Guidance to Machinery Manufacturers for Consideration of Related IT-Security (Cyber Security) Aspects

ANSI-Accredited Standards Developer and Secretariat:

A Technical Report prepared by
B11 Standards, Inc.
POB 690905
Houston, TX 77269
www.b11standards.org
and

Registered with ANSI: **07 APRIL 2019**

AMERICAN NATIONAL STANDARDS / TECHNICAL REPORTS

The B11 Series of American National Standards and Technical Reports are developed through a consensus process. Consensus is established when substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward resolution. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While B11 Standards, Inc. administers the process and establishes procedures to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards or guidelines.

American National Standards and Technical Reports are promulgated through ANSI for voluntary use; their existence does not in any respect preclude anyone, whether they have approved the standards/technical reports or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to these documents. However, users, distributors, regulatory bodies, certification agencies and others concerned may apply American National Standards or Technical Reports as mandatory requirements in commerce and industry.

The American National Standards Institute does not develop standards or technical reports and will in no circumstances give an interpretation of an American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the Secretariat (B11 Standards, Inc.).

B11 STANDARDS, INC. MAKES NO WARRANTY, EITHER EXPRESSED OR IMPLIED AS TO THE FITNESS OF MERCHANTABILITY OR ACCURACY OF THE INFORMATION CONTAINED WITHIN THIS TECHNICAL REPORT, AND DISCLAIMS AND MAKES NO WARRANTY THAT THE INFORMATION IN THIS DOCUMENT WILL FULFILL ANY OF YOUR PARTICULAR PURPOSES OR NEEDS. B11 Standards, Inc. disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of, application or reliance on this document. B11 Standards, Inc. does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this technical report, nor does it take any position with respect to the validity of any patent rights asserted in connection with the items which are mentioned in or are the subject of this document, and B11 Standards, Inc. disclaims liability for the infringement of any patent resulting from the use of or reliance on this document. Users of this document are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

In publishing or making this document available, B11 Standards, Inc. is not undertaking to render professional or other services for or on behalf of any person or entity, nor is B11 Standards, Inc. undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment, or as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

B11 Standards, Inc. has no power, nor does it undertake to police or enforce conformance to the requirements of this document. B11 Standards, Inc. does not certify, test or inspect products, designs, or installations for safety or health purposes. Any certification or other statement of conformance to any health or safety-related information in this document shall not be attributable to B11 Standards, Inc. and is solely the responsibility of the certifier or maker of the statement.

Published by: B11 Standards, Inc.
POB 690905, Houston, Texas 77269-0905, USA

Contents Page

FOREWORD

The B11 Standards Development Committee for Machinery Safety is the ANSI-accredited consensus body authorized to decide and vote on the adoption of relevant ISO International Standards as American National Standards through B11 Standards, Inc. which is the ANSI-accredited Standards Developing Organization (SDO). At its July 2018 semi-annual meeting, the B11 Standards Committee approved the decision to adopt this ISO Technical Report (ISO/TR 22100-4) as an American Technical Report with the new designation of B11.TR9. The technical content between the ISO and B11 Technical Reports is virtually identical. ISO/TR 22100-4 is the fourth part in a series of relational ISO Technical Reports to ISO 12100:2010.

The base standard (ISO 12100:2010) originally began as EN 292 and EN 1050 in the early-mid 1990s, which then became ISO 12100 parts 1 and 2 on general safety/risk reduction/validation, and ISO 14121 on risk assessment. These standards all underwent very minor (primarily editorial) revisions until the U.S. assumed convenorship of ISO/TC199 /WG5 and convinved the TC there was no reason the three could not be combined into a single standard, as evidenced by several different ANSI standards that had done just that, as well as the TC realization that it was difficult to harmonize and coordinate a concurrent revision of the three separate parts. The TC agreed to combine the three ISO standards into a single document, but editorially *only* resulting in ISO 12100:2010; no technical changes were allowed. Some years after that, the TC agreed to authorize WG5 to create several different ISO TRs on different aspects of the relationships to ISO12100; they are as follows:

ISO/TR 22100-1:2015 – *How ISO 12100 relates to type-B and type-C standards;*
ISO/TR 22100-2:2013 – *How ISO 12100 relates to ISO 13849-1;*
ISO/TR 22100-3:2016 – *Implementation of ergonomic principles in safety standards;*
ISO/TR 22100-4:2018 – *Guidance to machinery manufacturers for consideration of related IT-security aspects.*

