Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Setting the Standard for Automation™

TECHNICAL REPORT

ISA-TR84.00.09-2017

Cybersecurity Related to the Functional Safety Lifecycle

Approved 10 April 2017

ISA-TR84.00.09-2017, Cybersecurity Related to the Functional Safety Lifecycle

ISBN: 978-1-945541-49-0

ISA
67 Alexander Drive
P. O. Box 12277
Research Triangle Park, NC 27709 USA

PREFACE

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-TR84.00.09-2017.

This document has been prepared as part of the service of ISA, the International Society of Automation, toward a goal of uniformity in the field of instrumentation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA; 67 Alexander Drive; P. O. Box 12277; Research Triangle Park, NC 27709; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

It is the policy of ISA to encourage and welcome the participation of all concerned individuals and interests in the development of ISA standards, recommended practices and technical reports. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA or of any of the standards, recommended practices and technical reports that ISA develops.

CAUTION — ISA DOES NOT TAKE ANY POSITION WITH RESPECT TO THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS ASSERTED IN CONNECTION WITH THIS DOCUMENT, AND ISA DISCLAIMS LIABILITY FOR THE INFRINGEMENT OF ANY PATENT RESULTING FROM THE USE OF THIS DOCUMENT. USERS ARE ADVISED THAT DETERMINATION OF THE VALIDITY OF ANY PATENT RIGHTS, AND THE RISK OF INFRINGEMENT OF SUCH RIGHTS, IS ENTIRELY THEIR OWN RESPONSIBILITY.

PURSUANT TO ISA'S PATENT POLICY, ONE OR MORE PATENT HOLDERS OR PATENT APPLICANTS MAY HAVE DISCLOSED PATENTS THAT COULD BE INFRINGED BY USE OF THIS DOCUMENT AND EXECUTED A LETTER OF ASSURANCE COMMITTING TO THE GRANTING OF A LICENSE ON A WORLDWIDE, NONDISCRIMINATORY BASIS, WITH A FAIR AND REASONABLE ROYALTY RATE AND FAIR AND REASONABLE TERMS AND CONDITIONS. FOR MORE INFORMATION ON SUCH DISCLOSURES AND LETTERS OF ASSURANCE, CONTACT ISA OR VISIT WWW.ISA.ORG/STANDARDSPATENTS.

OTHER PATENTS OR PATENT CLAIMS MAY EXIST FOR WHICH A DISCLOSURE OR LETTER OF ASSURANCE HAS NOT BEEN RECEIVED. ISA IS NOT RESPONSIBLE FOR IDENTIFYING PATENTS OR PATENT APPLICATIONS FOR WHICH A LICENSE MAY BE REQUIRED, FOR CONDUCTING INQUIRIES INTO THE LEGAL VALIDITY OR SCOPE OF PATENTS, OR DETERMINING WHETHER ANY LICENSING TERMS OR CONDITIONS PROVIDED IN CONNECTION WITH SUBMISSION OF A LETTER OF ASSURANCE, IF ANY, OR IN ANY LICENSING AGREEMENTS ARE REASONABLE OR NON-DISCRIMINATORY.

ISA REQUESTS THAT ANYONE REVIEWING THIS DOCUMENT WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE DOCUMENT NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER.

ADDITIONALLY, THE USE OF THIS DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR PROCESS EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS TECHNICAL REPORT SHOULD EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER SHOULD ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS TECHNICAL REPORT.

ISA (www.isa.org) is a nonprofit professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern

automation and control systems used across industry and critical infrastructure. Founded in 1945, ISA develops widely used global standards; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its 40,000 members and 400,000 customers around the world.

ISA owns Automation.com, a leading online publisher of automation-related content, and is the founding sponsor of The Automation Federation (www.automationfederation.org), an association of non-profit organizations serving as "The Voice of Automation." Through a wholly owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (www.isasecure.org) and the ISA Wireless Compliance Institute (www.isa100wci.org).

