2024 NFPA TECHNOLOGY TASK FORCE REPORT

MACHINE SAFETY COMPENDIUM

TABLE OF CONTENTS

© 2024, National Fluid Power Association

BACKGROUND

As defined in the 2023 NFPA Technology Roadmap, many machine-level technology trends are actively shaping the future of the fluid power industry. These trends include the increasing electrification, connectivity, and autonomous functionality of mobile and industrial machines that use fluid power in their power or control systems.

In September 2023, NFPA launched two Technology Task Force teams, one focused on Mobile machinery and the other on Industrial machinery. Their task was to better understand these trends and engage stakeholders across the supply chain in developing the resources and connections needed to keep fluid power positioned as an actuation technology of choice on mobile and industrial platforms.

The Industrial Task Force identified several projects that would help it fulfill this mission, including:

- **Functional Safety**. Produce a white paper that (1) Reviews existing safety standards and machine directives; (2) Assesses risks and hazards associated with fluid power's use in upgrading older machines to automated functions and identifies common functions to address; (3) Identifies best practices and emerging technologies that minimize risks and hazards in those functions; and (4) Provides a resource to members that helps them understand and address the safe use of their systems.

The Task Force met multiple times to discuss this project, to share information and resources, and to develop a set of responses and recommendations. This report concludes the Task Force's final consensus, published on November 15, 2024.

This document is the intellectual property of NFPA. It is not for reprint, resale, or redistribution, in whole or in part, without the written permission of NFPA. It can be used, with permission obtained from NFPA, by organizations that wish to develop new technologies or applications that benefit the industries, markets, and people served by fluid power. By putting forth this report, representing a broad consensus of industry players, NFPA demonstrates a commitment to collaboration and the long-term growth and sustainability of fluid power technologies.

INTRODUCTION

The National Fluid Power Association's core mission is strengthening the fluid power industry. Machine Builders and OEMs agree that Functional Safety has become an essential part of the fluid power discussion regarding machine design, regardless of the energy source. The NFPA core membership has collaborated to produce this guide on the fundamentals of functional safety integration with fluid power components. Statistics indicate that control of hazardous energy has remained a top 10 violation for worker fatalities (OSHA, 2023).

The NFPA recognizes the need for a broader discussion and general understanding amongst the fluid power community to address proper processes in machine design. As such, this paper covers functional safety basics as a reference guide from a community of members interested in supporting machine builders and equipment manufacturers invested in building safe and compliant machinery for the global market.

REVIEW EXISTING SAFETY STANDARDS AND MACHINE DIRECTIVES

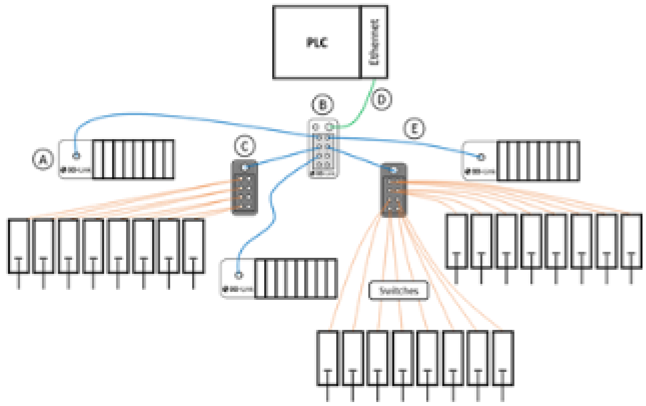
The Architecture of Machine Design

Machine design architecture has modernized from traditional collective wiring, known as hardwired, to more advanced networked arrangements. Networked communication typically uses an industrial bus protocol to transfer data, such as Ethernet/IP or ProfiNet. The bus connection is the physical layer of information and the communication language protocol. Advantages of networked communication include faster data response time, less wiring, fewer I/O cards at the PLC, and less cost. Most importantly, the devices on the network have IP addresses, allowing parameter data to be stored in the devices (such as valves) and process data (critical data) to be sent back to the master controller/PLC on the network.

This setup indicates shorts, over/under voltages, thermal warnings, and other critical data unavailable on the hardwired network. Engineers designed this communication to avoid failures that could lead to unplanned downtime, supporting predictive maintenance. Traditionally, they still hardwired safety on the machine as a separate, independent circuit. Each PLC manufacturer developed unique proprietary protocols: Rockwell/Allen Bradley uses Ethernet/IP, while Siemens uses ProfiNet. Initially, these networks used a bus topology, broadcasting data to all devices. Eventually, a ring topology emerged, allowing data to travel in a unidirectional loop.

IO-Link

IO-Link has become popular in recent years. It is a point-to-point means of networking components with an open protocol. IO-Link is a serial, bi-directional point-to-point connection for signal transmission and energy supply under any networks, field buses, or backplane buses*F[1]. It is a cost-effective connecting method despite limitations like cable length and transfer rate. IO-Link devices (not addressed) would connect to a master device (addressed), providing ease of installation, less cost for the devices, and the ability to communicate from the master back to the PLC over a bus network. This architecture is known as star topology because the devices connected to the master look like a spider or star when connected with the master as the body the devices plug into.



Item		Qty
A	IO-Link Valve Manifold	3
B	8 Port IO-Link Master	1
C	16 Port I/O Block	2
D	Ethernet Cable	1
E	5 Pin M12 Proximity Cable	5

Figure 1

Safety Over Network

Now, with three options for designing a machine (hardwired, networked, or IO-Link), thoughts turned back to how to integrate safety best. Safety over the network drove demand for "network safe" devices embedded with Profisafe, CIP safety, FSoE, and other safety protocols. Safety over the network required proprietary safety stacks to be embedded into products to communicate in the proper sequence, timing, and language to ensure safety was not lost or

© 2024, National Fluid Power Association

overlooked by the network traffic. Safety over the network has priority. The possibility to transfer safe (as opposed to "non-safe") data over networks has only really been possible since the turn of the 21st century when standard IEC 61784-3 was published, which covers functional safety field buses and gives the general rules and profile definitions of adding a safe data layer on top of existing field-bus protocols. (Kidman, Ph.D., 2020). Driving the push to network safety was dramatically simplifying wiring using existing field bus wiring, reducing I/O on devices, and reducing cabling and installation costs.

Further safety on a network can capture how many times an e-stop was pressed vs a traditional hardwired system with no data logs. This data could be used to eliminate downtime, find the source of problems, and reduce scrap materials in the production process. Safety protocols enable fail-safe communication between nodes by using the "Black Channel" approach recommended in IEC 61784-3. Black Channel is a secure method for transmitting safe signals between devices using a dedicated channel. Safe communication has a very low probability of dangerous failure and enables performance levels of up to PLe (EN ISO 13849) and safety integrity levels of up to SIL3 (IEC 62061). This principle allows for the transmission of both fail-safe and standard data on the same bus system.

