



IADC

CYBERSECURITY GUIDE FOR THE UPSTREAM ENERGY SECTOR

IADC CYBERSECURITY COMMITTEE

Version 03.03.2026



I. Version History		Date
Prepared by	Kris Hardwick, IADC Cybersecurity Committee Technical Writer/Project Manager	07.17.2025
Reviewed by	Jim Rocco, IADC Cybersecurity Committee Liaison	08.15.2025
Reviewed by	IADC Cybersecurity Committee	09.30.2025
Reviewed by	IADC Cybersecurity Committee	10.24.2025
Reviewed by	IADC Cybersecurity Committee	12.12.2025
Final Draft Prepared by	Kris Hardwick, IADC Cybersecurity Committee Technical Writer/Project Manager	01.28.2026
Reviewed by	IADC Cybersecurity Committee	01.10.2026
Approved by	IADC Cybersecurity Committee	03.03.2026

Copyright © 2026 International Association of Drilling Contractor (IADC), Houston, Texas USA. All rights reserved. No part of this publication may be reproduced in any form without the prior written permission of the publisher.

International Association of Drilling Contractors
3657 Briarpark Dr. Suite 200
Houston, Texas 77042
USA

Cover illustration uses elements of photos by Kindel Media: <https://www.pexels.com/photo/female-engineer-in-reflective-vest-8487396> and Los Muertos Crew: <https://www.pexels.com/photo/maintenance-guy-in-yellow-hard-hat-8853506>.

IADC Cybersecurity Guide for the Upstream Energy Sector

INTERNATIONAL ASSOCIATION OF DRILLING CONTRACTORS CYBERSECURITY COMMITTEE

VERSION DRAFT 03.03.2026

II. Foreword

IADC (the International Association of Drilling Contractors) was founded in 1940 by a group of visionaries who believed that drilling contractors needed a collective voice to advocate for their interests within the upstream energy industry. IADC members work to improve health, safety, and environmental practices, advance drilling and completion technology, and champion projects that influence safe, efficient, and environmentally sound drilling operations worldwide.

This document, "IADC Cybersecurity Guide for the Upstream Energy Industry 2026" was developed by the IADC Cybersecurity Committee.

This guide was written to support a revision of

1. *IADC Guidelines for Baseline Cybersecurity for Drilling Assets January 2018*
2. *IADC Guidelines for Assessing and Managing Cybersecurity Risks to Drilling Assets 2016*

Although IADC believes the information presented is accurate as of the date of publication, IADC does not warrant the completeness, reliability, or accuracy of this information. Any action a reader takes in using this information is at the user's own risk, and IADC, its committees, subcommittees, and contractors will not be liable for losses or damages.

III. Acknowledgements

Heartfelt thanks and appreciation goes to the members of the IADC Cybersecurity Committee leaders, their companies, and the Committee members for their diligent and patient time and attention-to-detail in support of this guide and questionnaire. Many thanks also to IADC for sponsoring this project and to the upstream industry and its related associations' partners.

Officers

Co-Chairs

Onshore:

Darren Ruhr, *Precision Drilling*

Offshore:

Robert Roell, *Valaris*

Onshore:

Ming Yeo, *Nabors*

Offshore:

Dominic Keller, *Transocean*

Project Team

Staff Liaison:

Jim Rocco, *IADC*

Technical Writer/Project Manager:

Kris Hardwick, *IADC*

Scribe:

Angel Caballero, *Transocean*

Senior IT Coordinator:

Veronica Spencer, *IADC*

Corporate Services Coordinator:

Leslie Winters, *IADC*

IADC Cybersecurity Guide for the Upstream Energy Sector

CONTENTS

I. Version History	i	8. Interviews	5
II. Foreword	ii	8.1 Team Lead Responsibilities	5
III. Acknowledgements	ii	8.2 Interview Style	5
Officers	ii	8.3 Review	5
Co-Chairs	ii	8.4 Followup and Closeout	5
Project Team	ii	9. Next Steps	5
1. Introduction	1	10. Results Evaluation	6
2. Scope of the Guide	1	11. Digital and Automation Changing Roles	6
2.1 Relevant Roles	1	12. Cybersecurity and HSE Collaboration	6
2.2 Purdue Model Diagram	1	Cybersecurity SME Strengths	6
3. References	2	HSE SME Strengths	7
4. Terms and Definitions	2	12.1 Bowtie Risk Assessments for Upstream Energy Operations	7
5. Benefits	2	12.2 How Does a Bow-Tie Diagram Work?	8
6. Registering vs Conforming to a Standard	2	12.3 What is Bow-Tie Analysis?	8
6.1 Certification	3	12.4 When is Bow-Tie Analysis Used?	8
6.2 Conformance	3	12.5 Compensating Controls as a Prevention Barrier	8
7. How to Use the Cybersecurity Questionnaire	3	12.6 Benefits of Bow-Tie Analysis	8
7.1 Evidence	3	12.7 Bow-Tie Diagrams with Network Topology for Cybersecurity Risk Analysis	8
7.2 Planning	4	13. Disaster Recovery and Incident Response Plans	9
7.3 Schedule	4	14. After Action Review (AAR)	9
7.4 Records Repository and Retention Guidance	4	15. Bibliography	10
7.5 Scope of the Questionnaire	4	16. Appendix: Questionnaire	10
7.6 Notification	4		
7.7 Communication	5		
7.8 Team Selection	5		

1. Introduction

The use of this guide is to supply the basics of evaluating upstream energy IT and OT processes and performance with an established set of criteria. It is a voluntary process. The information is useful to provide an evaluation of conformance with a set of defined processes, standards, and recommended practices which support cybersecurity.

This document provides guidance for using methods and standards to evaluate upstream cybersecurity risks of energy assets, business, operational processes, and people. These are the organizational components which support upstream energy operations. This document contains information intended for exercising two main elements to account for an organization's IT and OT risk prevention and mitigation objectives: 1) a questionnaire for evaluating information and operation security; and 2) a list of references to guide the responses to each question.

The questions have been organized by category.

2. Scope of the Guide

This guide is intended for use by operators, contractors, service providers, and vendors whose work includes the upstream energy sector. This guide highlights the standards which support establishing, implementing, maintaining, and continually improving upon an informational and operational (IT and OT) management systems within the context of an upstream organization.

This guide is not intended to supersede any policies, procedures, and practices from enterprise protocols but are designed to complement current existing practices. The IT questions in the questionnaire are limited in scope to IT processes related to OT operations and **do not include enterprise-level IT practices**.

2.1 Relevant Roles

The guide is most applicable to those tasked with completing the questionnaire and associated corrective actions and priorities and to include:

- IT professionals
- OT professionals

Other upstream roles which may gain insight from this guide and the questionnaire include:

- Asset owners
- IT and OT service providers
- IT and OT product suppliers
- Cybersecurity auditors, assessors, consultants, and other professionals
- Regulatory agencies
- Cybersecurity advocates and educators
- Industrial technicians
- Other upstream cybersecurity stakeholders

2.2 Purdue Model Diagram

The Purdue Reference Model (PRM) is a framework that organizes industrial control systems into distinct layers which separate OT from IT. These layers are illustrated in this model comprising five levels.

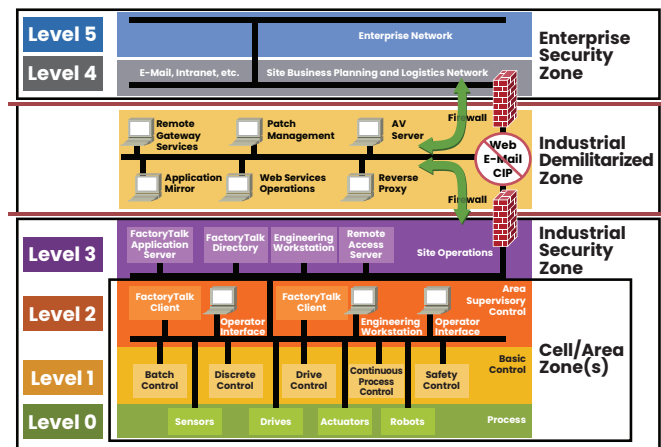


Figure 1: "Purdue Model of Computer Integrated Manufacturing" (Provided by NIST)

- **Level 0: Cell and Area:** contains sensors, devices, actuators, and robots which perform basic industrial automation and control system processes.
- **Level 1: Process Control:** communicate with the Level 0 devices and may include programmable logic controllers (PLCs), remote telemetry units (RTUs), or a basic controller known as a distributed control system (DCS).
- **Level 2: Supervisory:** communicate with PLCs and RTUs in Level 1. In some cases, Level 2 communicates with the site or enterprise (Level 4 and Level 5) systems and applications.
- **Level 3: Site-level and Industrial Perimeter Network:** communicate with the production zone and share data with the enterprise (Level 4 and Level 5) systems and applications.

