



GUIDANCE NOTES ON

DATA INTEGRITY FOR MARINE AND OFFSHORE OPERATIONS

ABS CyberSafety™ VOLUME 3

SEPTEMBER 2016

**American Bureau of Shipping
Incorporated by Act of Legislature of
the State of New York 1862**

**© 2016 American Bureau of Shipping. All rights reserved.
ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA**

Foreword

The marine and offshore industries are integrating connected sensors, communications, storage and processing capabilities into vessels, offshore units and facilities as networking and computational power penetrates all aspects of industry operations. The “Big Data” phenomenon has emerged as a direct result of this growth, enabling development of tremendous new sources of data and information. But challenges have also emerged. Sensors and data must be trustworthy in order to support the new analytic and decision methods available for maritime industry use.

These Guidance Notes are intended to clarify the basic principles and concepts of Data Integrity for marine and offshore assets. The document is intended to help the industry realize the new benefits from data sources and data analytics systems via implementation of Data Integrity concepts. It also supports owners who are increasingly required to provide data reporting to regulatory agencies. The intended users for these Guidance Notes are cybersecurity specialists, data specialists, owners, shipyards, operators, designers, suppliers, review engineers and Surveyors.

These Guidance Notes are Volume 3 of the ABS CyberSafety™ series, and are intended to be used in conjunction with other volumes.

These Guidance Notes become effective on the first day of the month of publication.

Users are advised to check periodically on the ABS website www.eagle.org to verify that this version of these Guidance Notes is the most current.

We welcome your feedback. Comments or suggestions can be sent electronically by email to rsd@eagle.org.

Terms of Use

The information presented herein is intended solely to assist the reader in the methodologies and/or techniques discussed. These Guidance Notes do not and cannot replace the analysis and/or advice of a qualified professional. It is the responsibility of the reader to perform their own assessment and obtain professional advice. Information contained herein is considered to be pertinent at the time of publication, but may be invalidated as a result of subsequent legislations, regulations, standards, methods, and/or more updated information and the reader assumes full responsibility for compliance. This publication may not be copied or redistributed in part or in whole without prior written consent from ABS.



GUIDANCE NOTES ON

DATA INTEGRITY FOR MARINE AND OFFSHORE OPERATIONS

ABS CyberSafety™ VOLUME 3

CONTENTS

SECTION 1	General	1
1	Purpose and Scope	1
3	Data Lifecycle Management	2
5	Outline	3
7	Definitions	3
9	Abbreviations and Acronyms	4
11	References	5
11.1	ABS	5
11.3	IEEE	6
11.5	ISO	6
11.7	Other	6
	FIGURE 1 Data Source and Flow	1
	FIGURE 2 Data Lifecycle Management	2
	FIGURE 3 Guidance Notes Outline	3
SECTION 2	Data Sources	7
1	General	7
3	Raw Data Input	8
3.1	Data from Sensors (Raw/Unconditioned)	8
5	Organized Data Sources (Information)	8
5.1	Data from Databases	8
5.3	Data Traces from Identified Equipment or Systems	8
5.5	Data from Industrial Internet-of-Things (IIoT)	9
7	Conditioned Data Sources (Knowledge)	10
7.1	Data Conditioned for Machine Interpretation/Use	10
7.3	Data Conditioned for Human Interpretation/Use	10
9	Actionable Data Sources (Applied Knowledge)	10
9.1	Manual Systems Control	10
9.3	Mechanized System Control	11
9.5	Automated System Control	11
9.7	Analysis	11