The following members of ISA84 Working Group 9 served as active contributors in the development of this technical report revision:

NAME	AFFILIATION
Harold W Thomas (Hal), Chair	exida
Kevin Arnold	Phillips 66
David Bennett	Phillips 66
Rahul Bhojani	BP
John D. Day	Air Products and Chemicals
David Deibert	Air Products and Chemicals
Andrew Feben	Eigen Ltd
David Gunter	Air Products and Chemicals
Eric Hopp	Rockwell Automation
Kevin Klein	Chevron ETC
Vic Maggioli	Feltronics Corp
Marcelo Mollicone	SYM PCS
Nagappan Muthiah	Wood Group
Eric Persson	exida
Jeff Potter	Emerson
Richard Roberts	Suncor Energy
Eloise Roche	SIS-TECH Solutions
Byron Schneidau	BP Pipelines & Logistics
Herman Storey	Herman Storey Consulting
Paulo Vergara	Zavior Consulting

The following members of ISA84 and ISA99 are acknowledged for their peer review of this technical report revision:

NAME	AFFILIATION
John Ayuk	Wood Group
Marcio Baeta	SIS-TECH Solutions
Marc Baque	Total
Brad Bonnette	Wood Group
Bob Brown	Consultate LLC
Libero Corvaglia	SIS-TECH Solutions
Eric Cosman	OIT Concepts
John Cusimano	aeSolutions
David Dalke	Wood Group
Koji Demachi	Yokogawa
Harvindar Gambhir	Reliance JIO
James Gilsinn	Kenexis Consulting
Paul Gruhn	aeSolutions

Rahul Gupta	Wood Group
James Harris	UOP
Jean-Pierre Hauet	KB Intelligence
William Hearn	SIS-TECH Solutions
Dennis Holstein	OPUS Consulting Group
Eric Jandik	Chevron ETC
Kevin Klein	Chevron ETC
Scott Nielsen	Wood Group
Khar Peng Ong	Chevron ETC
Nicholas Sands	DuPont
Angela Summers	SIS-TECH Solutions, LP
Joseph Weiss	Applied Control Solutions
Dennis Zetterberg	Chevron

The following served as members of the Standards and Practices Board and approved the document on 10 April 2017:

NAME	AFFILIATION
M. Wilkins, Vice President	Yokogawa
D. Bartusiak	ExxonMobil Research & Engineering
D. Brandl	BR&L Consulting
P. Brett	Honeywell Inc.
E. Cosman	OIT Concepts, LLC
D. Dunn	Phillips 66
J. Federlein	Federlein & Assoc. LLC
B. Fitzpatrick	Wood Group Mustang
J. Gilsinn	Kenexis Consulting
J.-P. Hauet	KB Intelligence
D. Lee	UCDS
G. Lehmann	AECOM
K.-P. Lindner	Endress+Hauser Process Solutions AG
T. McAvinew	Consultant
V. Mezzano	Fluor Corp.
C. Monchinski	Automated Control Concepts Inc.
G. Nasby	City of Guelph Water Services
M. Nixon	Emerson Process Management
D. Reed	Rockwell Automation
N. Sands	DuPont
H. Sasajima	Fieldcomm Group Inc. Asia-Pacific
H. Storey	Herman Storey Consulting
K. Unger	Consultant
I. Verhappen	Industrial Automation Networks
D. Visnich	Burns & McDonnell
W. Weidman	Consultant
J. Weiss	Applied Control Solutions LLC
D. Zetterberg	Chevron Energy

This page intentionally left blank.

CONTENTS

FOREWORD

This technical report is part of a series of standards and technical reports that address the issue of safety instrumented system security. It has been developed by Working Group 9 of the ISA84 committee in cooperation with the ISA99 committee.

This technical report provides guidance on how to implement cybersecurity within the IEC-61511 and ISA-84.00.01-2004 lifecycle. This is the second issue of this technical report. Members of the ISA84 and ISA99 committees contributed to this effort.

