# 11 | 2021

# CIMAC Guideline

## Monitoring Systems for Marine Hybrid Propulsion Systems

From the CIMAC WG20 System Integration

This publication is for guidance and gives an overview regarding the implementation of performance monitoring systems for Marine Hybrid Propulsion Systems. The publication and its contents have been provided for informational purposes only and is not advice on or a recommendation of any of the matters described herein. CIMAC makes no representations or warranties express or implied, regarding the accuracy, adequacy, reasonableness or completeness of the information, assumptions or analysis contained herein or in any supplemental materials, and CIMAC accepts no liability in connection therewith.

The first edition of this CIMAC Guideline Paper was approved by the members of the CIMAC WG20 'System Integration' at its meeting on September 29, 2021.

# Content

# 1 Introduction

With a focus on the internal combustion engines, the System Integration Working Group (WG20) discusses development drivers for energy efficient optimization concepts in ships or land-based applications. The final goal is to contribute to the development and promulgation of multi-source energy system design optimizations for ships and land-based power plants.

The group focuses on the implementation and optimization of such systems to provide inputs and contribute to the development of guidelines and rules with classification societies, and to cope with the state of the art in system integration design principles. Keeping an eye on trends of electrification of propulsion systems e.g., in the marine industry we realize that system integration is gaining more and more importance in order to achieve maximum customer value in an efficient and safe way. Within the wide range of possible system integration tasks WG20 will therefore concentrate on system integration of marine hybrid drives.

## 1.1 Motivation & Goal

Hybrid systems are one of the most complex energy systems to use chemical and electrical energy in parallel by using different energy conversion machinery producing mechanical and electrical output. Therefore, the use of monitoring systems is essential for ensuring optimum operation and maintenance as well as for safety and satisfying rule requirements. WG20 aims to define the core tasks of such systems as a basis for standardization requirements regarding system and component specification as well as interfacing according to common standards.

## 1.2 Terminology

### 1.2.1 Monitoring

The term monitoring covers a wide area of use cases and depending on the user’s background, raises certain expectations or implicates a set of scenarios. Figure 1 shows three of the most common use cases in the field of marine applications. Here the intention of the monitoring function is the provision of information for succeeding processes like decision making. Within the scope of this paper, the focus will be set especially on business intelligence methods for hybrid propulsion architectures.

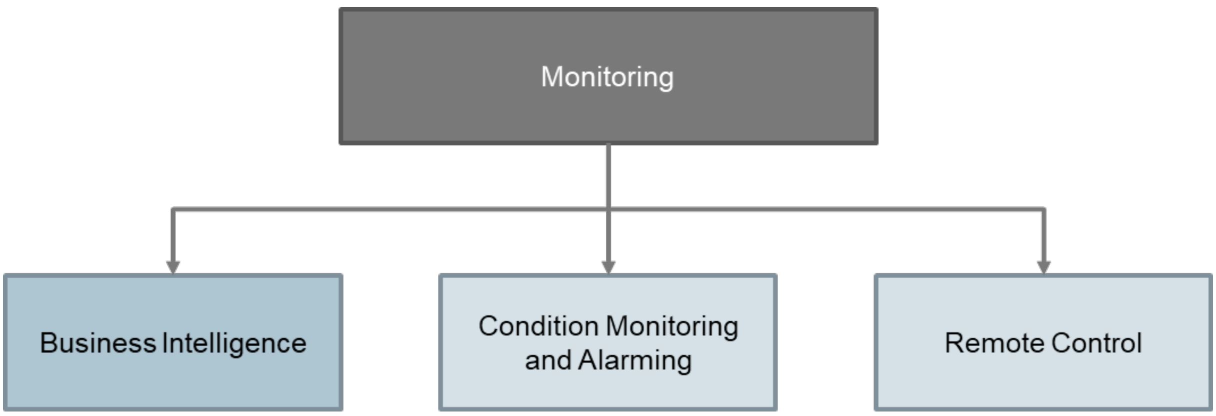


*Figure 1 Recipients of Monitoring*

The objective of monitoring is the collection of information about a process and its resources based on observations (observation task). Evaluation methods can be included to enrich or pre-process the data, e.g., by adding meta information, smoothing signals, or transforming physical to logical information. The necessary basic intelligence used is defined as “low-level” type. In subsequent modules, the provided data support the creation of recommendations and/or decision making. The combination of observation and automated evaluation of the information can be seen as an integrated monitoring system. The intelligence of the integrated system is defined as “high-level” type.