- **Levels 4 and 5: Business and Enterprise**

Networks: has centralized IT systems and functions. The IT organization directly manages the services, systems and applications at these levels.

3. References

Utilizing the most current references is recommended. It is expected that the references which helped to inform the development of this guide will become obsolete over time as updated editions are made. The following references are acknowledged in support of this guide:

- ISA/IEC 62443-2-1-2024 *Industrial Communication Networks – Network and system security*
- ISO/IEC 27000:2022 *Information Security, cybersecurity, and privacy protection – Information security management systems – Requirements*

4. Terms and Definitions

For the purposes of this guide, the terms and definitions supplied in the current versions of the following standards apply.

- ISO/IEC 27000:2018 *Information technology – Security techniques – Information security management systems – Overview and vocabulary*
- ISA/IEC 62443-1-1-2007 *Security for Industrial Automation and Control Systems – Part 1-1: Terminology, Concepts and Models*

5. Benefits

The questionnaire derived by IADC for the evaluation of upstream operations cyber risk profile is informed by international IT, OT, and industry standards and best practices. The IADC questionnaire provides a number of benefits. These include:

- **Resilient company culture:** facilitates a thorough and inclusive “top-down”

organizational awareness with a primary aim towards promoting responsive and adaptive methodologies that meet upstream cyber risk challenges.

- **Enhanced risk management:** elicits awareness of the need to identify organizational frameworks that actively support security risk management.
- **Facilitates effective compliance considerations for regulators:** identifies critical functional concerns that may inform compliance measures to effectively address bespoke risk profiles; intended to promote use of recognized international instruments and best practices to optimize execution of the organization’s performance-based mitigation protocols.
- **Incident prevention & response effectiveness:** encourages attention towards supporting processes that reduce the likelihood and impact of costly cyber breaches.
- **Increased trust:** demonstrate support for business partner relationships/supply-chain interoperability to promote reliable/robust business and operational value-chain processes.

6. Registering vs Conforming to a Standard

This guide is designed to provide performance-oriented support for organizations in the upstream energy industry with a fundamental focus on objectives that facilitate continual improvement of cybersecurity risk prevention and mitigation strategies.

The use of the terms conformance and compliance may be found to be mistakenly used when discussing adherence to a prescribed/recognized criteria set and/or levels of performance. Proper attribution in the use of these terms is critical to ensure consistent expectations across stakeholders and processes for addressing cyber risk. When identifying an expectation of *conformance* to a criteria set and/or levels of performance, it is implied that practices and/or protocols are generally intended to meet the stated objective of a referenced benchmark such as a standard or other recognized industry performance set.

Conversely, the stated level of performance requiring *compliance* is a higher-order expectation that requires explicit satisfaction of a law, statute, or regulation. In short, a company *complies* with regulation/law and *conforms* to a standard.

6.1 Certification

When a company chooses to register to a standard, the steps toward registration (also known as certification) include successfully completing a certification audit or certification assessment by an independent certified auditor or certified assessor depending on the standard. The certificate is issued by the auditor agency which is the certification body. Companies may also choose to perform internal audits which demonstrate conformance with a standard but not proceed to register (certify) to the standard.

6.2 Conformance

Conformance refers to meeting the provisions of a particular standard. A company may elect to follow a standard without going through the process of registering and being certified to the standard. A company may choose to conduct internal audits using their own personnel to determine their conformance with the standard.

7. How to Use the Cybersecurity Questionnaire

The questionnaire contains two question tabs – one tab with IT questions and one tab with OT questions (both together referred to as the questionnaire). The questionnaire is designed to be used for each location and facility in an organization.

Completing the questionnaire informs the intentions for pursuit of effective work processes. The questionnaire supplies evidence for stakeholders which includes internal managers and external clients to identify best practices and areas identified for improvement.