FIGURE 1	Data Source Model	7
FIGURE 2	Various Sensors.....	8
FIGURE 3	Industrial Internet-of-Things (IIoT)	9
SECTION 3	Data Uses	12
1	Monitoring for Situational Awareness	12
3	Monitoring for Intervention	12
5	Monitoring by Regulatory Bodies.....	12
7	Input to Control Systems.....	12
9	Input to Analysis and Patterning	13
11	Input for Maintenance	13
SECTION 4	Data Importance	14
1	Data Integrity and Vessel Operations	14
3	Data Integrity and Business Strategy Development	14
5	Data Integrity and Integrated System Support.....	15
7	Data Integrity and Compliance Reporting.....	15
SECTION 5	Data Security	16
1	Data Types/Protocols.....	16
1.1	Serial Data.....	16
1.3	Bus Data.....	17
1.5	Streaming Data.....	18
3	Data Classification (Protection Level).....	19
5	Data At-Rest (DAR)	21
7	Data In-Motion (DIM)	22
9	Data In-Use (DIU)	22
9.1	Authorized Access Only.....	22
9.3	Penetration Protection	22
9.5	Handling Policies and Procedures	22
11	Security Measures and Controls.....	23
TABLE 1	Data Types.....	16
TABLE 2	Data Classification	20
FIGURE 1	Serial Data Illustration	17
FIGURE 2	Bus Data Illustration	18
FIGURE 3	Streaming Data Illustration.....	19
FIGURE 4	Data Classification	20
FIGURE 5	Three States of Data	21
SECTION 6	Data Integrity	24
1	General	24
1.1	Definition.....	24
1.3	Data Integrity and Data Security	25

3	Maintain Data Integrity from Traceable/Trustworthy Data Source ...	25
3.1	Origin: Supplier and Sensor Accuracy.....	25
3.3	Organization: Data Schema Transformation Accuracy.....	26
3.5	Transmission: Transfer from Point of Use Accuracy and Timing.....	27
5	Protect Data Integrity from Unintended and Intended Modification	29
5.1	Protection against Accidental Integrity Loss	29
5.3	Best Practices for Intended (Beneficial) Integrity Loss	30
5.5	Preventive Actions Against Intended (Malicious) Integrity Loss	31
7	Monitor, Verify, Validate and Measure Data Integrity	31
7.1	Data Integrity Monitoring (Overall System of Systems)	31
7.3	Verification and Validation of Data Integrity	32
7.5	Measurement of Data Integrity	33
FIGURE 1	Data Schema	26
FIGURE 2	Data and Software Relationship	27
FIGURE 3	Authentication, Authorization and Accounting	29
FIGURE 4	Notional System of Systems Onboard Vessel.....	32
FIGURE 5	Gauged System Value	34
FIGURE 6	Gauged Incident Value and Corruption Vector Index	35

This Page Intentionally Left Blank

Copyright American Bureau of Shipping
Provided by IHS
No reproduction or networking permitted without license from IHS
Full document details: ABS 252 2016

SECTION 1 General

1 Purpose and Scope

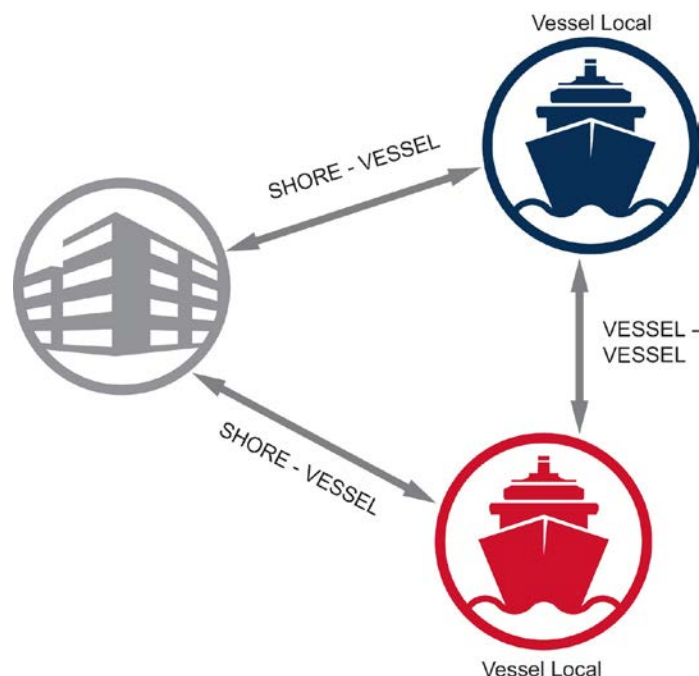
The maritime industry is beginning to use data as an asset. Historically, marine and offshore owners' and operators' major concerns were safety, asset integrity, and environmental protection. Increased presence and use of cyber-enabled data systems introduces data as both an enabler to address safety risks and as another area for concern. Vessels and their sensors generate large amounts of data from multiple sources.

Note: The general term "vessel" used throughout these Guidance Notes denotes a ship, a barge, an offshore unit or facility, or any other floating or fixed structure.