As a hybrid vessel consists of different parts, the understanding of the term “system” can be applied to a variety of levels of abstraction. Starting from individual elements that are arranged in a superordinate system, this system itself may be a sub-system of an even larger system. Figure 2 shows an exemplary architecture for a hybrid application that will be used in this document.

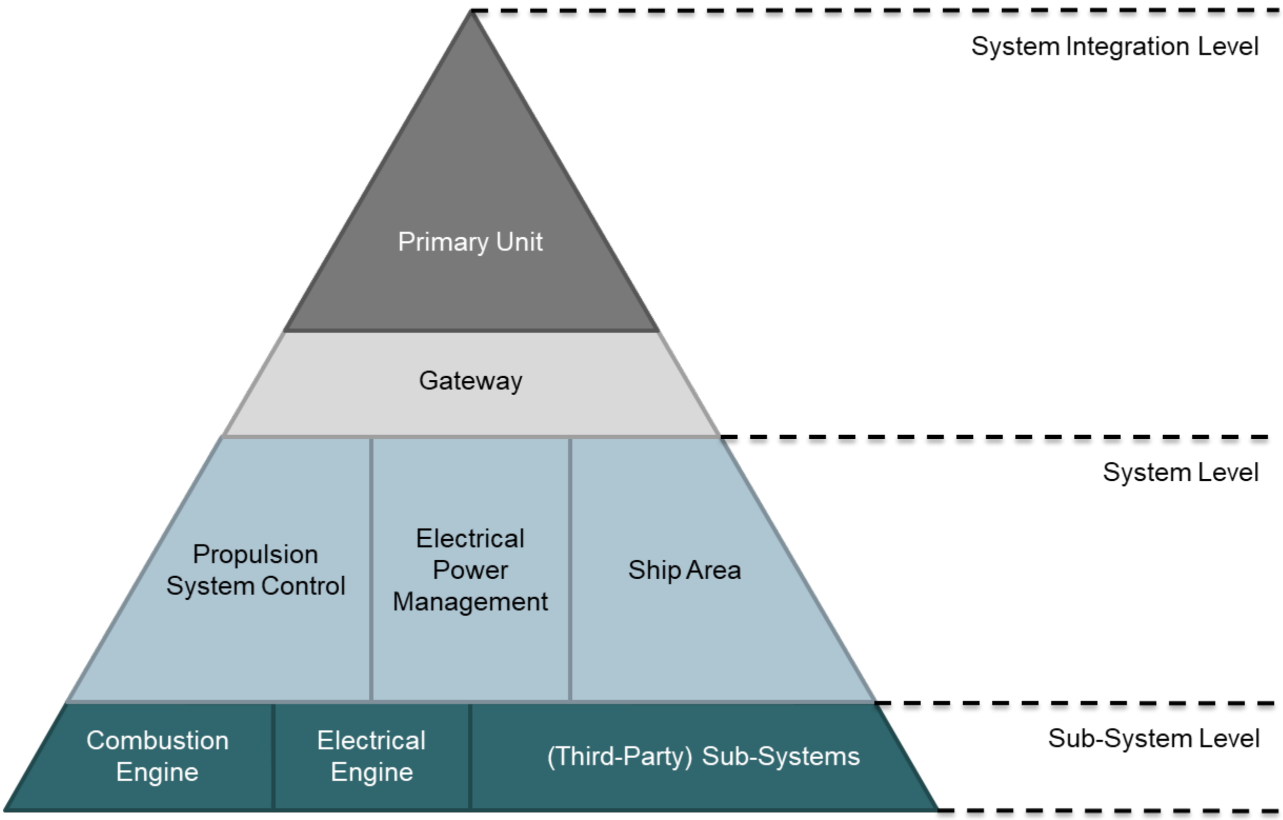


*Figure 2 Definition of System Level Architecture*

Although one would easily refer to a monitoring process as a “system”, it needs to be clarified that it can be of either real or virtual nature. As a conclusion, the term “monitoring system” (or part of monitoring system as a “module”) may indicate the existence of a standalone product, even if this definition does not explicitly demand it to be separated from the accompanied part to be monitored. Each subsystem (or component) may come along with its individual monitoring module. Whether or not provided with a high-level evaluation module, the monitoring system shall be able to connect to a higher system level. A central operation station which takes the role of the primary unit could be arranged to manage the collected data and the decisions derived from the connected sub-systems.

### 1.2.2 Data

Data according to ISO8000-8 [1], ISO/IEC 2382:2015 [2] is defined as the reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing. A data element is a unit of data for which the definition, identification, representation, and permissible values are specified by means of a set of attributes.