Publication of this Technical Report has been approved by the Accredited Standards Developer – B11 Standards, Inc. This document is registered as a Technical Report in the ANSI B11 series of publications according to the *Procedures for the Registration of Technical Reports with ANSI*. This document is not an American National Standard and the material contained herein is informative, not normative in nature. Suggestions for improvement of this technical report are welcomed. They should be sent to: *B11 Standards, Inc., POB 60905, Houston TX 77269*. This Technical Report was developed by Work Group 5 of ISO Technical Committee 199, processed and submitted for approval by the B11 Accredited Standards Committee on Safety Standards for Machines. At the time this Technical Report was registered, the ANSI B11 Standards Development Committee was composed of the following members:

Organizations Represented	Name of Representative (Delegate / Alternate)	
AHT Insurance	John Russell, PE, CSP, CPE	George Forrester
Aluminum Extruders Council	Mel Mitchell, CSP	Bradley Wyatt, CSP
American Society of Safety Professionals	Bruce Main, PE, CSP	Anne Mathias, PE (Vice-Chair)
Association For Manufacturing Technology	Russ Bensman	Alan Metelsky, FS Eng (Chair)
The Boeing Company	Don Nelson	Steven Thomas
Bridgestone	Kenji Furukawa	Joey Hinson
Bureau Veritas	David Natalizia, CPE	
Canadian Standards Association	Andrea Holbeche, P.Eng	Walter Veugen
Deere & Co.	Tony Beeth	Scott Winter
Euchner	Mark Witherspoon	Henry Toal
Exponent	Stephen Andrew, PE	Torsten Skujins
FDR Safety	Mike Taubitz	Joe Wolfsberger
General Motors Corporation	Mike Douglas	
Grantek	Jeff Winter, FS Eng	Patric Brown
Komatsu America Industries	George Schreck	James Landowski
Liberty Mutual	Stan Brubaker, CSP	Julie Thompson
MAG Automotive	Erik Carrier	Doug Watts
Metal Powder Industries Federation	Dennis Cloutier, CSP	James Adams
National Institute for Occupational Safety & Health	Richard Current, PE	
Occupational Safety & Health Administration	Ken Stevanus	James McManus
Omron Scientific Technologies Incorporated	Frank Webster	Tina Hull
Packaging Machinery Manufacturers Institute	Charles (Fred) Hayes	Tom Egan
Pilz Automation Safety, LP	Michael Beerman	Doug Sten, PhD, CSP
Plastics Industry Association	Megan Hayes	Steve Petrakis
Precision Metalforming Association	Jim Barrett, Jr. PhD	David Klotz
Presence-sensing Device Manufacturers Assoc.	Jim Kirton	Mike Carlson
Robotic Industries Association	Carole Franklin	Jeff Fryman
Rockwell Automation	Pat Barry	Michael Poynter
Safe-T-Sense	Chris Gerges	Federico Badillo
SICK, Inc.	Chris Soranno, FS Exp	Mark Nehrkorn, FS Exp
Sheet Metal & Air Cond. Contractors Nat'l. Assn.	Mike McCullion	Scott Lollar
Sub-Zero Group	Chad Pierce, CSP	James Fritz
Toyota Motor Manufacturing North America	Earl Sowders	

Overview of the ANSI B11 Series of Machinery Safety Standards

The purpose of the ANSI B11 series of machinery safety standards is to devise and propose ways to eliminate or minimize risks of the potential hazards associated with the required tasks. This can be accomplished either by an appropriate machine design or by restricting personnel or other individuals' access to hazard zones, and by devising work procedures to minimize personnel exposure to hazardous situations. This is the essence of the ANSI B11 series of safety standards. These standards recognize that zero risk does not exist and cannot be attained. However, a good faith approach to risk assessment and risk reduction should achieve an acceptable risk level.

Organization and Application of B11 Documents
The B11 standards and technical reports can be associated with the ISO "type A-B-C" structure as described immediately below, and as shown in Figure 1.

- **Type-A standards** (basis standards) give basic concepts, principles for design, and general aspects that can be applied to machinery;
- **Type-B standards** (generic safety standards) deal with one or more safety aspects or one or more types of engineering controls that can be used across a wide range of machinery:
- **Type-C standards** (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines**.**

The B11.0 standard on general safety requirements common to ANSI B11 machines is primarily a "Type -A" standard in that it applies to a broad array of machines and contains very general requirements. However, in many areas it also contains very specific requirements. B11.19, B11.20, B11.21, B11.25, B11.26, as well as the entire B11 series of Technical Reports are all typical "Type-B" documents addressing general safety elements that can be used across a wide range of machinery (such as B11.19 and B11.26) or as a standard when combining machines (B11.20). The B11 series of Technical Reports are informative documents that may be generally applied to many different machines, and as such would fall into the "Type-B" category. The machine-specific ("Type-C") B11 standards contain detailed safety requirements for a particular machine or group of machines (such as this standard). The Type-A B11.0 and the Type-C (machine-specific) B11 standards are intended to be used concurrently by the supplier and user of machines. When a Type-C standard deviates from one or more provisions dealt with by this standard or by a Type-A standard, the Type-C standard requirement generally takes precedence. Any deviation in conforming to a requirement of any standard should be carefully evaluated and based on a documented risk assessment.