IO-Link Safety

Manufacturers are preparing to introduce IO-Link Safety masters that use the Black Channel approach to enable IO-Link Safety (an open protocol) up to the Black Channel. The master then communicates with the network on a safety bus platform. These devices are expected to launch in 2025 and early 2026, offering an open protocol IO-Link method to transfer safety data across the network, which will significantly reduce development costs for network-capable safety devices.

Safety Circuits

A typical safety circuit includes an input device, a logic controller, and an output device. These three devices work together to achieve a safe function. Safety is not possible with one device. It is a functional result of the input communicating to the logic controller (usually via an electrical signal) and the controller then initiates a response from the output device for safety. Safe functions can include stopping, blocking, holding, reversing, and exhausting, to name a few. The pneumatic, hydraulic, and electrical safety functions will be elaborated later. Safety sub-functions are also commonly included in the safety circuit.

Two distinct architectures exist for safety circuits—Single-channel and Two-channel construction. The single channel is a single channel of connectivity, which can result in the loss of safe function*[F2]. It is used for lower categories of safety. The two-channel construction offers redundancy in the connections (dual contactors, etc.) to ensure a fail-safe method of interconnecting the devices*[F3]. Coupled with high diagnostic coverage in the logic controller and monitoring of the outputs, the two-channel architecture is used for higher safety level applications where risk is greater.

Figure 2

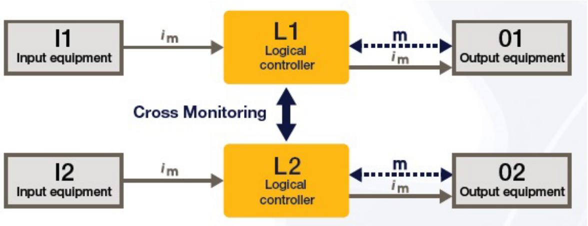


Figure 3

Risk Assessment

Regardless of the machinery architecture used to design machinery and the associated safety for a machine, Type A standards become relevant. These standards outline basic safety requirements for any machine. It is a legal requirement to perform a risk assessment on machinery. Machinery must be risk assessed by a qualified person who did not design the machinery. The risk assessment aims to determine possible mishaps, likelihood of occurrence, and consequences. This early assessment results in a PLr (performance level required). The machine must meet or exceed the PLr in final construction to achieve a final PL (performance level). The process typically involves conducting a risk analysis and then a risk evaluation[F4].

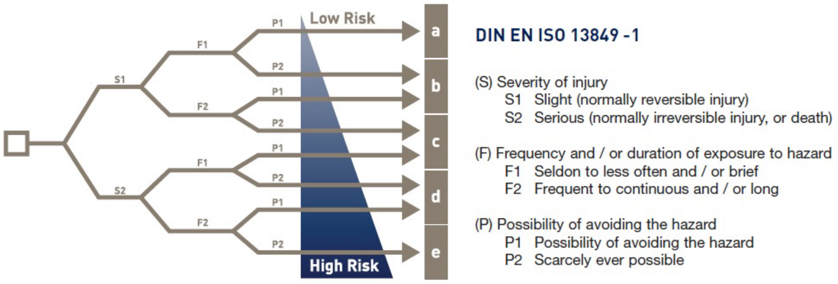


Figure 4

Risk Analysis

Risk analysis is a study of the machine design to determine the machine's limits, eliminate foreseeable misuse of the machine, and identify hazards (ergonomic, thermal, electrical, entanglement, mechanical, i.e.:(crushing, cutting, etc.). The list of liabilities is long, and extensive time spent here can save money, especially if risk can be designed out early in the design concept. Several methods can be used to conduct risk analysis, and a commonly used method is the HRN (hazardous rating number) system.

Risk Evaluation

The risk evaluation allows the machine builder to design out risk (where possible), and institute technical measures to protect from the risk. Technical measures usually come in the form of safety devices like light curtains, machine guarding, sensors, and laser scanners. These devices add cost to the machine build but may be necessary. Instructive measures (labeling) should only be used as a last resort when the risk cannot be safely eliminated and machine guarding or protective devices will not work. After risk evaluation, products with corresponding safety integrity may be selected to build the safety circuit. This is done through the calculation of $MTTF_{D,}$ (Mean time to dangerous failure) DC (Diagnostic Coverage) and CCF (Common cause failure)[F5].

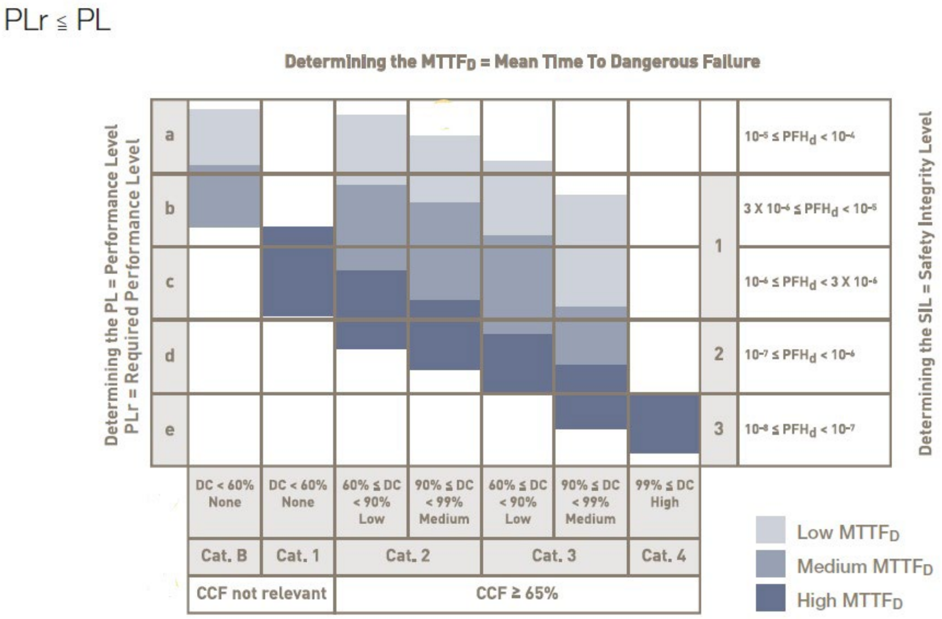
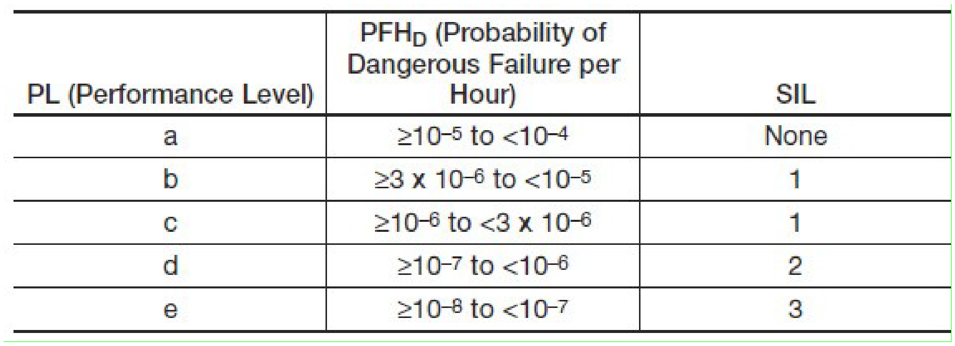