### 1.2.3 Information

Information, on the other hand, is knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, which have a particular meaning within a certain context [1] [2].

As traditional industries are transformed by digitalization, both data and information are increasingly considered as assets themselves, and as parts of, and prerequisites for, the operation of physical assets [3].

### 1.2.4 Data Analysis

Depending on one's personal background, the understanding of different terms in the world of data processing can drift apart. As this paper is not intended to define the basic language but to focus on the application of the process itself, a short introduction into the terminology is taken from [4].

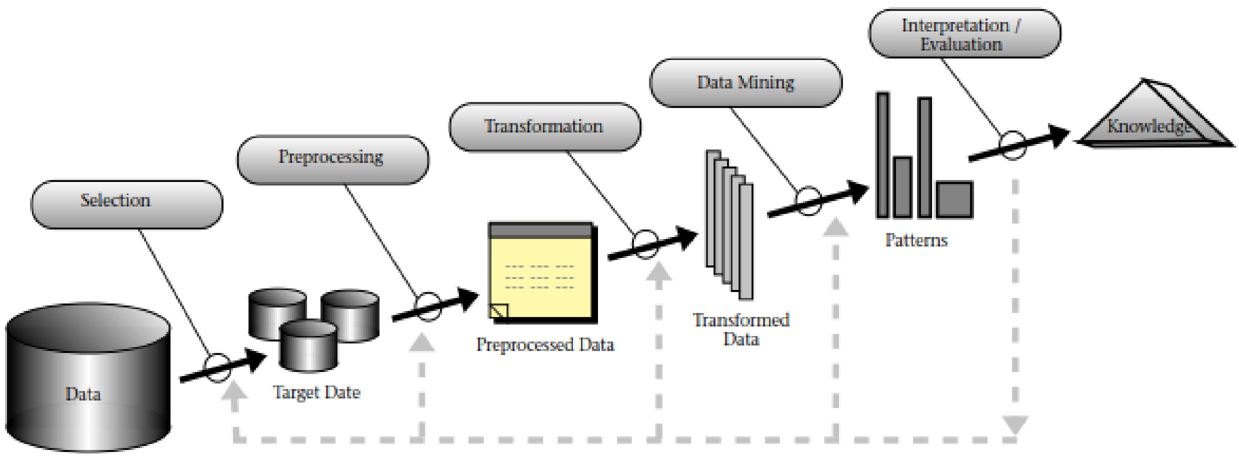


*Figure 3: An Overview of the Steps That Compose the KDD Process. [4]*

In their KDD (knowledge discovery in databases) process (see Figure 3), they describe different steps to extract the knowledge out of the sampled data. Within this paper, these steps are summarized under the term "data analysis". Data analysis is considering the selection of relevant signals (sometimes also referred as filtering of relevant signals), pre-processing and transformation of the data, data mining and interpretation/evaluation of the resulting information.