Section 1, Figure 1 illustrates nominal data sources and flows in marine and offshore operations. Three typical data sources and paths include:

- *Data Generated and Communicated Locally.* With the development of modern electronics and control technologies, extensive data can be generated and captured. The data covers a wide range of on-onboard systems and instruments, both from permanently-installed equipment and from cargo or portable equipment.
- *Data Communicated between Vessels.* The data communicated between vessels could be vessel status such as position, speed, direction, etc., but it may also include performance data, cargo carriage data, rig operational status data, or other raw or composite data sources.
- *Data Communicated between Shore and Vessel.* Operational, performance, and commercial data may come from shore-based systems as well as onboard systems. Data transferred from vessel to shore for data processing such as fleet management and benchmarking and maintenance management.

FIGURE 1
Data Source and Flow



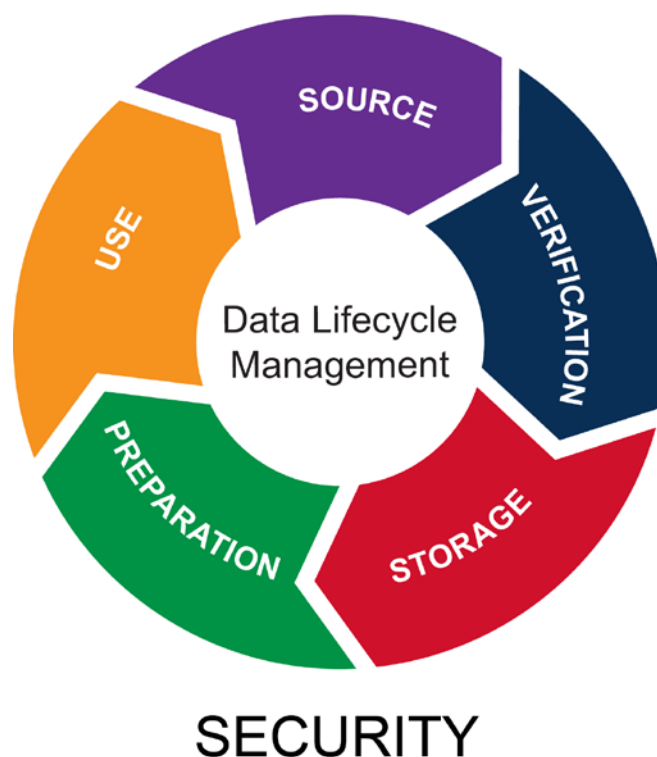
Data may be used for many functions beyond the traditional domains – for health and performance monitoring, operation, accomplishment prediction, business decision support, and others. New technical sources of data imply greater concern for data integrity and data security. Trustworthiness of data is vital to decision processes and to decision support.

These Guidance Notes are intended to clarify the concept and principles of Data Integrity for Marine and Offshore operations. The document will address data integrity as it relates to asset safety including human safety, safety of the vessel and/or threat to the environment. The objective of these Guidance Notes is to help the review engineers, surveyors, suppliers, shipyards, owners and operators to understand the application of Data Integrity in marine and offshore operations. The practices described in these Guidance Notes will improve the integrity of data.

3 Data Lifecycle Management

Data Lifecycle Management is illustrated in Section 1, Figure 2. The focus of this document is the security and integrity of the data management lifecycle. These Guidance Notes do not encompass all phases of the data lifecycle, but rather are directed at data source, data use, and data verification from the perspective of data security and data integrity.