Readers of this technical report are asked to send comments on the content and suggestions for coverage in future revisions to the following email address:

standards@isa.org

This page intentionally left blank.

0 Introduction

0.1 Executive summary

Safety Instrumented Systems (SIS) represent one layer of protection that may be implemented in order to reduce risk within the process industry. Other layers of protection may consist of instrumented systems performing alarms, interlocks, permissive functions or controls using devices within the basic process control system (BPCS), as well as non-instrumented systems such as relief devices, check valves, etc. Traditional process hazard analysis (PHA), in the past, has generally excluded the potential for cyber related attacks to cause process safety incidents. Given that targeted attacks on industrial automation and control systems (IACS), including the systems executing safety controls, alarms, and interlocks (SCAI), have occurred and these systems are increasingly being connected to other business systems, cyber vulnerabilities represent a significant potential for common mode failure. As a result, it is necessary in today's world to include cyber risk in the overall PHA.

Without addressing cybersecurity throughout the entire safety lifecycle, it is not possible to adequately understand the relative independence and integrity of the various layers of protection that involve instrumented systems, including the SIS.

The underlying premise of this document is to help the reader understand how to integrate cybersecurity into the safety lifecycle. Guidance is provided on how to implement, operate and maintain safety controls, alarms, and interlocks (SCAI) in a secure manner. As part of this integration, it should also be understood that achieving higher security levels may result in less convenience to the end user. Addressing cybersecurity and functional safety of the SCAI systems within the IACS requires that this document serve both the ISA84 series of standards as well as the ANSI/ISA-62443 series of standards.

0.2 Integrated lifecycle

The work process to ensure security of the IACS should account for the entire functional safety lifecycle, including risk assessment, design, manufacture, factory acceptance testing (FAT), site acceptance testing (SAT), commissioning, operation, maintenance, the ongoing mechanical integrity program, modification and decommissioning. As part of the safety lifecycle (SLC), as documented in ISA-84.00.01-2004 (see Figure 1), security should be addressed at all phases.

Figure 2 seeks to show, at a high level, how functional safety and cybersecurity could integrate within the overall safety lifecycle, starting with a new process plant at the initial scope stage and continuing throughout all phases of the lifecycle. Although the NIST (National Institute of Standards and Technology) framework is not the only one that can be selected, it was used as a quality assurance tool when developing this technical report to help ensure any potential gaps were minimized. The overall result is an example of a single process safety management process, incorporating IEC-61511, ISA-84.00.01, ANSI/ISA-84.91.01, Draft ISA-84.91.03, and the applicable ANSI/ISA-62443 series of standards. Additional lifecycle details are provided throughout this technical report. It is recognized that the lifecycle figures in this technical report are an interpretation and that there may be other appropriate means to address the IEC 61511 lifecycle with respect to functional safety and cybersecurity. It should also be recognized that different functional disciplines will of necessity be responsible for different aspects of the lifecycle. This technical report is mainly targeted at process control, process safety, and operations personnel so that the impact of cybersecurity regards process safety can be better understood as well as to help understand the necessary relationship with information technology (IT) personnel. While not directly targeted at IT personnel, they may find this document useful regards the relationship between safety and cybersecurity in the process industry.