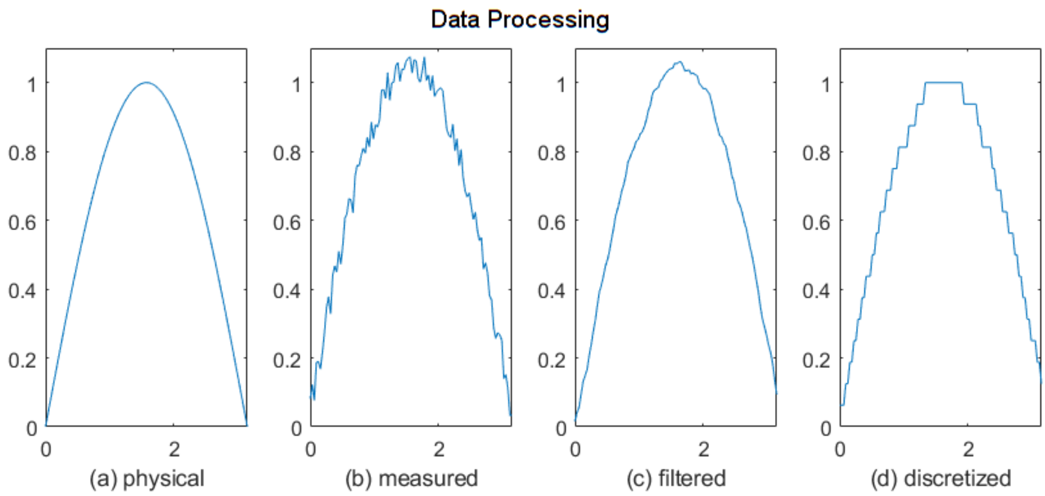


*Figure 4: Different steps in signal processing*

The data processing, which does contain both, pre-processing and transformation, is intended to make the information accessible for computer algorithms. Therefore, the signals will undertake several procedures e.g., cleaning (also referred to as signal filtering), formatting, synchronization, modulation, event detection and signal feature extraction. Figure 4 shows three exemplary steps from acquisition to digitalization of a physical signal. To generate knowledge out of the data of the monitored assets, algorithms and tailored visualisations can support the interpretation and evaluation of the asset data. Therefore, domain knowledge of the monitored system is essential in order to derive such beneficial functionalities and to draw the right conclusions out of the collected data.

## 1.3 The Purpose

Hence, the scope of a monitoring system, in addition to collecting data, is to convert these into relevant information for various stakeholders / beneficiaries. Regarding the operation of the vessels, the monitoring systems could be classified and organized based on three factors:

- **The Beneficiaries.** The operation of the vessel is in the middle of a large ecosystem which is composed of several stakeholders such as the ship owners, managers, charterers, regulatory authorities, classification society, global organizations, technical institutes, legal, insurance etc. These beneficiaries/stakeholders can be defined as ‘statutory’ and ‘non-statutory’ stakeholders. This distinguishes between those organisations and bodies that are by law required to be involved in planning, development, or operational activities and those that will be impacted directly or indirectly by it. Each part of this ecosystem needs monitoring systems to acquire information that will reduce the risk of their decisions or expose a new opportunity.
- **The Purpose.** The monitoring systems could be classified according to their main scope such as:
    - Safety, security and maintaining regulatory compliance
    - Evaluation of the operation status
    - Evaluation of the performance of systems and processes
    - Monitoring the life cycle of an asset
    - Supporting business and financial decisions

- **The Observation Level.** Monitoring systems can be implemented to monitor the operation of a vessel, a fleet of vessels, a group of vessels with common particulars, a subsystem of a vessel or even a specific asset in any part of the vessel.

Based on these three factors, the vessel monitoring systems could be indexed and classified at a first level. A useful information to understand the primary scope of each monitoring system is the evaluation of the end users' interest for the results of each system, like the one that is depicted in Table 1.