Figure 5

Correlation of SIL and Cat./PL

The language and methodology used in safety depends on the standards you follow. Industrial machinery typically follows machinery standards referencing category and performance level (IEC 62061/ ISO 13849). Both standards harmonize with the EU Machinery Directive 2006/2/EC. They both offer differing methods of conducting risk assessment but will result in a similar outcome. Note that the performance level (PL) ratings in ISO 13849 are correlated with a probability of dangerous failures per hour PFH_D value. SIL also correlates to PFH_D. This allows direct comparisons between the two standards. While there are no strict guidelines as to which standards you must use, some industries are more familiar with SIL, such as the process industry or nuclear applications. General industrial machinery tends to follow ISO 13849 and the PL (performance level) methodology[F6].



PL (Performance Level)	PFH_D (Probability of Dangerous Failure per Hour)	SIL
a	$\geq 10^{-5}$ to $< 10^{-4}$	None
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3

Figure 6

The PL can be assigned to a specific safety integrity level (SIL) level. However, it is not possible to infer the PL from the SIL.

Selecting Products B10 vs. MTTF

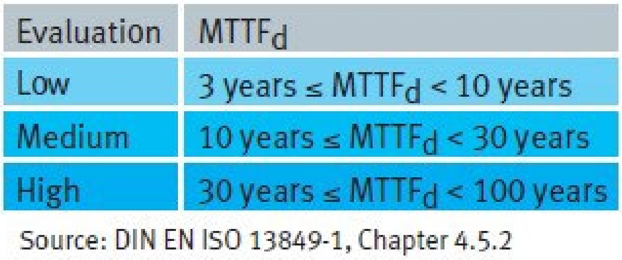
B10

In safety, it will come as no surprise that the higher the performance level or SIL level you wish to achieve based on your risk assessment, the more critical the component selection will become. Higher safety levels required the PLCs and safety controllers to have higher "diagnostic coverage." This detail can be found in the standards and in the many journals produced by manufacturers *(see Glossary of Terms).* Products in the higher safety echelon must be proven for use and made of well-tried and tested components, etc. This requirement has necessitated manufacturers publishing rated endurance life known as B10 or B10d (B10 dangerous) values. Following testing standards ISO 19973 for assessment reliability, manufacturers will test and publish values for products that are suitable for use as a safety-related part of a control system (SRP/CS). This test requires products to be mechanically tested or cycled until 10% of the sample lot has failed (under given conditions). The resultant value measured in switching cycles is the life expectancy of the product. B10 x 2 is equal to B10d (the point of dangerous failure).

MTTF

The MTTF (mean time to failure) of a product is the B10 value divided by 0.1 x nop (number of operations). Mathematically, it appears as MTTF=B10/0.1 x nop. Equivocally, MTTF_D =B10D/0.1 x nop.

In pneumatics, the number of operations is important in the calculation and can impact the MTTF value significantly. For this reason, pneumatic manufacturers will almost always publish the B10 or B10_D value. Hydraulics, on the other hand, are allowed to assume a given number of operations (ISO 13849-1) and will, therefore, do the calculations and publish an MTTF or MTTF_D value. The standards describe low, medium, and high life values as follows[F7]:



Evaluation	MTTF_d
Low	3 years ≤ MTTF_d < 10 years
Medium	10 years ≤ MTTF_d < 30 years
High	30 years ≤ MTTF_d < 100 years

Source: DIN EN ISO 13849-1, Chapter 4.5.2

Figure 7

There is often no means of mechanical cycle testing for electromechanical products. This is common in products with electronic boards, where failure is more likely than mechanical wear and will typically represent end-of-life. In this case, an MTTF calculation is performed on the wear components of the electronic board (resistors, diodes, optocouplers, etc.).

Functional safety uses many acronyms (*see Glossary of Terms*). Overall, the point is to determine the longevity and suitability of the part for the given SRP/CS so designers can make informed decisions about the life expectancy and mission time of components on machinery.

Coming Changes

Functional safety often refers to the Machinery Directive 2006/42/EC, which has been largely used since 2006 as law in Europe but has existed for over 50 years. It defines the mandatory essential health and safety requirements for the European market. Many countries harmonized with the standards, often introducing a relaxed version of the stringent European requirements. In January 2027, the directive 2006/42/EC will be replaced by regulation 2023/1230/EU. The new regulation is directly applicable in Member states in Europe, unlike those of a directive, which have to be transposed into national legislation. The legalities were one reason for the switch but also a modernization of the document. New changes include more emphasis on the technical file, which is documentation required for each machine, and new technologies like artificial intelligence (AI), autonomous mobile machinery (robots, and the Internet of Things (IoT), to name a few.

ANSI AND ISO STANDARDS FOR MACHINE INTEGRATION WITH FLUID POWER

Adhering to applicable ANSI and ISO standards is crucial to ensuring both compliance and safety when integrating fluid power systems into older machinery for automation. Different types of standards, categorized as Type A, B, and C, govern the safety requirements for machinery and fluid power systems. Machine integrators must apply a combination of these standards based on the specific machine type and the fluid power components used.

Type A Standards

Type A standards are overarching safety standards that cover the general safety principles and risk reduction strategies applicable to any machinery. These standards set the foundation for safe design practices.

- **ISO 12100:2010 (Safety of Machinery – General Principles for Design)**: Provides guidelines for risk assessment and reduction for machinery, including fluid power systems. The risk assessment process identifies hazards and implements design changes or safeguards to minimize risks.

- **ANSI B11.0 (Safety of Machinery – General Requirements and Risk Assessment)**: This standard mirrors ISO 12100 and is widely used in the U.S. It offers a systematic approach to identifying hazards and implementing protective measures essential for fluid power system integration.