The questionnaire supports an evaluation of plans, processes, and systems for:

- Resilience
- Conformance
- Effectiveness
- Opportunities for improvement

The questionnaire contains four tabs:

- Disclaimer
- IT questions
- OT questions
- List of references

The IT and OT question tabs contain 10 columns:

- Item number
- Question
- Evidence
- Risk level
- Corrective action priority
- Category
- Reference
- Response
- Corrective action
- Notes and comments

Responses are limited to the following:

- One (1) for yes
- Zero (0) for no
- N/A for not applicable
- Partial (0.5) for partial conformance

The question categories differ based on the tab selected, IT or OT. IT questions include the following categories:

1. Leadership
2. Planning
3. Support
4. Operation
5. Performance evaluation

OT questions include the following categories:

1. Organizational security measures
2. Configuration management
3. Network and communication security
4. Component security
5. Protection of data
6. User access control
7. Event and incident management
8. System integrity and availability

7.1 Evidence

Use one (1) to indicate a “yes” response. One (1) requires associated management system evidence such as a citation from the organization’s management system policy, procedure, standard, work instruction, or a certification, inspection result, or audit.

Use zero (0) for a “no” response. A zero (0) score indicates no action has been taken to conform.

Use a half credit (0.5) for a “partial” response. A partial response (0.5) represents partial conformance indicated by a comment describing the compensating control(s) employed as an alternative security measure or other relevant explanation.

An “N/A” will appear as N/A in the drop-down selection of the questionnaire response. The N/A selection indicates the question is not applicable and requires evidence to explain the lack of applicability.

7.2 Planning

Completing the questionnaire for each location and facility relies on support from senior organization representatives to incorporate “top-down” planning. Thoughtful planning helps ensure assets, processes, and employees are identified and included with minimal disruption.

Some responses may not change from year to year. For example, a top level organizational policy may not change for years where work instructions or procedures may change more often. The time for completing the questionnaire drops as the process becomes more efficient.

7.3 Schedule

The schedule for completing the questionnaire is at the discretion of the organization. It may be completed all at once or by category. Questions may be divided and a number completed each month, each quarter, or twice per year based on resources available.

It is recommended that the responsible managers plan and align schedules on location with designated subject matter experts (SMEs) which account for IT and OT components to obtain the information/considerations needed for completing the questionnaires.

7.4 Records Repository and Retention Guidance

It is recommended that managers follow the organization’s guidance as to repository administration of the questionnaire records and any applicable retention policies which apply including applicable legal and regulatory requirements.

Systematic documentation processes and adherence to such processes are critical for any organization to support continual improvement. Conformance is impaired without proper attention and diligence to recordation and documentation practices.

7.5 Scope of the Questionnaire

The scope of the questionnaire is limited to IT functions that directly support OT processes as well as the OT processes themselves. Enterprise-level IT processes that do not support OT operations are considered out of scope for this questionnaire.

An organization may also limit the scope of the questionnaire during planning. For example, follow-up questioning may occur more frequently for items which are identified as nonconformant and high priority. Reviewing results from the previous questionnaire for each facility and location helps establish the scope and focus areas to be included on subsequent questionnaires.

Key items to consider from past questionnaires include, but are not limited to:

- Items previously marked zero (0) or partial (0.5)
- Negative result trends that occur across a series of questionnaires
- Lingering corrective actions from previous questionnaires
- Questions which may have been skipped or not completed from the previous questionnaire

Completeness and clarity are important to establish a clear understanding between the person(s) assigned to complete the questionnaire and the personnel interviewed as part of the process.

7.6 Notification

It is helpful to set expectations for the questionnaire process. Questionnaire team members should supply the facility or location to be questioned with a notification ahead of the questionnaire process. Advanced notice markedly contributes to the quality of the feedback sought.

It is helpful to supply those identified to participate in the collection of information with a notification of not less than two weeks, or up to 30 days prior to the beginning of the questionnaire process. Include necessary communication to targeted questionnaire participants including any key elements of

information which may better elicit more complete and thorough responses from the interviewees.

7.7 Communication

For the interviewing process to be successful, ample communication between the questionnaire team and the participants to be interviewed is key. Ensure leadership endorsement is included, having an authorized questioning process will encourage the necessary “buy-in” on the part of those administering and completing the questionnaire.

