6	High	
T4	Maintenance	Maintenance	Adjust or Replace Heaters	Weekly (or less)	H3	Combination of Hazards	Electrical, Thermal, & Mechanical		2	2	4	Medium	
T5	Operator	Operation	Clear Jam	Daily	H4	Laceration from Knife	Mechanical	Knife Area	2	4	8	High	
T6			Roll Change	Daily		Severing from Cutting Parts			3	4	12	High	
						Crushing from Moving Parts			2	4	8	High	
T14	Operator	Operation	Adjust pickoff	Weekly (or less)	H10	Crushing from Moving Parts	Mechanical	Pickoff Area	2	2	4	Medium	
T15	Operator	Operation	Clean during running	Daily	H11	Crushing from Moving Parts	Mechanical	Discharge Area	1	4	4	Medium	
T16	Maintenance	Maintenance	Troubleshooting in Panel	Weekly (or less)	H12	Arc Flash/Shock from Electrical Parts	Electrical	Electrical Control Panel	4	2	8	High	
T17	Any	Operation	Any	Daily	H13	Burn from seal heaters	Thermal	Side/Bottom Seal Area	2	2	4	Medium	
T18	Any	Operation	Start/Stop Machine	Daily	H14	Combination of Hazards	Mechanical	Infeed Area, Side/Bottom Seal Area, Knife Area	3	4	12	High	
T19	Maintenance	Maintenance	Service and Repair of any Machine Components	Weekly	H15	Combination of Hazards	Electrical & Mechanical	Any	3	4	12	High	

Task Based Risk Assessment

STEP 2: Risk Reduction Plan



RISK REDUCTION INFORMATION								RESIDUAL RISK				
Risk Reduction Measure ID	Inherently Safe Design Measures	Engineered Controls Measures	Administrative Control Measures	Description of Risk Reduction Requirements	Associated Hazard Areas	Associated Tasks	Associated Hazards	S	P	Risk Score	Anticipated Residual Risk	Comments
R1	Not Required	Not Required	✓	• Appropriate pinch point hazard labeling shall be placed at the feed rollers • Proper safe work procedures developed for loading material	Infeed Area	T1	H1	1	1	1	Low	None
R2	Impractical	✓	✓	• An interlocked door shall be installed at the Main Drive Access. Opening this door during normal operation shall put the machine in a safe state. • Appropriate pinch point hazard labeling shall be placed at door handle	Infeed Area	T1	H1	1	1	1	Low	None
R3	Impractical	✓	✓	• An enclosure shall be installed around the machine to prevent access to all associated hazard areas. The enclosure shall start at the Top/Side Seal Area and end at the Discharge Area. The left and right panels of the enclosure shall be a fixed barrier guard that allows visibility into the machine and allows product to pass through. The back of the barrier shall be a fixed barrier that allows visibility into the machine and shall prevent the ability to crawl under or reach over into the hazard areas. The front barrier shall be comprised of a series of Interlocked access doors. Opening of any of these doors during normal operation shall put the machine in a safe state. These doors shall prevent the ability to crawl under or reach over into the hazard areas. • Proper safe work procedures developed for all tasks requiring authorized access. • Appropriate crushing and sheering hazard labeling shall be placed at each door handle	Side/Bottom Seal Area, Knife Area, Filler Area, Top Seal Area, Pickoff Area, Discharge Area	T2, T3, T5, T6, T7, T8, T9, T10, T11, T12, T14, T15, T17, T18	H2, H4, H5, H6, H7, H8, H10, H11, H13, H14	1	1	1	Low	None
R4	Impractical	✓	✓	• A fixed guard shall be installed as a shroud around the heating elements to prevent accidental contact. • Appropriate burn hazard labeling shall be placed on the interlocked access door for the corresponding hazard area	Side/Bottom Seal Area, Top Seal Area	T4, T13	H3, H9	1	1	1	Low	None

STEP 2.5: Evaluation of Existing Measures

Effectiveness of Existing Safeguarding Methods		
Evaluation Category	Analysis	Comments
Installation and Performance of Safeguarding Devices	Acceptable	Interlocked guard door meets the application and installation requirements of ANSI B11.19.
Proper use, design, and performance of Safety Functions	Acceptable	The interlocked guard appears to act as the safety function "Safety-Stop Initiated by a Safeguard." This function meets the requirements of ISO138149-1
Consideration of industry best practices/methods for selection, design, and application of safeguarding devices	Unknown	No industry standards were specified by customer or provided in documentation by the Machine Builder in regards to the assessment process, risk reduction process, application of safeguarding measures, or safety-related parts of control systems.
Stopping performance of equipment	Acceptable	Use of Safe Torque Off (STO) function on drives achieves adequate stopping performance. Machine Stop time <100ms and interlocked guard meets the safe mounting distance requirements of ANSI B11.19 Annex D.
Measures to ensure exclusivity/individual control	Acceptable	The access point is only large enough for one person to access at a time. Full visibility of the access point is possible during the entire duration of the task
Measures to ensure tamper resistance	Acceptable	Interlock Switch is a non-contact, type 4, coded magnetic switch as defined in ISO14119 and cannot be easily defeated by mechanical means.
Safeguarding does not introduce new hazards	Unacceptable	The design of the lift-up interlocked door introduces a shear hazard near the hinge when closing
NOTES:		