Type B Standards

Type B standards are more specific and focus on common safety aspects such as protective devices, control systems, and ergonomics. The following standards are particularly relevant for fluid power systems:

- **ISO 13849-1:2015 (Safety-Related Parts of Control Systems)**: Covers safety requirements for the design of control systems, particularly for safety-related components in fluid power systems. It is critical when implementing control systems such as emergency stops and fail-safe measures in hydraulic or pneumatic setups.

- **ISO 4413:2010 (Hydraulic Fluid Power – General Rules and Safety Requirements for Systems and Their Components)**: These standards outline the design, installation, and maintenance of hydraulic systems. It is vital for ensuring the safe operation of hydraulic components, particularly in automated machines.

- **ISO 4414:2010 (Pneumatic Fluid Power—General Rules and Safety Requirements for Systems and Their Components)**: Similar to ISO 4413, this standard focuses on pneumatic systems and outlines safety practices to ensure proper design and operational safety.

- **ANSI B11.19 (Performance Requirements for Safeguarding)**: This standard specifies performance criteria for safeguarding mechanisms, including those in fluid power-driven machinery. It covers devices like interlocks, presence-sensing devices, and emergency stops to protect operators from moving machinery.

Type C Standards

Type C standards are machine-specific safety standards and provide detailed safety requirements for particular machine categories. For machine integrators upgrading older machines with fluid power systems for automated functions, a wide range of Type C standards apply based on machine type. Here are additional examples of Type C standards relevant to fluid power systems:

- **ISO 16092-1:2017 (Machine Tools – Safety – Presses)**: This standard applies to hydraulic and pneumatic presses, commonly retrofitted with automated controls. It provides detailed requirements for mechanical, electrical, and control system safety features, including emergency stops and safety interlocks.
- **ISO 10218-1:2011 (Robots and Robotic Devices – Safety Requirements for Industrial Robots)**: When fluid power systems are integrated into robotic applications, this standard governs the safety of the entire robotic system, including hydraulic and pneumatic actuators used for movement or control.
- **ISO 19085-1:2017 (Woodworking Machines – Safety – General Requirements)**: For woodworking machines, this standard outlines specific safety features when integrating fluid power systems, such as those used for clamping or automated cutting processes.
- **ISO 11161:2007 (Safety of Machinery – Integrated Manufacturing Systems)**: This standard applies when multiple machines, including those using fluid power, are integrated into a larger system for automated production. It ensures that safety systems are coordinated across all machines to prevent accidents from occurring during automated operations.
- **ISO 16090-1:2021 (Machine Tools – Safety – Milling Machines)**: For milling machines using hydraulic or pneumatic systems for tool or workpiece handling, this standard defines the safety requirements. It includes provisions for guarding, control systems, and safe energy dissipation.

- **ISO 23125:2015 (Machine Tools – Safety – Turning Machines)**: When fluid power systems are integrated into turning machines, this standard provides guidance on ensuring operator safety and preventing mechanical hazards such as ejection of parts or tools during high-speed operations.
- **ISO 23849:2010 (Guidance on the Application of ISO 13849-1 to Hydraulic and Pneumatic Safety Systems)**: A companion to ISO 13849-1, this standard offers specific guidance on applying functional safety principles to hydraulic and pneumatic systems, addressing how to meet different safety performance levels (PL) in fluid power applications.

Compliance and Risk Reduction

Machine integrators must identify the appropriate Type of standard based on the specific machinery they are upgrading with fluid power. These standards offer detailed safety requirements for designing and operating machinery safely, particularly when automating functions. Compliance with these standards ensures legal adherence and significantly reduces the risk of accidents or equipment failure.

Understanding Safety Subfunctions Categories CAT 1 to 4

When integrating fluid power systems into older machinery, safety-related parts of control systems (SRP/CS) play a crucial role in ensuring machine safety. The **ISO 13849-1** standard outlines four categories (CAT 1 to CAT 4) that define the reliability and fault tolerance of these systems. These categories help guide machine integrators in designing safety control systems that meet the required safety performance levels (PL) based on the application.

CAT 1: Basic Safety Measures

Category 1 safety systems rely on well-tried components and principles, ensuring basic functionality but minimal fault tolerance. In fluid power systems, these can be simple control circuits for hydraulic or pneumatic components. If a fault occurs, the system may not detect it immediately, posing a potential safety risk. As a result, CAT 1 is usually suitable only for low-risk applications where the consequences of failure are not severe.

CAT 2: Monitoring Safety Functions

Category 2 safety systems incorporate periodic monitoring to check for faults in control systems, typically at regular intervals. For example, a hydraulic press might include sensors to monitor pressure levels, ensuring that unsafe pressure does not build up over time. However, faults might go undetected between intervals because the system is only checked periodically, limiting its application in high-risk scenarios.

CAT 3: Redundant Safety Design

Category 3 safety systems use redundancy, meaning the failure of one channel or system component does not result in the loss of safety functionality. CAT 3 systems are designed to detect faults and maintain a minimum level of safety, making them suitable for applications where failure could lead to significant hazards, such as in hydraulic presses or automated robotic arms.

CAT 4: High-Level Fault Tolerance and Continuous Monitoring

Category 4 is the highest level of safety and is designed to detect faults immediately, ensuring that the safety system remains fully functional even with multiple faults. In fluid power systems, CAT 4 might include continuous monitoring of hydraulic pressure and actuator position, along with redundant safety circuits and emergency shutdown functions. CAT 4 systems provide the highest level of fault tolerance and ensure that even with a fault, safety functions remain operational.

BEST PRACTICES AND EMERGING TECH TO MINIMIZE RISKS AND HAZARDS

A. ISO 12100 builds the foundation for machinery safety. This standard will specify the basic terminology, principles, and methodology for achieving safety in machinery design. This standard should be used with ISO 13857 (Safety Distances), 13850 (Emergency Stop), ISO 13849 (Safety-related parts of control systems), ISO 14120 (Guards), and ISO 4413 (Hydraulic Systems). The standards are meant to help guide machine safety from concept to operation and after installation modification.

B. Tools exist that can help guide a team through a successful implementation of the ISO standards.

    a. SISTEMA is a free software tool for commercial use. It will assist your team in achieving a specific Performance Level (PL) and help you comply with ISO 13849:2023 and ISO 13850:2015.

    b. Pilz's safety Distance Calculator is free for commercial use. This application will help you comply with ISO 13857:2019.

    c. Other standards will require an understanding of the text as written. If additional assistance is needed, consulting services are offered to train your team.

C. SRA – Safety Risk Assessment

    a. A collection of stakeholders should perform an SRA to evaluate the process, machine, or operation. This team should not just be made up of one specific role in the design process (i.e. only engineers, only management, etc.).