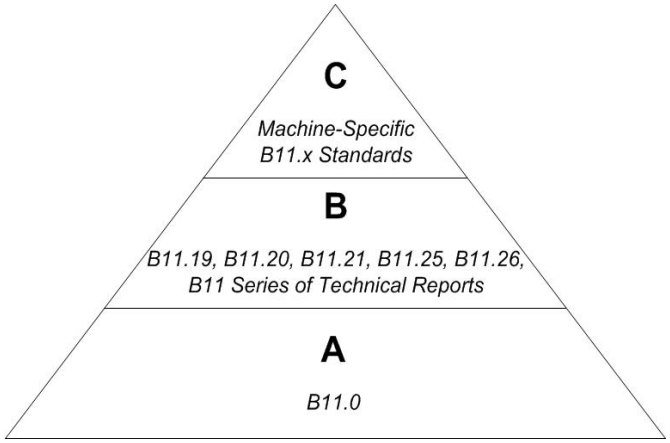

Figure 1: Organization of the B11 Series of Documents

The responsibility for reducing these risks to an acceptable level is divided between the equipment supplier, the equipment modifier, the equipment user and its operating personnel, as addressed in Figure 2 which provides the structure of a typical type-C standard and in particular, the responsibilities of and requirements for the supplier, modifier, user, and the user personnel. It is provided so the reader can better understand the responsibilities for reducing risk, since this type-B standard applies when a control system is used as a risk reduction measure. Parenthetical numbers denote the particular clause/subclause of the type-C standard.