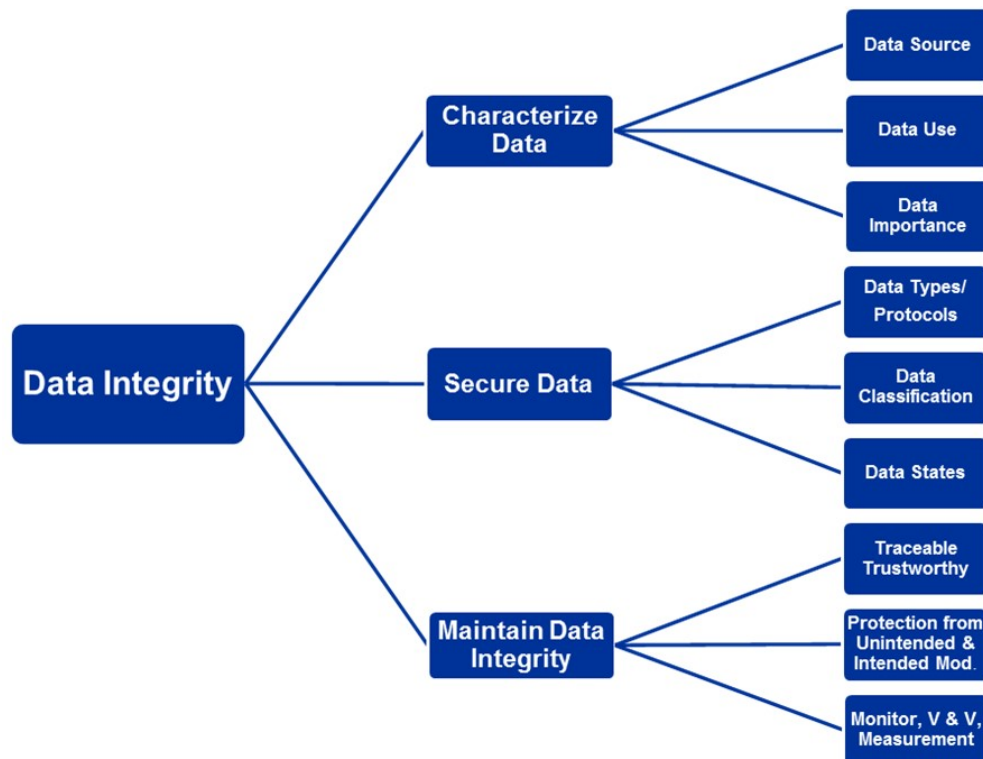
FIGURE 2
Data Lifecycle Management
INTEGRITY



5 Outline

The outline of these Guidance Notes is illustrated in Section 1, Figure 3. The outline indicates the development plan for these Guidance Notes. It shows how to characterize data, how to secure data, and how to maintain data integrity.

FIGURE 3
Guidance Notes Outline



Note: V & V: Verification and Validation

7 Definitions

The following definitions are applied to the terms used in these Guidance Notes.

Access Control: Means to ensure that access to assets is authorized and restricted based on business and security requirements. [ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary]

Bus Data: Data transmitted among multi-point networks.

CANbus: The data link layer of CAN; open transmitting of data between equipment, system controllers and data analyzers.

Chain of Custody (CoC): Chronological documentation, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.

Data At-Rest (DAR): Data that resides in storage (a device or backup medium in any form) but excludes any data frequently transferred in the network or residing in temporary memory.

Data In-Motion (DIM): Data in transit, traveling across a network or contained in a computer's RAM ready to be read, updated, or processed.

Data Integrity: Accuracy, consistency (validity), and completeness of data over its lifecycle.

Data In-Use (DIU): Data that is being processed by one or more applications.

Data Schema: Skeleton structure that represents the logical view of the entire database.

Data Security: Protecting data from the unwanted actions of unauthorized users.

Database: An organized collection of data.

Integrity Level: A number assigned by an Owner and/or Driller or Crew Organization (DCO) to a computer-based function based upon the severity of the consequence of a failure of the function. Where 0 has little consequence to 3 where the consequence of a function failure is of significant concern. For control systems refer to *ABS Guide for Integrated Software Quality Management (ISQM Guide)*.

MODBUS: A common serial communications protocol for connecting industrial electronic devices such as sensors and programmable logic controllers (PLCs).

Penetration Test: Testing that places an attack on a computer system looking for security weaknesses and potentially gaining access to the computer's features and data.

PROFIBUS: PROFIBUS (Process Field Bus) is a standard for fieldbus communication in automation technology.

Sensor: An electronic device that produces electrical, optical, or digital data derived from a physical condition or event. [IEEE 1451: IEEE Standard for a Smart Transducer Interface for Sensors and Actuators]

Serial Data: Data transmitted in serial communication.

Software Management of Change (SMOC): The process of how to manage software changes or software evolution.

Streaming Data: Sequence of message-oriented data in-sequence used to transmit or receive information in a real-time application among the networks.

System of Systems: Vessels with multiple existing standalone and networked systems.