© 2024, National Fluid Power Association

b. Each member should individually examine the process, design, or machine and record their findings using a risk matrix.

c. Findings should be discussed and stored in an appropriate yet accessible location for transparency.

d. Each risk should be considered using industry-standard methods to remove or reduce the potential for injury:

    i. Elimination – Remove the risk by design changes

    ii. Substitution – Lessen the risk by replacing the hazard with a lesser hazard

    iii. Engineering Controls – Using guards, shields, isolation to lessen the risk

    iv. Administrative Controls – Developing best practices, work instructions and procedures

    v. PPE – Additional protection items required due to not being able to reduce the hazard potential using any other methods

e. An external facilitator should be considered until proper training for risk assessments is completed.

f. Additional SRAs should be considered at significant project milestones. This will help prevent the discovery of risks after design, fabrication, and delivery are completed.

g. Customer acceptance of SRA is paramount in ensuring acceptable risk mitigation methods and helping ensure the protections put in place will be deployed.

Risks and Mechanical Hazards in Fluid Power-Driven Industrial Machinery

Fluid power systems—whether hydraulic or pneumatic—pose specific mechanical hazards when integrated into industrial machinery. These systems are often used to automate functions like actuation, movement, or clamping; however, the forces and pressures involved introduce unique risks. Identifying and mitigating these hazards is critical to ensuring safe operation.

Common Mechanical Hazards in Fluid Power Systems

1. **Stored Energy Hazards:** Hydraulic and pneumatic systems store energy in pressurized fluids or compressed air. This energy can result in severe injuries if released suddenly—due to a failure in seals, hoses, or valves. Machine integrators should apply **ISO 4413** and **ISO 4414** standards to manage stored energy, ensuring the use of proper pressure relief devices and implementing energy isolation procedures like lockout/tagout.

2. **Crushing and Pinching Hazards:** Fluid power systems often move large, heavy machine components, creating risks of crushing or pinching injuries. For example, hydraulic

cylinders used in automated presses can generate significant force, leading to serious injuries if an operator's hand is caught between moving parts. To mitigate these risks, safeguarding measures, such as fixed and movable guards or two-hand control devices, are essential and should follow **ISO 13857 (Safety Distances)** to ensure that hazardous areas are not easily accessible.

3. **Component Failures:** Burst hoses, leaking seals, or valve malfunctions can cause uncontrolled movements or sudden system depressurization in fluid power systems, potentially leading to accidents. Safety measures should include redundant systems, continuous monitoring, and fail-safe mechanisms to halt operations in the event of a component failure immediately. **ISO 13849-1** provides guidance on designing safety-related control systems to prevent or mitigate these types of failures.
4. **Noise and Vibration Hazards:** Pneumatic systems can generate excessive noise, while hydraulic systems may produce vibration during operation. Prolonged exposure to noise above acceptable levels can cause hearing damage, while vibrations may lead to equipment fatigue or operator discomfort. Compliance with **ISO 3744 (Acoustics – Determination of Sound Power Levels)** is necessary to measure and control noise levels in fluid power systems, while vibration mitigation strategies may involve the use of dampers or isolators.

Risk Assessment and Mitigation Strategies

A risk assessment, following **ISO 12100** or **ANSI B11.0**, is critical to identifying hazards associated with fluid power systems. Effective mitigation strategies include:

- **Regular maintenance and inspection** to identify wear and prevent catastrophic failures.
- **Use of appropriate safety devices** such as pressure relief valves, emergency stops, and guarding systems.
- **Safeguarding** through physical barriers or distance to prevent access to hazardous zones, especially around moving machinery driven by fluid power systems.

By addressing these mechanical hazards, integrators can ensure that machines upgraded with fluid power systems operate safely and reliably in industrial environments.

Validation of the Control System

One of the most critical aspects of machine design is one of the most overlooked. Validation of the control system (ISO 13849-2). Validation ensures the system will operate as intended and, in the event of a failure, will fail safely. Validation is also a spot check to ensure the Category and performance level are met. The best method of observing this performance and behavior is simulation testing. Fault injection testing can be a reliable means of detecting errors (or an accumulation of errors) in a system. Did the control system detect the fault? Did the machine fail safely? A detected fault is considered safe in functional safety because the control system has an opportunity to respond. Undetected faults are dangerous. Validation consists of applying analysis and executing functional tests in accordance with a validation plan. Testing can avoid costly mistakes if done in parallel with the design process. Fault tree analysis (FTA), as well as failure modes, effects, and criticality analysis (FMECA), are often used. Parts may perform fine in testing by the manufacturer, but many situations have arisen where parts do not work well together due to timing, software, or environmental factors such as temperature, stress, and corrosion that would not be seen without the validation. ISO 13849-2 is an excellent guide to better understanding the validation process.

Compliance and Markings

Machinery must comply with the laws of the country in which it will reside. This poses challenges for the machine builder to comply with standards they may need to familiarize themselves with if they are exporting. Some countries (Europe) require a representative body responsible for their equipment to reside with the EU. Partially completed machinery is subject to very similar rules as completed machinery (a loophole once used to avoid compliance requirements). In Europe, products must bear the CE mark, which is a declaration from the manufacturer that the product meets the legal requirements. It is a self-declared mark applied by the manufacturer and comes with applicable documentation, including a Declaration of Conformity signed by the manufacturer. Products that do not bear the CE mark are removed from service.

Similarly, in North America, products require electrical certification marks (given voltages). These marks are not self-declared and must be tested by an NRTL (Nationally recognized testing lab). Any legal NRTL can do the testing (https://www.osha.gov/nationally-recognized-testing-laboratory-program/current-list-of-nrtls), and some specialize in specific testing like hazardous ratings. UL is common in the United States, and CSA is preferred for Canada; however, they can and do test/certify to each other's standards. They are not harmonized. UL testing to Canadian standards would apply a cULus. The large middle letters indicate who the notified body is: UL. The small c and small us means it was tested to both Canadian and US Standards and, therefore, is suitable for sale in both countries. Likewise, if CSA tested to both standards, the product would bear the mark cCSAus. Other NRTLs that are growing in popularity include TUV, Intertek, and ETL, to name a few.

EMERGING SAFETY SOLUTIONS: PLCs, NETWORKS, TEST PULSED, IO-LINK, AND OSSD

The risk analysis will dictate the safety sub-function necessary for the application. For example, entering a gated area to add raw material in an automated process may require PUS or prevent unexpected start-up. Traditionally, this can be done by removing an energy source (e.g., removing air or disconnecting electric power). However, other methods are beneficial for modern controls.

Consider using a modern safety PLC with a safety I/O module and a safe network protocol. A modern control architecture can improve installation time, reduce complex circuits, and improve machine performance. For pneumatic systems, consider safety without exhausting compressed air. Energy costs are reduced, and cycle time is not extended for refilling the machine.