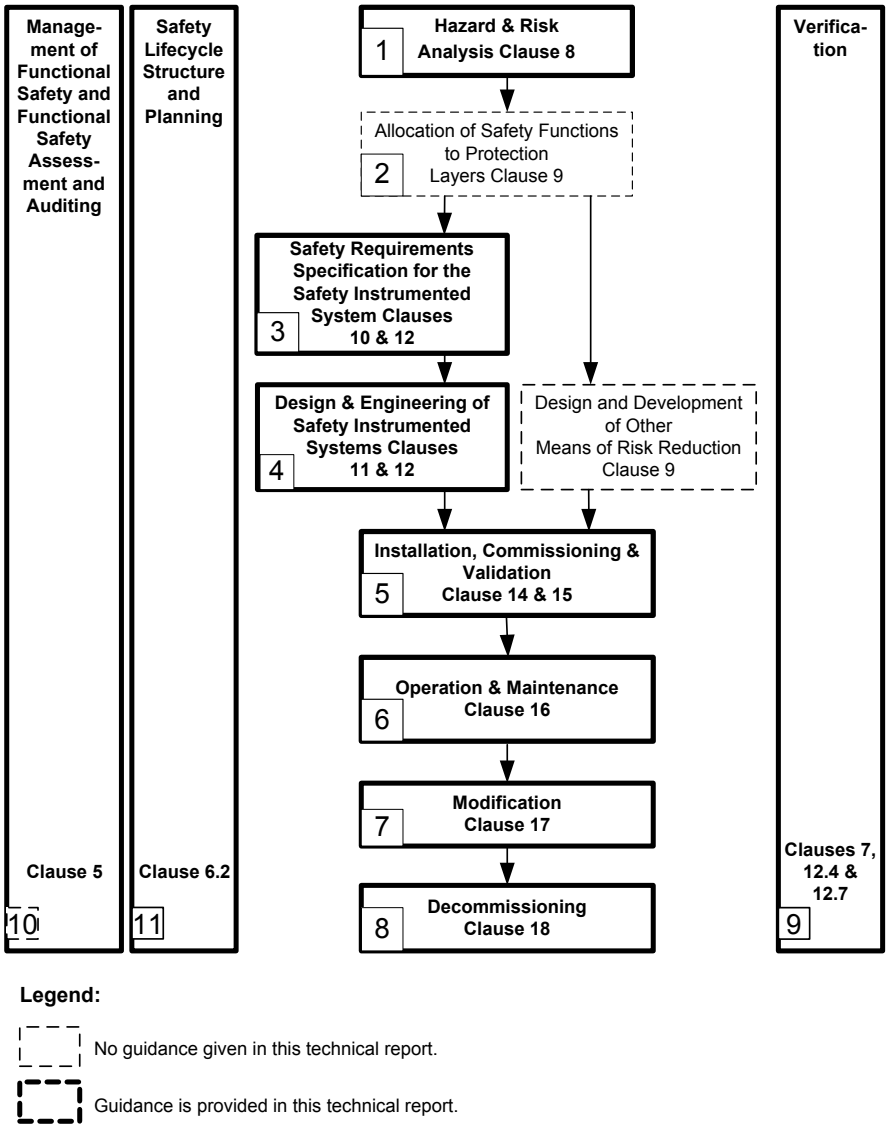

Figure 1 – Graphical representation of the safety lifecycle

NOTE The clause numbers within the elements of Figure 1 above refer to clauses in ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod).