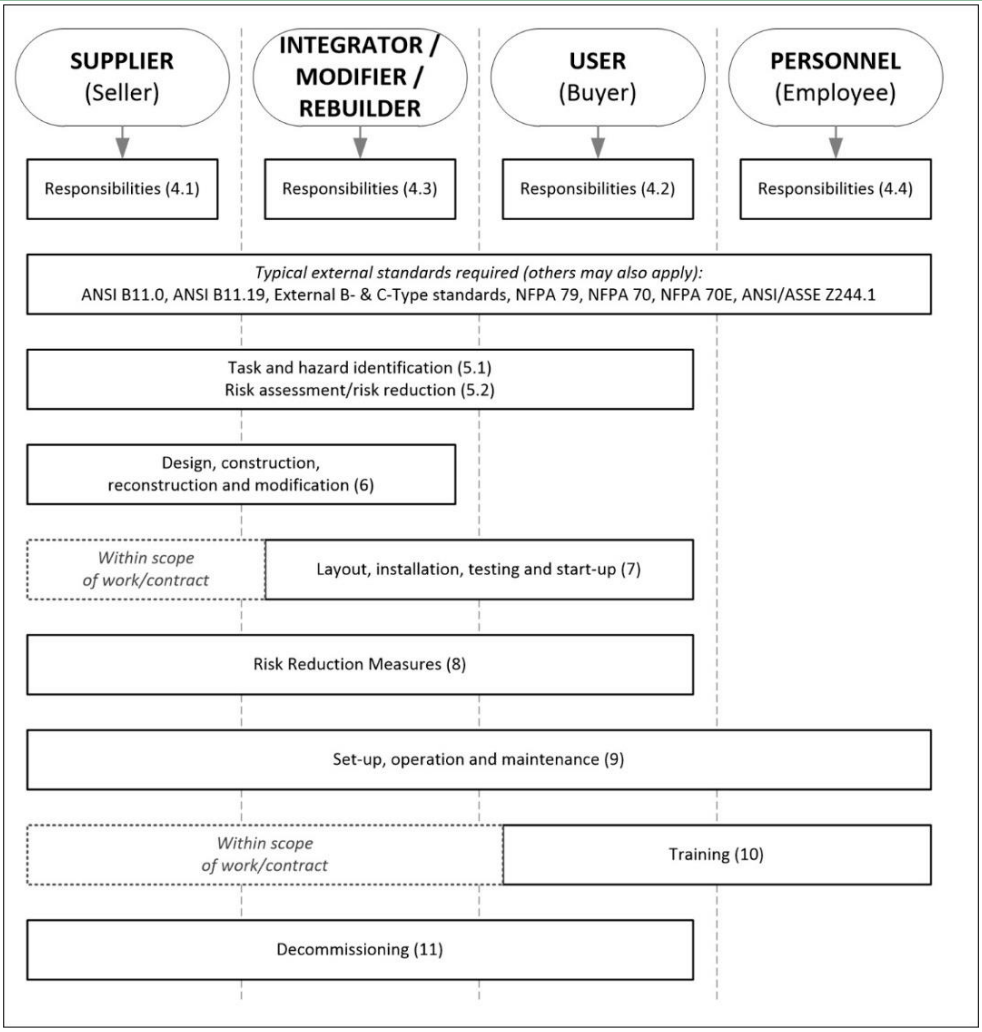

Figure 2: Typical clause layout of B11 base standards showing the various responsibilities

- **SUPPLIER: T**he early stages of a project present the greatest opportunity to determine project requirements and to anticipate and eliminate hazards and hazardous situations.
- **MODIFIER:** The entity (OEM, Supplier, or the expert) in that discipline responsible for creating or modifying the system, machinery or equipment, shall have all relevant design standards documentation. The entity shall begin by working with the end user to list all tasks to achieve an appropriate comprehensive task list base of the "context of use" for the system, machine or equipment.
- **USER:** The company representatives (can be from many disciplines) where the system, machinery or equipment will reside during its productive life. They should engage in participating or reviewing the risk assessment and what will be necessary for a final safety buy-off at the final location.
- **PERSONNEL:** The group "at risk" from any hazards or hazardous situation presented by the system, machinery, or equipment while performing their tasks to achieve the company's desired productive life. This would include at a minimum, operators, maintenance personnel for both planned and unplanned maintenance, housekeeping and safety representatives. This group would evaluate the engineering controls and administrative controls (see ANSI B11.19).

Reports on machinery safety consisted of the following documents shown in the list below. The user should check a licensed reseller such as ANSI (www.ansi.org) for the current versions of any of these documents. All archival / historical versions of the documents are available at www.b11standards.org.

List of the ANSI B11 Series of Safety Standards and Technical Reports

#	SHORT TITLE / TOPIC	YEAR	TYPE
B11.0	Safety of Machinery	2015	A
B11.1	Mechanical Power Presses	2009 (R14)	C
B11.2	Hydraulic & Pneumatic Power Presses	2013	C
B11.3	Power Press Brakes	2012	C
B11.4	Shears	2003 (R13)	C
B11.5	Ironworkers	1988 (R13)	C
B11.6	Manual Turning Machines w/ or without Auto Control	2001 (R12)	C
B11.7	Cold Headers and Cold Formers	1995 (R15)	C
B11.8	Manual Milling, Drilling, & Boring Machines	2001 (R12)	C
B11.9	Grinding Machines	2010 (R15)	C
B11.10	Sawing Machines	2003 (R15)	C
B11.11	Gear and Spline Cutting Machines	2001 (R12)	C
B11.12	Roll Forming and Roll Bending Machines	2005 (R15)	C
B11.13	Single & Multiple-Spindle Automatic Bar and Chucking Machines	1992 (R12)	C
B11.14	Coil Slitting Machines (combined into B11.18)	Withdrawn	---
B11.15	Pipe, Tube and Shape Bending Machines	2001 (R12)	C
B11.16	Powder / Metal Compacting Presses	2014	C
B11.17	Horizontal Hydraulic Extrusion Presses	2004 (R15)	C
B11.18	Machines Processing or Slitting Coiled or Non-Coiled Metal	2006 (R12)	C
B11.19	Performance Requirements for Risk Reduction Measures (Safeguarding)	2010	B
B11.20	Integration of Machinery into Systems	2017	B
B11.21	Machine Tools Using Lasers for Processing Materials	2006 (R12)	B
B11.22	Turning Centers and Automatic Numerically Controlled Turning Machines	2002 (R12)	C
B11.23	Machining Centers & CNC Milling, Drilling & Boring Machines	2002 (R12)	C
B11.24	Transfer Machines	2002 (R12)	C
B11.25	Large Machines	2015	B
B11.26	Functional Safety for Equipment	2018	B
B11.27	Electro-Discharge Machines	201x	C
B11.TR1	Ergonomics	2016	B
B11.TR2	Metal Working Fluids	1997 (R16)	B
B11.TR3	Risk Assessment / Risk Reduction	2000 (R15)	B
B11.TR4	Selection of Programmable Electronic Systems (PES/PLC)	2004 (R15)	B
B11.TR5	Noise Measurement	2006	B
B11.TR6	Safety Control Systems for Machines	2010	B
B11.TR7	Integration of Lean and Safety	2007 (R17)	B
B11.TR8	Inspection and Maintenance of Risk Reduction Measures	201x	B
B11.TR9	Guidance on Machinery Safety Cybersecurity Aspects	2019	B
ANSI/ISO 12100	Safety of machinery (identical adoption of ISO 12100-2010)	2012	A