9 Abbreviations and Acronyms

The following abbreviations and acronyms are applied to the terms used in these Guidance Notes.

AAA:	Authentication, Authorization, and Accounting
ABS:	American Bureau of Shipping
ACLs:	Access Control Lists
ARQ:	Automatic Repeat Request
BSEE:	Bureau of Safety and Environmental Enforcement
CRCs:	Cyclic Redundancy Checks
CPU:	Central Processing Unit
DAR:	Data At-Rest
DCO:	Driller or Crew Organization
DCS:	Distributed Control System
DIM:	Data In-Motion (equivalent to Data In-Transit)
DIU:	Data In-Use
DP and DPS:	Dynamic Positioning (Systems)
ECC:	Error-Correcting Code
ERP:	Enterprise Resource Planning
FDD:	Functional Description Document

<i>FEC:</i>	Forward Error Correction
<i>HMI:</i>	Human Machine Interface
<i>ICS:</i>	Industrial Control System
<i>IIoT:</i>	Industrial Internet of Things
<i>IoT:</i>	Internet of Things
<i>IP:</i>	Internet Protocol
<i>NAC:</i>	Network Access Control
<i>OEM:</i>	Original Equipment Manufacturer
<i>PC:</i>	Personal Computer
<i>PLC:</i>	Programmable Logic Controller
<i>PMS:</i>	Power Management System
<i>RAID:</i>	Redundant Array of Independent Disks
<i>RTD:</i>	Resistance Temperature Detectors
<i>SAN:</i>	Storage Area Network
<i>SCADA:</i>	Supervisory Control and Data Acquisition
<i>SIS:</i>	Safety Instrumented Systems
<i>SMOC:</i>	Software Management of Change
<i>SoS:</i>	System of Systems
<i>USB:</i>	Universal Serial Bus
<i>USCG:</i>	United States Coast Guard

11 References

11.1 ABS

ABS Guidance Notes on Application of Cybersecurity Principles to Marine and Offshore Operations – ABS CyberSafety™ Volume 1

ABS Guide for Cybersecurity Implementation for the Marine and Offshore Operations – ABS CyberSafety™ Volume 2

ABS Guide for Software Systems Verification – ABS CyberSafety™ Volume 4

ABS Guidance Notes on Software Provider Conformity Program – ABS CyberSafety™ Volume 5

ABS Guidance Notes on Equipment Condition Monitoring Techniques

ABS Guidance Notes on Failure Mode and Effects Analysis (FMEA) for Classification

ABS Guidance Notes on Risk Assessment Application for the Marine and Offshore Oil and Gas Industries

ABS Guide for Hull Condition Monitoring Systems

ABS Guide for Integrated Software Quality Management

ABS Guide for Risk Evaluations for the Classification of Marine Related Facilities

ABS Guide for Surveys Using Risk-Based Inspection for the Offshore Industry

ABS Rules for Building and Classing Steel Vessels

11.3 IEEE

IEEE 1451: *IEEE Standard for a Smart Transducer Interface for Sensors and Actuators*

IEEE 1012 – 2004, *IEEE Standard for Software Verification and Validation*

11.5 ISO

ISO/IEC 27000: *Information technology - Security techniques - Information security management systems - Overview and vocabulary*

ISO/IEC 27001: *Information technology – Security techniques - Information security management systems - Requirements*

ISO/IEC 27002: *Information technology – Security techniques - Code of practice for information security controls*

11.7 Other

National Institute for Science and Technology (NIST) *Guide to Storage Encryption Technologies for End User Devices*

SECTION 2 Data Sources

1 General

For assets in the marine and offshore industries, data processing starts with the collection of data at the sensor level. Examples of data include location, direction and speed, hull structural stresses encountered, vessel motions, engine performance, equipment status, and environmental conditions. At this stage, both structured and unstructured data is collected. Structured data is formatted for use in specific systems, such as in transaction databases. Unstructured data may be data streams, messages, documents or other data types or artifacts that may be stored by means other than in a transaction database.

Massive quantities of “random” data of sensed behavior are electronically transformed into organized data, then into knowledge, and finally into purposeful actionable knowledge. Typically, an enterprise will organize its data across many different systems and applications. Graphically, the data source model’s fundamentals are shown in Section 2, Figure 1 below.

FIGURE 1
Data Source Model