The principles of a safe network system require that the endpoints are designed to be safe. Today, this is primarily an ethernet-based network, but it does not have to be. IO-Link and AS-I both have a safety variant as well. These protocols have a safe service that assures messages are not disrupted, stale, incomplete, broken, etc. They typically have additional checksum and timestamping methods as compared to standard messaging. However, the endpoints must also be able to assemble and decode these messages safely. This requires redundancy built into the safety devices of dissimilar components and crosschecking.

A Black Channel is a secure communication method for transmitting safe signals between devices using a dedicated channel. This is independent of the standard communication used for control and allows for the use of standard physical media such as ethernet cables, switches, etc. Networked safety devices are more expensive, but since they coexist on the same networked infrastructure as standard devices, they reduce infrastructure costs associated with deploying a separate safety system.

Modern networked systems can reach PLe by observing the requirements of ISO EN 13849-1. To reach high-performance levels, systems must be monitored. For PLe, >99% diagnostic coverage (monitoring) is required. To reach these levels, modern control systems employ several techniques that can be used with fluid power systems.

A. **Safety Outputs with Test Pulses:** Fluid power devices such as solenoid coils or valve manifold coil power can be driven by the safety outputs of a safe controller or safe I/O module. The safe output will have redundancy built in, but it must be certain that the cable connecting the devices is not shorted to a source or ground. In this case, a test pulse will drop the output signal momentarily to a level where internal electronics can determine if short circuits exist. (Short circuits may happen accidentally, may have been a result of troubleshooting, or maybe an intentional override). This pulse can be in a fraction of a MS to several MS. Continuous monitoring means DC > 99%. It must be noted for fluid power systems that some solenoid coils may be sensitive to pulses from some devices, and these coils may have an audible tick, plus also may have a reduced life span due to this pulse. Some systems have been designed to mitigate this. Fluid power users should check this before deploying a test pulsed system.

B. **OSSD Signals:** OSSD stands for output signal switching device. OSSD outputs are from a safety device such as a light curtain or a sensor. They will connect to the safe input of an electronic module. The OSSD device uses redundant signals, with each having a test pulse out of phase with the others. The device can detect a fault or cable short and shut off. These sensors are part of the safety-related part of the control system and must be continuously monitored.

C. **Pilot-Air Control:** A redundant method for preventing a valve from operating may be to remove its pilot air in addition to solenoid power. Many pneumatic valves are internally air-piloted, and they require both an electric signal to energize the solenoid and a pneumatic force to shift the spool. The SRP/CS must monitor both channels for a high PL. Networked inputs can be used to monitor power and pressure. Modern valve terminal design can easily support voltage monitoring of the pneumatic solenoids and provide integrated pressure sensors for monitoring pilot air via the network.

D. **Safe Exhausting Can Also be Achieved in a Similar Way as Pilot-Air Control**: A redundant exhaust valve can be used to control all the air supplied to a valve terminal. The SRP/CS can also monitor this for both actuation power and pressure. Depending on the directional control valve design, this can be safely exhausted, allowing actuators to come to a resting state without pneumatic potential. This typical use case may be done if a directional control valve position or actuator cannot be determined.

E. **Directional Control Valve Design with Negative Overlap Spools Can Also Add to the SRP/CS:** These valves are designed to allow compressed air to exhaust if they are in an undetermined position due to missing power or a jam. In combination with safe exhausttting, this ensures the removal of pneumatic potential within the system.

© 2024, National Fluid Power Association

F. **Modern Safety Systems Will Typically be Controlled by a Safety PLC**: This will dedicate a portion of their logic capability to safety. They are designed to provide protected configuration and safe execution of the safety devices and logic. Safety instructions or function blocks are provided by the PLC Supplier or Manufacturer to make safe logic executions easier. The PLC Supplier or Manufacturer provides safety instructions or function blocks to make safe logic executions easier. The function block will ensure these signals are within a synchronized period and will safely shut off power if the signals are out of sync or if commanded by a safety device such as an OSSD sensor, Emergency Stop button, or other safety device.

GLOSSARY OF MACHINE SAFETY TERMS AND ABBREVIATIONS

Term	Defined
a, b, c, d, e	Performance level designation
Adequate risk reduction	Action to prevent risk that is considered reasonable based on technology available
Adjustable guard	A guard which can be wholly or partially adjusted or moved
ANSI	American National Standards Institute
AOPD	Active optoelectronic protective device (light curtain)
B, 1,2,3,4	Category designation
B10	Number of switching cycles until failure occurs in 10% of the sample lot
B10d	Number of switching cycles until dangerous failure occurs in 10% of the sample lot.
Black Channel	Communication channel without available evidence of design or validation
Cat.	Category (B,1,2,3,4)
Category	Classification of SRP/CS parts by resistance to faults and reliability
CCF	Common Cause Failure
CEN	European committee for standardization
CENELEC	European committee for electrotechnical standardization
Common Cause Failure	Failure of different items resulting from a single event
Common mode failures	Failures of items by the same fault mode (can be from different causes)
Comparative emission value	Set of data used to compare two or more machines pollutants
Condition Monitoring	Major component of predictive maintenance monitoring a parameter of condition in machinery (vibration, temperature, etc.)
Control system	The system that is used to manage components on a machine circuit

CS	Control system
Dangerous Failure	Failure that results in dangerous state or malfunction
DC	Diagnostic coverage
DCavg	Average diagnostic coverage
Design measures	Specific actions, techniques, or features incorporated into a product, structure, or system during the design phase to achieve a particular goal
Diagnostic Coverage	The effectiveness of a system's diagnostic capabilities in detecting and addressing faults or failures within the machine's components or processes
DTI	Device Tool Interface, a software interface for navigation to and invocation of Dedicated Tools including parameter transfer
Emergency operation	Actions and functions to end an emergency situation
Emergency situation	Hazardous situation needing urgent attention
Emergency stop	A function initiated by a single human action to prevent or stop a hazardous situation
Emission value	A number to quantify a machine generated pollutant (such as noise or vibration)
Enabling device	A device that is used in conjunction with a start control to allow a machine to function
Energy dissipation	Removal of stored energy from a machine
E-stop	Emergency stop
ESD	Emergency Shut Down
EU	European Union
F, F1, F2	Frequency of exposure to hazard
Failure	Termination of the ability of an item to perform a required function
Failure to danger	A malfunction that increases a risk
Fault	Inability to perform a required function in a components normal state
FB	Function block
Fixed guard	A guard secured to provide protection that is not easily removed
FS-AI / AO	Functional Safety Analog Input / Output module in a remote I/O
FSCP x	Functional Safety Communication Profile for a particular fieldbus x
FS-Device	Single passive peer such as a functional safety sensor or actuator or to a Master with functional safety capabilities
FS-DI / DO	Functional Safety Digital Input / Output module in a remote I/O
FS-Master	Active peer with functional safety capabilities connected through ports to one up to n Devices or FS-Devices and which provides a Standardized Master Interface to the gateway to the upper level communication systems (NSR or SR) or controllers with functional safety capabilities
Gateway	Network node equipped for interfacing with another communication system that uses different protocol
Guard	A physical barrier installed to provide protection