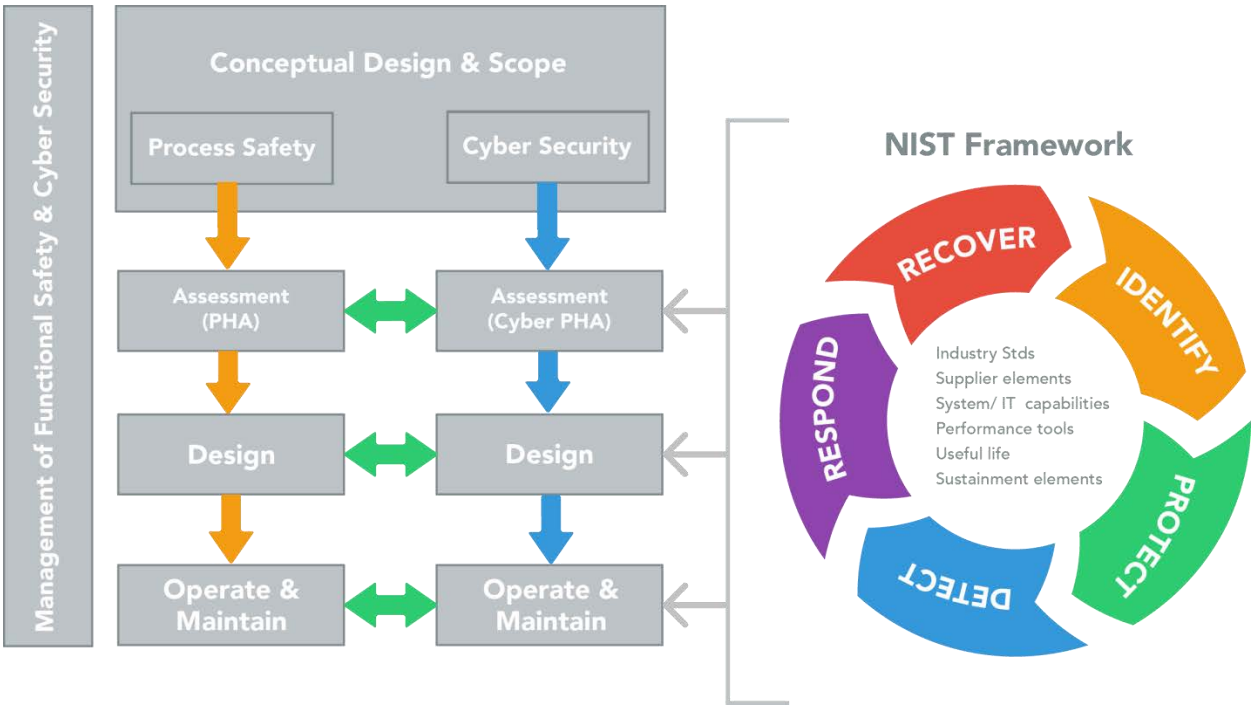

Figure 2 – Cybersecurity lifecycle integrated with process safety management

0.3 Safety versus cybersecurity considerations

Traditionally, different disciplines have dealt with safety and cybersecurity with not much overlap. In today's world, neither functional safety nor information technology are independent of one another. It is important for both functional areas to understand the differences as well as the overlaps so that jointly, appropriate best practices can be employed and any culture of "Us versus Them" can evolve into "We." As such, it is important to understand the typical differences in how the IT professional views their requirements versus how a process control engineer views theirs.

Common differences between IT and IACS that typically exist today are included in Table 1:

Table 1 – Current snapshot comparison of IT versus IACS disciplines

	IT	IACS
Response time performance	Limited knowledge of process response time requirements	Should be real time relative to the process dynamics, e.g., milli-seconds, seconds.
Availability	Occasional outages tolerated	Outages not tolerable
Data confidentiality	Data privacy is critical	Data privacy generally less critical
Data integrity / Configuration and/or software integrity	Critical	Critical
Technology lifecycle	3 – 5 years	20+ years
Outsourcing	Common	Less common
Patching	Timely	Less frequent / As required
Anti-virus	Common	Old legacy systems may not be supported. Potential undesirable side-effects with real-time process control software.
Cybersecurity awareness	Good	Poor / Improving
Process safety risk awareness	Poor	Good
Risk assessment granularity	Coarse (e.g., all control loops)	Fine (e.g., individual loop)
Changes	Easy to implement	Difficult to implement
Safety integrity awareness	Poor	Good
PHA revalidation	No explicit requirement	No greater than 5 years

Successful cybersecurity programs consider the differences between traditional IT roles and IACS to develop a cohesive program that delivers on the needs of both organizations.

Table 2 below contrasts cybersecurity versus functional safety as a function of the safety lifecycle.