7.8 Team Selection

When establishing a team, work with appropriate management to obtain the personnel and other resources necessary to complete the questionnaire. Keep in mind a focus for retaining a necessary measure of independence and objectivity while identifying personnel with the appropriate skill sets and knowledge to efficiently engage in the questionnaire process and obtain the feedback needed to determine the efficacy of the questionnaire responses.

SMEs helpful to facilitating the questionnaire process include IT, OT, QHSE, compliance specialists, document management specialists, records management specialists, and technicians. Coordination among the cross-section of SMEs required to administer the questionnaire may be necessary beforehand to ensure an effective execution of the effort.

8. Interviews

Best practices for interviewing personnel to complete the questionnaire include team lead responsibilities, maintaining focus, mindfulness of time constraints, an objective clinical approach, and looking for trends.

8.1 Team Lead Responsibilities

The team lead for the questionnaire provides the interviewee with information pertaining, but not limited to:

- An introduction
- Purpose of the questionnaire
- How responses will contribute to a necessary focus on processes, including workforce interface, but not solely directed at personnel

8.2 Interview Style

A focused interview process benefits by:

- Following the questionnaire list ensuring the questions asked match the role of the interviewee
- Keeping the language objective and neutrally oriented to avoid leading the interview or implying certain responses are preferable as positive or negative
- Avoiding providing feedback during the questioning process and focus on collection of answers to the questionnaire exercise
- Selecting the records as evidence samples and not allowing the interviewee to select the record samples

8.3 Review

Review results of the questionnaire by

- Prioritizing written answers. It may be helpful to remind interviewees that documentation is the key to a successful response
- Sample enough questionnaire feedback/ answers as within the time allotted to ensure the question is answered
- Look for trends in the interviews, collected evidence, etc.
- Look for areas in which the process flow may have broken

8.4 Followup and Closeout

To conclude the interview process, let the interviewees know when the questionnaire will be made available for review and where it will be located. Follow up with an email with this same information and thank the interviewees for their time.

Once completed for each business/operations/geographical unit as applicable, it is recommended that a questionnaire review/revisit exercise be undertaken annually. Updates and revisions should be documented when significant changes occur to business processes, equipment, or employees.

9. Next Steps

Follow your organization's management system procedures for corrective actions, next steps, and due

dates. Assigned leads from each area interviewed such as the corporate office, onshore location, offshore facility, manufacturing site, warehouse, etc. may need coordination from their leadership to follow up on outstanding items identified on the questionnaire.

The responsibilities for closing corrective actions will vary for each organization. It is necessary that the corrective action processes be explicit and clearly understood.

The questionnaire has a column for assigning priority designations to corrective actions. Corrective action priorities range from three (3) for high priority, two (2) for medium priority, one (1) for low priority. A selection of N/A for not applicable is also provided. The priorities are set internally by the organization using their own internal prioritization process.

10. Results Evaluation

The questionnaire data does not support comparison with other organizations as the raw score data is “weighted” by an organization’s bespoke matrix and unique priority selections.

It may seem helpful to engage in comparisons across organizations when evaluating raw questionnaire scoring results, however such action is strongly discouraged as erroneous deductions will result. As each organization maintains its own unique risk profile, matrix, and processes for evaluating risk, a raw score comparison between organizations consequently lacks context for evaluating any level of equivalency.

These risk management practices assist organizations when deciding on how to prioritize process efficiency through continuous improvement, system maintenance, and corrective actions that provide for the optimized application of resources.

Risk considerations that drive the formulation of organizational risk matrix frameworks are sustained, elevated, or reduced over time via the determinants that underpin the fundamental values for sustaining organizational performance. Analysis of questionnaire responses over time may indicate trends which offer value to support effective and efficient operations. These trends may be used in support of organizational objectives, targets, and goals.

11. Digital and Automation Changing Roles

As organizations continually improve, organizational structures are changing. IT/OT convergence is the integration of data management systems with industrial operations systems (OT). Objectives that drive this confluence of systems is illustrated by strategic precepts established via the evolving organizational roles taken on by the Chief Digital and Information Officers (CDIO), Chief Automation Officers (CAO), along with Chief Information Security Officers (CISO). In some organizations, IT and OT roles are merging into consolidated and integrated reporting chains under these digital and automation officers.

Many of these senior-level officer responsibilities overlap.