Item Evaluated	OK?	Current Solution	Suggested Corrective Actions
Interlocked Door	N	Vertical door that prevents access to machine. Position switches are not safety rated	Upgrade interlock switch per Safety Requirements Specification
Machine Enclosure	N	Enclosure surrounds entire machine, however there are numerous access panels that are not securely attached to the machine	Bolt all access panels in place using fastener that requires a tool for removal.
Safety photoeye	N	A safety photoeye is used to detect attempted access to machine while the door is in motion, however it provides insufficient detection area	Replace safety photoeye with Light Curtain to detect attempted access to machine while door is in motion
Emergency Stop Device(s)	N	Emergency Stop pushbutton located on Operator Station	Emergency Stop pushbutton shall be readily accessible and have a yellow background
Safety Logic Devices / Safety Circuitry	Y	Safety Logic Devices appear to be sufficient	None
Labeling and Awareness	N	None	Install hazard labels on all access doors that contain at a minimum: Hazard Word: Warning Hazard Icon: Pinch Point, Impact
Safe Work Procedures	N/A	Information not available	Create Safe Work Procedures for every task that requires regular access to hazard areas
Control of Hazardous Energy	Y	Electrical and Pneumatic lockout points provided	None

STEP 3: Evaluation of Task for Lockout

Areas of Interpretation	Grantek's Interpretation and/or Position
Determination of exposure to hazard(s)	Grantek follows the process established in ANSI B11.0:2010 to properly identify tasks, identify hazards, evaluate risk, score risk, and determine necessary risk reduction measures to reduce risk to an acceptable level. See Section 5.3 for Grantek's risk scoring matrix.
Definition for a "Routine Task"	*OSHA CPL 02-00-147 defines "Routine" as an activity that must be performed as part of a regular and prescribed course of procedure and be performed in accordance with established practices.* Grantek determines a task to be "Routine" if ***all*** the following conditions are met: • Task is required to be performed as part of a normal operating procedure as defined by the OEM, Machine Builder, or designer of the equipment/process. • Task has a documented procedure in order to perform in a safe manner.
Definition for a "Repetitive Task"	*OSHA CPL 02-00-147 defines "Repetitive" as an activity that must be repeated regularly as part of the production process or cycle.* Grantek determines a task to be "Repetitive" if ***one*** of the following conditions are met: • Task is required to be performed at regularly scheduled intervals (More than once per 24-hour period on continuous operations). • Task is required as the result of a consistent condition that normally occurs (More than once per 24-hour period on continuous operations)
Definition for a "Integral Task"	*OSHA CPL 02-00-147 defines "Integral" as an activity that must be inherent to the production process.* Grantek determines a task to be "Integral" if ***one*** of the following conditions are met: • Not performing the task may stop or damage the machine or process • Not performing the task may negatively affect the product or process being produced • The task requires the removal or bypassing of a guard or safeguarding device to perform the task

Task Evaluation				Available Methods	
Minor Task?	Task Performed During Normal Production Operation?	Task Integral, Routine, & Repetitive?	Lockout/Tagout Prohibit Task from Being Completed?	Lockout/Tagout	Alternative Methods
N	-	-	-	X	-
Y	N	-	-	X	-
Y	Y	Y	N	X	X
Y	Y	Y	Y	-	X
Y	Y	N	-	X	-

STEP 3: Evaluation of Task for Lockout

CONTROL OF HAZARDOUS ENERGY											RESIDUAL RISK				
Minor Service Exception Qualification						Control Measure			Requirements						
Task ID	Task Classification	Task Require Access to Machine?	Exposed to Hazard or Safeguard Not Utilized?	Is the task integral, Routine, & Repetitive?	Lockout/Tagout Prohibit Task From Being Completed?	Lockout/Tagout	Alternative Protective Measure(s)	Hazard Eliminated through Safeguarding	Description of Requirements (or Method of Equivalent Protection)	Measures for Exclusive Control	S	P	Risk Score	Anticipated Residual Risk	Comments
T10	NPO	Y	Y	Y	Y	-	✓	-	• Risk Reduction Measure R2 sufficient.	• Full body access not possible, therefore opened doors with interlocking device provides exclusive control. • Clear visibility of operator controls from hazardous area	1	1	1	Low	• Unsure if task can be modified to pull pouch at different points. Unsure if proposed guarding would hinder tasks. If so, additional protective measures are required. (Need to re-interview personnel who performs task)
T11	NPO	Y	Y	Y	N	-	✓	-	• Risk Reduction Measure R2 sufficient.	• Full body access not possible, therefore opened doors with interlocking device provides exclusive control. • Clear visibility of operator controls from hazardous area	1	1	1	Low	
T12	NPO	Y	Y	Y	Y	-	✓	-	• Risk Reduction Measure R2 sufficient.	• Full body access not possible, therefore opened doors with interlocking device provides exclusive control. • Clear visibility of operator controls from hazardous area	1	1	1	Low	• Unsure if power is needed on the machine to perform task (Need to re-interview personnel who performs task)
T13	S/M	Y	Y	N	N	✓	-	-	• Proper Arc Flash PPE required. Category of PPE determined by arch flash study • Electric and pneumatic energy isolating devices to be installed at or near the control panel.	• Disconnect devices shall be capable of being locked.	1	1	1	Low	