Harm	Physical injury or damage to health
Hazard	Potential source of harm
Hazard Area	Zone where person can be exposed to a hazard
Hazardous event	An event that can cause harm
Hazardous situation	Where a person is exposed to at least one potential harm
Hold to run control device	A device which initiates and maintains machine function only when manually actuated
I, I1, I2	Input devices
Industry 4.0/IoT	Current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of Things and cloud computing
I/O	Inputs / outputs
i_m	Interconnecting means
Impeding device	A device that creates an obstruction (such as a rail or barrier)
Instruction measures	The guidelines, procedures, and information provided to ensure the safe and correct use, maintenance, and troubleshooting of a machine
Intended use	Use of a machine as set out in the operating instructions
Interlocking device	A device that will prevent the operation of a machine if conditions are not met
Interlocking guard	A guard which works with the SRP/CS to provide protection based on the state of the machine
Interlocking guard with start function	A guard which allows a machine to start only when ideal conditions are obtained.
IODD	Electronic device description
IO-Link Safety	Functional safety communication extension for IO-Link
ISO	International Standards Organization
Isolation	Disconnecting or separating
L, L1, L2	Logic devices such as a PLC
Limiting device	Device that prevents a hazardous condition based on a machine's operating variables
LOTO	Lockout-tagout (LOTO)
Machinery	Components joined together to perform and intended function
Maintainability	Ability of a component to be looked after to fulfil an intended function
Malfunction	Failure to provide an intended function
Manual reset	Function in the SRP/CS used to restore safety functions before restarting a machine
Monitoring	A function to ensure adequate protection is provided in the event of a failure
Movable guard	A guard which can be opened or moved without the use of tools
MTBF	Mean time between failures

MTTF	Mean time to failure
MTTFd	Mean time to dangerous failure
MTTR	Mean time to repair
n_{op}	Number of operations (annually)
NSR	Non safety-related
O, O1, O2	Output devices
OSSD	Output signal switching device
OTE	Output on test equipment
P	Potential of avoiding the hazard
Performance Level	Level used to specify the ability of safety-related parts of control systems to perform a safety function
PFH	Probability of failure per hour
PFHd	Probability of dangerous failure per hour
PL	Performance level
PLC	Programmable logic controller
PLr	Performance level required in order to achieve the required risk reduction for each safety function
Port	IO-Link communication channel on a Master /FS-Master
Predictive Maintenance	Techniques to help determine the condition of in-service equipment in order to predict when maintenance should be preformed
Protection Against Tampering	A benefit from integration or safety functions
Protective measures	A measure taken to provide protection from a hazard
PUS	Prevention of unexpected start-up (lockout-tagout)
Reasonably foreseeable misuse	Use of a machine for purposes other than intended in the operating instructions
Relevant hazard	A hazard associated with a machine
Reliability	Ability of a component to perform a specific function without failing for a period of time
Remote I/O	(Fieldbus-)
Residual	Remaining or left behind
Residual risk	Risk remaining after protective measures have been taken
Risk	The potential for harm or adverse effects resulting from the operation, malfunction, or failure of a machine
Risk analysis	Determining risk based on hazards and machine limits
Risk assessment	Process of analysis and evaluation of risk
Risk estimation	Determining the probability of an occurrence that could be harmful
Risk evaluation	Process of assessing and interpreting identified risks to determine their significance and decide on appropriate actions
S, S1, S2	Severity of injury

© 2024, National Fluid Power Association

Safeguarding	Actions or equipment to protect where design measures cannot adequately provide protection
Safe Reversing	Covered under safe direction (SDI), but more explicit.
Safe Switch-Off	Switching off electric power to a pneumatic valve coil. It's what happens during an emergency shut down (ESD)
Safety function	A function that can result in a potential risk if failure occurs
Safety-related part of a control system	Part of a control system that responds to safety-related input signals and generates safety-related output signals
SAR	Safe Acceleration Range
SB	Safe blocking
SBC	Safe brake control
SCA	Safe cam
SDE	Safe de-energization
SDI	Safe direction
Sensitive protective equipment	Equipment capable of detecting persons or parts and able to generate a signal for the CS
SET	Safe equilibrium of torque
SEZ	Safe energization
Significant hazard	A hazard requiring specific action to remedy it
SIL	Safety integrity level
SLA	Safe limited acceleration
SLC	Safety Light Curtain
SLI	Safely limited increment
SLP	Safe Limited Pressure
SLP	Safely limited position
SLS	Safely limited speed
SLT	Safely limited torque (force)
SMD	Safely monitored deceleration
SMT	Safe motor temperature
SOS	Safe operating stop
SPE	Sensitive protective equipment
SRP	Safety-related part
SPM	Safe pressure monitoring
SRP/CS	Safety related parts of a control system
SRS	Safety requirements specification
SS1	Safe stop 1
SS2	Safe stop 2
SSB	Safe stopping and blocking
SSC	Safe stopping and closing
SSM	Safe speed monitoring

© 2024, National Fluid Power Association

SSR	Safe speed range
SSx	Safe stopping
Start-up	A change in motion from rest to movement
STO	Safe torque off
STR	Safe torque range
SVP	Safe valve position
Systematic failure	Failure related to a certain cause in the design, manufacturing or other factors
T10d	Mean time until 10% of components fail dangerously
TE	Test equipment
THC	Two hand control
T_M	Mission time
Two handed control device	A device requiring actuation with both hands to allow machine function
Unexpected start-up	A motion that creates a risk which was unintended
Usability	The ease of understanding the function of a machine or its controls
ISO	International Standards Organization

Glossary of Common Machine Safety Standards (for Industrial Machinery)