Where digital trust has and continues to grow in its prominence as one of the most formidable of organizational risks, the need for a cross-section of professionals to collaborate in identifying gaps has never been greater. Cybersecurity and HSE professionals are critical to meeting this challenge and are posed to provide crucial insight to building operational resilience.

12. Cybersecurity and HSE Collaboration

Cybersecurity IT, Cybersecurity OT, and Health, Safety, and Environment (HSE) professionals bring unique strengths to operations, which may be leveraged to enhance the safety and security of critical infrastructure for upstream energy operations. Their interaction may generate innovation during disaster recovery drills, enterprise risk management planning, and other strategic planning processes.

Cybersecurity and HSE professionals and SMEs (Subject Matter Experts) are critical to meeting digital transformation and resilience challenges and are critically positioned to provide crucial insight as organizations grow and change.

Cybersecurity SME Strengths:

- **Threat/Risk Identification:** expertise in identifying and analyzing potential cyber threats, including malware, phishing, and other types of cyber-attacks.

- **Vulnerability Assessment:** assess vulnerabilities to identify weaknesses in systems and networks, enabling proactive mitigation strategies.
- **Incident Response:** plan for incidents with rapid and effective responses which minimizes downtime and reduces the risk of data breaches.
- **Compliance and Governance:** support operations which are fit for purpose and comply with applicable legal and other requirements for cybersecurity. These SMEs also oversee conformance with standards for information and operating security which include ISO/IEC 27001 and ISA/IEC 62443.

HSE SME Strengths:

- **Risk Assessment:** expertise in assessing and managing physical risks, including those related to equipment, personnel, operational processes, and environmental factors.
- **Safety Management:** develop and implement safety management systems with responses supporting prevention and mitigation of accidents, injuries, and environmental incidents.
- **Emergency Response:** develop, train for, and implement emergency response plans for events

such as spills, fires, and other incidents that pose a risk to people, the environment, and assets.

- **Regulatory Compliance:** support operations that are fit for purpose and comply with applicable legal and other requirements for HSE. These SMEs oversee conformance with standards for health and safety management and risk management like ISO 45001 and ISO 31000, among other applicable HSE industry derived provisions.

By combining respective risk assessment tools, cybersecurity and HSE SMEs may work together to create a more secure and resilient critical infrastructure.

12.1 Bowtie Risk Assessments for Upstream Energy Operations

A bow-tie diagram is a risk management tool used to illustrate how critical path considerations for preventing and responding to undesirable incidents/top events could occur and what may ensue. It is a tool frequently used in the development of HSE cases for upstream energy operations. (Note: IADC also has resources for the development of HSE cases for land drilling and mobile offshore drilling units. Bow-tie diagrams may be used in the development of these cases.)