Introduction

Internet, digital services and technology are important enablers for smart manufacturing, which is one part of the internet of things (IoT) (see ISO/IEC 20924). For the manufacturing environment, the foundations are vertical networking and horizontal integration across the entire value chain, convergence of design, ordering, delivery and manufacturing capabilities. This results in the transformation of conventional value chains and the emergence of new business models. Smart products based on smart manufacturing know many details on how they were made, their performance and how they are being used. The physical product is linked to its digital representation, and the digital content depends on life-cycle phases. Implementing smart manufacturing creates an efficient and highly responsive package by leveraging existing manufacturing systems, as well as technological and economic potential. However, smart manufacturing increases the vulnerability of machinery to IT-security threats.

Smart manufacturing leads to the emergence of dynamic, real-time optimized and self-organizing value chains. An appropriate regulatory framework is therefore necessary, as well as standardized interfaces and harmonized business processes. Smart manufacturing is characterized by:

a) increased product flexibility;
b) new intrinsic built-in product properties;
c) flexible work organization;
d) changed scale (up to a lot size 1) and location of manufacturing.

For smart manufacturing, the description of the network infrastructure needs to be further expanded to enable privacy, self-configuration and ease of use. Therefore, there is a need for fast, available, robust and secure communication networks.

The primary purpose of this document is to address aspects on safety of machinery that can be affected by IT-security attacks related to the direct or remote access to, and manipulation of, a safety-related control system(s) by persons for intentional abuse (unintended uses). IT-security attacks are increasingly becoming a potential threat to the safety of machinery. Although intentional abuse falls outside the scope of ISO 12100 (or ANSI B11.0) and the (safety-related) risk assessment process, it is not unreasonable for machinery manufacturers to consider such threats.

Current technologies enable machinery to be monitored and/or improved regarding their performance remotely by adjusting parameters without having to be on-site at the machine. This ability provides considerable benefits as machinery can be kept operating without the downtime and associated costs of a field service person making a service call. However, this same capability to adjust machine parameters to improve performance lends itself to the possibility for persons with nefarious or criminal intent to make adjustments that can put workers and others at risk of harm. For example, speeds or forces can be adjusted to dangerous levels, temperatures in food processing can be lowered below a kill-step level resulting in food contamination, or error codes or messages can be erased or falsified.

Human error can have little relation to IT-security in its strict sense. Those unintentional influences (reasonably foreseeable human error when adjusting parameters of the machine or its control system) are already covered within the normal (safety-related) risk assessment and the resulting inherently safe design of the control system (see ISO 12100:2010, 6.2.11.1).

Guidance to Machinery Manufacturers for Consideration of Related IT-Security (Cyber Security) Aspects

1 Scope

This document gives machine manufacturers guidance on potential security aspects in relation to safety of machinery when putting a machine into service or placing it on the market for the first time. It provides essential information to identify and address IT-security threats which can influence the safety of machinery.

This document gives guidance but does not provide detailed specifications on how to address IT-security aspects which can influence the safety of machinery. This document does not address the bypass or defeat of risk reduction measures through physical manipulation.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ANSI / ISO 12100:2012 (ISO 12100:2010 IDT), *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ANSI B11.0-2019, *Safety of machinery*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100 and the following apply.
ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at http://www.electropedia.org/

3.1 antivirus tool: Software used to detect malicious code, prevent it from infecting a system, and remove malicious code that has infected the system.

3.2 attack: An attempt to gain unauthorized access to system services, resources, or information. [Source: CNSSI-4009, modified — "…, or an attempt to compromise system integrity, availability, or confidentiality" has been deleted at the end of the definition.]

3.3 authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [Source: NIST SP 800-53]

3.4 authorization: Right or permission that is granted to a system entity to access a system resource. [Source: RFC 4949]

3.5 confidentiality: Preserving authorized restrictions on, and preventing *unauthorized access* (3.18) to, information.

3.6 encryption: Transformation of data into a form that conceals the data's original meaning to prevent it from being known or used.

Note: If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.

3.7 firewall: Software that restricts data communication traffic between two connected networks.

Note: It is also common to name specific hardware in which the software runs a firewall.