Standard	**Type**	**Defined**
Type A standards are basic safety standards giving basic concepts, design principles, and general aspects that can be applied to all machinery.		
IEC 61508 (International)	A	Functional Safety of Electrical/Electronic/Programmable Electric Safety-related systems.
IEC 61511	A	Functional safety – Safety instrumented systems for the process industry sector
ISO 12100:2010	A	Safety of machinery – General principles for design – Risk assessment and risk reduction.
ISO 14121		Safety of machinery – Principles for risk assessment
ANSI B11.0	A	Safety of Machinery
ANSI B11.26	A	Machines – functional safety for equipment – general principles for the design of safety control systems using iso 13849-1
Type B standards are generic safety standards covering safety aspects or one type of safeguard that can be used across a wide range of machinery. However, there are two types		

of B standards: **Type B1 standards** for particular safety aspects and **Type B2 standards** for safeguards.		
IEC 60204	B1	
IEC 62061:2024 (International)	B1	Safety of machinery – Functional safety of safety-related control systems
ISO 14118:2017	B1	Safety of machinery – Prevention of unexpected start-up
ISO 4414:2010	B1	Pneumatic Fluid Power - General rules and safety requirements for systems and their components
ISO 4413:2010	B1	Hydraulic Fluid Power – General rules and safety requirements for systems and their components
IEC 60204-1	B1	Safety of machinery – Part 1: General requirements
ISO 13849-1:2015/2023	B1	Safety of Machinery – Safety-related parts of control systems. Part 1: General Principles for Design
ISO 13849-2:2012	B1	Safety of machinery – Safety-related parts of control systems Part 2: Validation
ISO 13854	B1	Minimum gaps to avoid crushing parts of the human body
ISO 13850:2015	B2	Safety of machinery – Emergency stop function – Principles for design
ISO 13851:2019	B2	Safety of machinery – Two-hand control devices – Principles for design and selection
ISO 13855:2010	B2	Safety of machinery - Positioning of safeguards with respect to approach speeds of parts of the human body
ISO 13857:2019	B1	Safety of machinery – Safety distances to prevent hazard zones being reached by upper and lower limbs)
ISO 14118:2000		Safety of machinery – Prevention of unexpected start-up
ISO 14120:2015	B2	Safety of machinery – Guards – General requirements for the design and construction of fixed and movable guards.
EN ISO 14119:2013	B2	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection.
EN 953	B2	Fixed Guards
Type C standards are machine safety standards that detail the safety requirements for a particular machine or group of machines.		
ISO 16092-3	C	Hydraulic presses
ISO 10472	C	Safety requirements for industrial laundry machinery
ISO 10218	C	Safety requirements for industrial robots
EN 13128	C	Safety requirements for machine tools
EN 415 10:2014	C	Safety of packaging machines

References

Commonly Used Statistics. Occupational Safety and Health Administration. (2023). https://www.osha.gov/

Kidman, M. Ph.D.(2020). Safety over Industrial Communication Networks. https://www.linkedin.com/pulse/safety-over-industrial-communiction-networks-dr-martin-kidman-phd/

TASK FORCE PARTICIPATION

Functional Safety Working Group

The following people served on the working group with primary responsibility for the writing, editing, and review of this document.

- Brian Tritle, IFP Motion Solutions, Chair
- Pavan Kumar, Ajax Engineering
- Cory Geers, BDI
- Frank Latino, Festo
- Ben Holter, HUSCO
- Chris Kolbe, HYDAC
- Josh Scarbrough, IFP Motion Solutions
- Dave Geiger, Moog
- Denise Husenica, NFPA
- Linda Caron, Parker Hannifin
- Chadwick Conte, Peninsular Cylinder Company
- Jay Dalal, ROSS Controls
- Chris Vandermeer, Scanreco
- Manohar Kutre, THM Fluid Technik

Technology Task Force, Industrial Applications

The following people participated in at least one of the meetings where the concept for this document was discussed and/or early drafts were reviewed.

- A. W. Chesterton, Ajay Aripirala
- Afton Chemical Corporation, Brian Rhode
- Anfield Industries, Ada Leung
- B&B Management Labs, Dan Bagley
- Barksdale Control Products, Anhadveer Khokar
- Barksdale Control Products, Dhanraj Shelke
- Barksdale Control Products, Dipanshi Batra
- Bosch Rexroth Corporation, Jon Frey
- Bucher Hydraulics, David Stevenson
- Bucher Hydraulics, Edgar Torres
- Bucher Hydraulics, Jason Yu
- Bucher Hydraulics, Jessica Horn
- Bucher Hydraulics, Mazharul Hoque
- Bucher Hydraulics, Steve Miller

- CNH Industrial, Deepak Kadamanahalli
- Crown Equipment, Sharvari Divey-Teall
- Curry Fluid Power, Phil Sorrentino
- Daman Products, Dominic Catanzarite
- Danfoss, Anant Jain
- Danfoss, Mike Betz
- Danfoss, Sandeep Pawar
- Elevat, Adam Livesay
- Evonik, Mark Petit
- Fluid System Components, Harley Quarnstrom
- Fluid System Components, Logan Turgeon
- FORCE America, Matt Loeffler
- Gefran, Ron Akers
- Hallite Seals, Chuck White
- HED, Chad Repp
- HED, Matthew Via
- HED, Paul Ludwig
- Hengst, Michael Daker
- Hengst, Tracy Long
- HYDAC, Marcus Herrera
- Hydraforce, Russ Schneidewind
- Hydraforce, Travis Schmidt
- Hydro-Gear, David Shier
- Hydrotech, Charles Schreiner
- Hyster-Yale Group, Narendra Gupta
- Hyundai, Dylan Sladek
- Hyundai America Technical Center (HATCI), John Suh
- IFP Motion Solutions, Adam Vogts
- Innovative Hydraulics, David Tetzlaff
- Iowa State University, Brian Steward
- John Deere, Paul Marvin
- KersTech, Inc., Michael Miles
- Komatsu, Congmin Niu
- Komatsu, Doug Seeger
- Komatsu, Roy Schmoutz
- Kraft Fluid Systems Inc., Patrick Green
- Ligon Hydraulics, Keith Houser
- Marzocchi Pumps, Greg Shtrahman
- Milwaukee School of Engineering, Paul Michael

- Motion, Dave Mayer
- Muncie Power Products, Inc., Alan Jones
- National Fluid Power Association, Eric Lanke
- National Fluid Power Association, Pete Alles
- Norgren, Jared Amundson
- Nott Company, DJ O'Konek
- Oilgear, John Tudor
- OPS Controls, Brandon Flick
- OPS Controls, Michael Brooks
- Parker Hannifin, Howard Zhang
- Parker Hannifin, Mark Schoessler
- QP Hydraulics, Jesse Arias
- QP Hydraulics, Matt Ogden
- Thermal Transfer Products, Tom Grotophorst
- Tigercat, Joey Kadziolka
- Trelleborg Sealing Solutions, Mike Magsam
- Trelleborg Sealing Solutions, Stephen Garden
- Trelleborg Sealing Solutions, Trevor Combs
- VIS Hydraulics, Diego Guidi
- VIS Hydraulics, Rick Guidish
- VIS Hydraulics, Sara Baldoni
- Walvoil Fluid Power, Enrico Baiocchi
- WTWH Media, Mary Gannon

© 2024, National Fluid Power Association