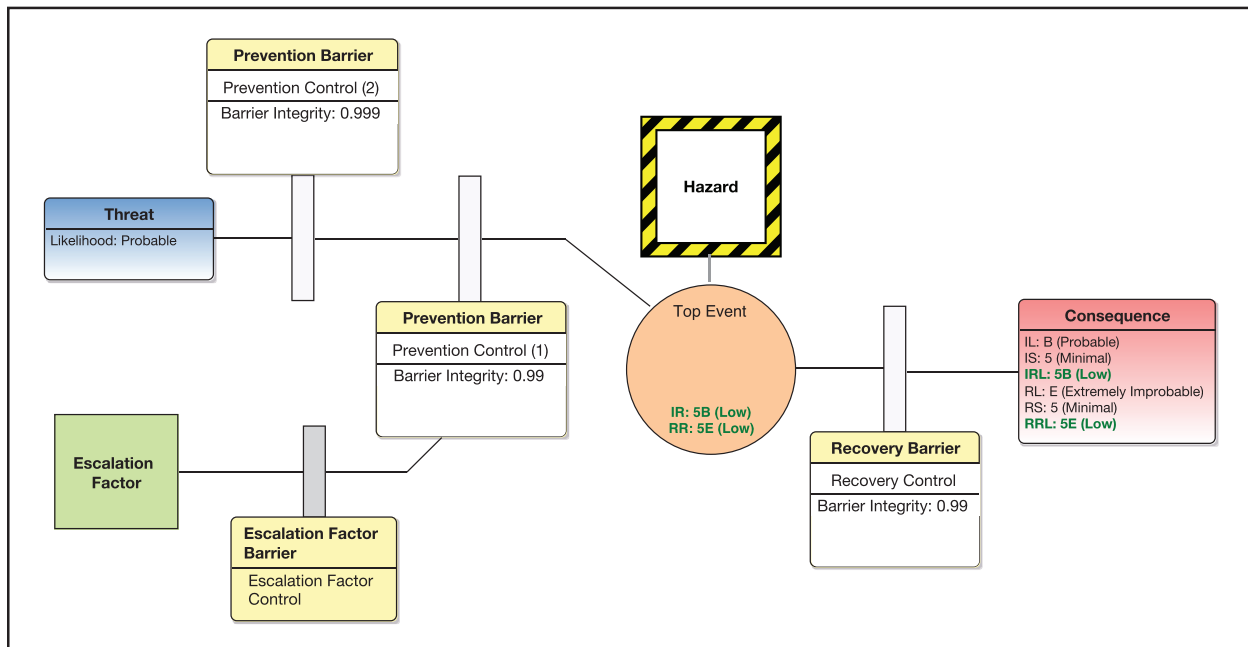


Figure 2: Bow Tie Diagram, Denney, Ewen, Ganesh Pai, and Iain Whiteside. Modeling the Safety Architecture of UAS Flight Operations. NASA.gov

A bow-tie risk assessment assists in identifying a variety of ways in which an undesirable or “top event” may be prevented (e.g. “left side” of the bowtie) via; the possible factors which increase or diminish risks, pre-incident leading indicators, and other identifiers, and the various scenarios which might precipitate or otherwise avoid an undesired top event. The “right side” of the bowtie depicts the potential consequences that may result from such a top event. This type of risk assessment combined with a resulting risk matrix helps to prioritize preventive and mitigating resources for managing risk.

12.2 How Does a Bow-Tie Diagram Work?

See the bow-tie diagram with three main parts:

- **Left side:** This identifies the possible options for preventing the top event from occurring and serves to recognize conditions which could increase the likelihood of such an event.
- **Middle (event):** This is the problem or “top event” itself.
- **Right side:** This illustrates the potential consequences of the top event and identifies response measures to be engaged upon the immediate manifestation of the undesirable top event.

12.3 What is Bow-Tie Analysis?

A bow-tie analysis is a methodology for identifying, mitigating, and responding to the risks associated with a top event. It helps organizations recognize and prioritize specific risks which, if left unchecked, will likely contribute to a top event. Once identified, the bow tie can align preventive and response measures that account for the top event risk.

12.4 When is Bow-Tie Analysis Used?

Bow-tie analysis is used to identify circumstances where a series of related or unrelated contributing factors might result in an undesired top event. This analysis is conducted to:

- Identify potential problems before they happen
- Mitigate problems that have already occurred
- Ensure controls are in place to prevent or mitigate risks.

12.5 Compensating Controls as a Prevention Barrier

Compensating controls in cybersecurity are alternative security measures implemented when primary controls may not be deployed due to technical or business constraints. These controls are designed to supply equivalent protection.

Examples of compensating controls include:

Scenario	Compensating Controls
Lack of username and password capability for equipment	Enhanced monitoring and physical security with adaptive access policies
Insufficient endpoint telemetry	Tighter network egress controls to limit data exposure

Compensating controls are essential components of a comprehensive risk management strategy for cybersecurity. As answers to certain questions may result in a zero score (0) when administering the cyber questionnaire, it is expected that descriptions of equivalent measure would be noted in the question’s corresponding comment block as an alternative control practice.

12.6 Benefits of Bow-Tie Analysis

A Bow-tie analysis is a simple and effective way to identify and show risks. It is less complex than other methods, such as fault tree analysis and event tree analysis, making it a good choice for organizations that need to quickly assess their overall risk concerns.

12.7 Bow-Tie Diagrams with Network Topology for Cybersecurity Risk Analysis

Bow-tie diagrams may be used in conjunction with network topology to improve cybersecurity risk analyses. By combining these two concepts, upstream organizations may:

- **Visualize Complex Networks:** Bow-tie diagrams may be used to visualize complex network topologies, making it easier to identify potential vulnerabilities and risks.
- **Identify Critical Assets, Processes, and People:** Mapping the network topology onto a bow-tie diagram enables organizations to identify critical assets and systems that are most vulnerable to cyber threats.