STEP 4 & 5: Verification & Validation

Safety Function	Functional Requirement per Risk Reduction Plan	Verification Activity	Pass / Fail	Comments
Emergency Stop	The removal of hazardous energy from Robot, Actuators, and Conveyors when the safety system detects that the Emergency Stop has been actuated.	Drawing Review	Fail	• Hazardous Energy Not removed: Pneumatic air is pressure still maintained on actuators
Safety Stop Initiated By A Safeguard	Actuation of the door switch or interruption of the light curtain will stop the machine and prevent motion by removal of hazardous energy from Robot, Actuators, & Conveyors.	Drawing Review	Fail	• Hazardous Energy Not removed: Pneumatic air is pressure still maintained on actuators
Prevention of Unexpected Start-up	After a stop command has been initiated by an Emergency Stop or a safeguard, the stop condition shall be maintained until safe conditions for restarting exist.	Drawing Review	Pass	

Design Verification

Safety Function	Associated Device IDs	Required Circuit Performance	Verification Activity	Pass/ Fail	Comments
Emergency Stop	I1, I2, I3, I4, I5, I6, I7, R1, L1, O1, O2, O3	Category 3 / Performance Level D	Drawing Review	Fail	• Output Contactors (O1 and O2) are not monitored for faults, reducing circuit architecture to *Category 1*. Suggest adding a N.C. contacts to each contactor (O1 and O2) as part of the "monitored manual reset" circuit on the safety relay (L1).
Prevention of Unexpected Start-up	R1, L1, O2, O3, O4	Category 3 / Performance Level D	Drawing Review	Pass	

Circuit Performance & Architecture Verification

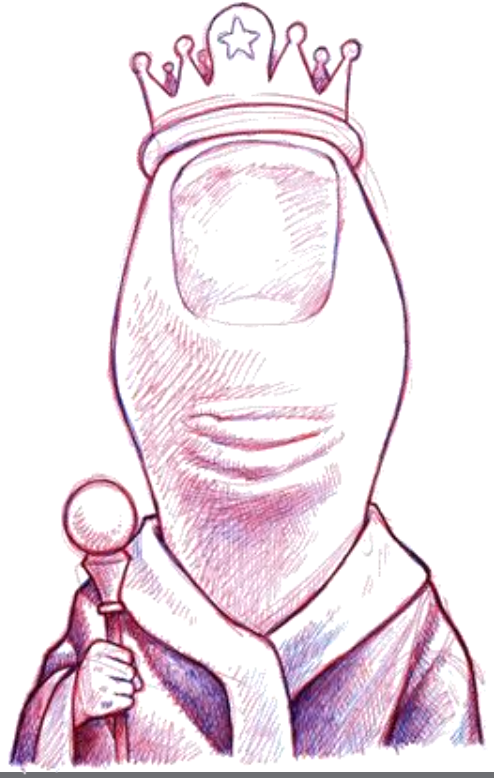
1.3	***Push E-Stop ES 126.021***	
a.	Verify illumination and color (red) on E-Stop	PASS / FAIL
b.	Verify that SIM126. 081 diagnostic indicators are not illuminated	PASS / FAIL
c.	Verify that SIM130.081 diagnostic indicators are not illuminated	PASS / FAIL
d.	Push Reset Button and verify that SIM126.081 and SIM130.081 indicators are not illuminated.	PASS / FAIL
e.	Pull E-Stop on ES126.021	
f.	Verify reset push button PBL126.101 illuminates	PASS / FAIL
g.	Push reset push button PBL126.101	PASS / FAIL
h.	Verify that the reset button PBL126.101 does not restart machine	PASS / FAIL
i.	Verify that SIM130.081 diagnostic indicators are illuminated green	PASS / FAIL
j.	Verify that SIM126.081 diagnostic indicators are illuminated green.	PASS / FAIL
k.	Verify reset push button PB126.101 is not illuminated	PASS / FAIL
l.	Push start button to verify power / functionality is restored to the machine	PASS / FAIL

Example Emergency Stop Validation Procedure

Summary

Rule of Thumb:

The absence of an injury does not mean the presence of safety. If you don't have written documentation explaining how your machine is safe, then its not safe.



Questions?