Table 2 – Comparison of functional safety and IT cybersecurity in IACS using a lifecycle approach [21]

Lifecycle phase		Functional safety	IACS cybersecurity
Risk analysis	Target of evaluation	- Equipment under control (EUC)	- System under Consideration (SuC)
	Failure likelihood	- Random failures due to operational and environmental stresses - Systematic failures due to errors during safety lifecycle	- Threats: internal, external or combination - Vulnerabilities due to • component or system design flaws • making non-validated changes • not following cybersecurity practices and procedures • Threats exploiting vulnerabilities leads to failure
	Consequence severity	- Impact on environment, health and safety of personnel and the general public	- Loss of availability and/or data integrity has direct impact, and loss of confidentiality has indirect impact on functional safety
	Risk categorization	- Based on likelihood and severity; risk may be quantified	- Based on likelihood and severity; risk is currently qualitative - Risk categorization for every cybersecurity requirement - Multi-dimensional problem - Assigned to zone with target SL for each zone/conduit
	Risk mitigation measures	- Relies on independent protection layers concept - Safeguards reduce likelihood of consequence evaluated - Identifies integrity requirements for safeguards; for SIF assigns target SIL	- Relies on cybersecurity countermeasures within zones, conduits interconnecting zones, and defense in depth concept - Countermeasures reduce likelihood - Identifies requirements for countermeasures to meet the zone target SL for each threat vector
Implementation of measures		- Safety manual for components - Quantitative SIL verification for SIF	- Cybersecurity manual for components - Verification through different levels of testing for target SL
Operation and maintenance		- Restrict access to IACS components to competent personnel with necessary access privileges - Periodic testing of measures - Demand rate and component failures to be monitored - Awareness and training	- Restrict access to IACS components to competent personnel with necessary access privileges - Periodic testing of measures - Frequent reviews to identify new vulnerabilities and take appropriate action, if necessary - Awareness and training - Cyber risk reassessment after each software or hardware change
Management system		- Defines requirements for competency, training, verification, testing, audit, MOC, and documentation	- Defines requirements for competency, training, verification, testing, audit, MOC, and documentation

This page intentionally left blank.

1 Scope

This document is intended to address and provide guidance on integrating the cybersecurity lifecycle with the safety lifecycle as they relate to Safety Controls, Alarms, and Interlocks (SCAI), inclusive of Safety Instrumented Systems (SIS). This scope includes the work processes and countermeasures used to reduce the risk involved due to cybersecurity threats to the Industrial Automation and Control System (IACS) network.

This scope provides recommendations to ensure SCAI are adequately secured due to the potential for cyber attacks that can act like common mode failures that initiate a hazardous demand and also prevent instrumented protection functions, including the SIS, from performing their intended purpose. The scope is intended to address cybersecurity from both external and internal threats. Although not directly within the scope, enterprise networks, business networks and process information networks (demilitarized zones) that represent a threat vector to the SCAI systems, or contain countermeasures that reduce the risk to the SCAI systems from external cyber threats, are included.

The scope does not address physical plant protection (for example, fences, bollards, and grounding) that has the intent of preventing unauthorized entry into the plant so as to prevent theft, vandalism, or physical damage, but does address physical access issues related to cybersecurity of the IACS (12.4 of this technical report). SCAI systems that are constructed exclusively of electrical/electronic components without digital signal technology are not vulnerable to cybersecurity attacks, and these technologies are not discussed in this technical report.

2 References

The following documents are important for understanding this technical report. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies. For information on obtaining ISA standards and technical reports, visit: www.isa.org/findstandards

In addition, readers should be aware of the ongoing development of additional standards in the ANSI/ISA-62443 series, *Security for Industrial Automation and Control Systems*, listed in the Bibliography. For an update on the status of these standards, visit https://www.isa.org/isa99/ .

- IEC-61508-2010, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*
- IEC-61511-1, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*.
- ISA-84.00.01-Part 1 (IEC 61511-1), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*.
- ANSI/ISA-84.91.01-2012, *Identification and Mechanical Integrity of Safety Controls, Alarms, and Interlocks in the Process Industry*, 2012.