- **Prioritize Risk Mitigation:** Bow-tie diagrams can assist organizations to prioritize risk mitigation efforts by identifying the most critical control measures to prevent or mitigate risks.
- **Enhance Incident Response:** By understanding the potential consequences of a cyber-attack, organizations may develop more effective incident response plans and procedures.

13. Disaster Recovery and Incident Response Plans

A disaster recovery plan focuses on restoring IT and OT systems and business operations after a major disruption. An incident response plan outlines the specific steps necessary to undertake during a cybersecurity incident to minimize damage and manage the situation effectively. Both plans are essential for organizational resilience but address different aspects of crisis management.

The job roles and departments represented in creating and testing these plans vary from organization to organization.

These IT and OT roles may include:

- Disaster Recovery Planning
 - ♦ Disaster recovery program/process analyst coordinating recovery capabilities
 - ♦ Disaster recovery architect leading systems design to ensure application availability
 - ♦ Disaster recovery testing/recovery analyst monitoring recovery processes and ensuring compliance with recovery objectives
- Incident Response Planning
 - ♦ Incident response manager leading response efforts
 - ♦ IT security analysts monitoring and analyzing security incidents
 - ♦ OT security specialists focusing on operational technology systems

HSE professionals play a crucial role in planning by ensuring safety measures and safety instrumented systems are integrated in processes and employees are protected during defined adverse events. They help develop and implement safety protocols and training to minimize risks and support business continuity.

14. After Action Review (AAR)

During each questionnaire process, it is helpful to finish with an AAR to find out: 1) what went well; and, 2) what can be improved. Ask these two questions of each participant and use the feedback to adapt the process. The responses support efficiencies and continual improvement for the questioning process.

BIBLIOGRAPHY & APPENDIX

15. Bibliography

1. RE Mahan, JD Fluckiger, SL Clements, et al. Secure Data Transfer guidance for Industrial Control and SCADA Systems. PNNL-20776. DOE.gov
2. Denney, Ewen, Ganesh Pai, and Iain Whiteside. Modeling the Safety Architecture of UAS Flight Operations. NASA.gov
3. IADC. (2018). Guidelines for Baseline Cybersecurity for Drilling Assets.
4. IADC. (2016). Guidelines for Assessing and Managing Cybersecurity Risks to Drilling Assets.
5. IADC. (2025). HSE Case Guidelines for Land Drilling Units.
6. IADC. (2025). HSE Case Guidelines for Mobile Offshore Drilling Units..

16. Appendix: Questionnaire

The spreadsheet is available as a separate file.

Item #	Category	IT Questions	ISO/IEC 27001-2022 Reference	Evidence Management system reference(s) (module, section, pdf, etc.), independent audit, internal audit, inspections, certifications, etc.) N/A if not applicable	Letter 1 for Pass, 0 for Fail, N/A for not applicable	Risk Level from organizational risk matrix	Corrective Action (CA)	CA Priority (high-3, medium-2, low-1)	Notes and Comments
Leadership		Does the organization have disaster recovery plans for every critical IT system with OT dependencies?	5.1						
		Are disaster recovery plans for critical IT systems with OT dependencies tested with regularly?	5.1						
		Management of change (MOC) for software and hardware?	5.2						
		Access to IT systems from the OT network?	6.2						
		Access to IT systems from the OT network?	6.2						
		Protected against unauthorized access?	6.7						
		Access prevention and mitigation?	6.2						
		Copies of IT information.	6.2						
9	Planning	Are backup schedules and recovery tests determined and maintained for IT systems?	6.2						
10	Planning	Are all relevant information processing systems within the organization or security domains connected to a single reference time source?	6.2						
11	Planning	Are IT processes controlled the installed software on OT systems?	6.2						

Columns

- A. Item #
- B. Category
- C. IT Questions
- D. ISO/IEC 27001-2022 IT Reference*
- E. Evidence

*ISA/IEC 62443-2022 OT tab reference

Columns

- F. Score
- G. Risk Level
- H. Corrective Action
- I. Corrective Action Priority
- J. Notes and Comments

Tabs

- Disclaimer
- IT Questions
- OT Questions
- Upstream Cybersecurity Reference

Figure 3: IADC Cybersecurity Guide for the Upstream Energy Sector questionnaire sample view, OT tab, 7 Nov 2025.