*Table 1 - Classification of monitoring systems according to end users' interest (Part 1)*

| | Level | | | | |
|---|---|---|---|---|---|
| **Beneficiaries** | Component | Subsystem | Cargo | Vessel | Group of Vessels |
| Authorities / Classification | Not at all | Rarely | Partly | Mostly | Mostly |
| Technical & Research Institutes | Rarely | Mostly | Rarely | Mostly | Mostly |
| Charterers / Brokers / Insurance Companies | Not at all | Not at all | Mostly | Mostly | Partly |
| Owners | Not at all | Not at all | Rarely | Mostly | Mostly |
| Operation Management | Not at all | Not at all | Mostly | Mostly | Partly |
| Technical Management | Partly | Mostly | Partly | Mostly | Partly |
| Captain / First Officer | Rarely | Mostly | Mostly | Mostly | Not at all |
| Chief Engineer | Mostly | Mostly | Partly | Partly | Not at all |
| Manufacturer | Mostly | Mostly | Not at all | Not at all | Mostly |
| Technical Consultants / Technical Service Providers | Mostly | Mostly | Not at all | Rarely | Partly |

| | Purpose | | | | |
|---|---|---|---|---|---|
| **Beneficiaries** | Safety / Regulation Compliance | Operation Status | Performance Evaluation | Life Cycle Monitoring | Support Business and Financial Decisions |
| Authorities / Classification | Mostly | Partly | Partly | Rarely | Partly |
| Technical & Research Institutes | Rarely | Rarely | Mostly | Mostly | Mostly |
| Charterers / Brokers / Insurance Companies | Mostly | Mostly | Partly | Rarely | Mostly |
| Owners | Mostly | Partly | Mostly | Mostly | Mostly |
| Operation Management | Mostly | Rarely | Mostly | Partly | Mostly |
| Technical Management | Mostly | Mostly | Mostly | Mostly | Rarely |
| Captain / First Officer | Mostly | Mostly | Partly | Partly | Rarely |
| Chief Engineer | Mostly | Mostly | Mostly | Mostly | Not at all |
| Manufacturer | Partly | Partly | Mostly | Mostly | Partly |
| Technical Consultants / Technical Service Providers | Mostly | Partly | Mostly | Partly | Partly |

# 2 Decomposition of Monitoring Systems

A monitoring system consist of the following elements:

- **Data Acquisition.** This term includes all involved hardware and software for measuring any physical parameter and condition and converting the signal into digital numeric values that can afterwards be handled by a computational system. Any sensor, transducer, M2M interface and reporting application that provides data to the monitoring system is part of the data acquisition. Although the combined parts are summarized under the term data acquisition, they do not form a coherent system that is clearly delimited.
- **Data Storage.** The storage of data can be implemented in various levels like in the data acquisition module or the propulsion control system, on a server in the field, on the cloud or any other backend system. It needs to be distinguished between the storage on the main server (mainly offboard for fleet management) or an onboard storage, which allows a system to store the data when no connection to the main server is available. Onboard applications can be used to select relevant data or perform the pre-processing before storing it on the persistent storage to optimize the data handling.
- **Data Pre-Processing and Transformation.** In any level of the data analysis, e.g., already during the acquisition phase, various mechanisms and algorithms for data processing could be implemented (see chapter 1.2.4). However, the responsible computation unit is then referred to as a node (e. g. fog-node, edge-node).
- **Interpretation and Evaluation.** The processing of the available data may vary for different approaches. Whereas typical rule-based evaluations of detected events can directly trigger system reactions in alarming or control algorithms, a more global view will inevitably lead to the consideration of Business Intelligence (BI) and handling of big data. The persistent BI comprises the technologies used for the evaluation and interpretation of the sampled data from an even more economic view. BI technologies provide historical, current, and predictive views of operations. Common functions of business intelligence technologies include reporting, online analytical processing, analytics, data mining, process mining, complex event processing, business performance management, benchmarking, text mining, predictive analytics, and prescriptive analytics. BI technologies can handle large amounts of structured and sometimes unstructured data. They aim to allow for the easy interpretation of these big data.
- **Information and Recommendations** is the final output of any monitoring system designed to support any decision-making process.

A monitoring system doesn't necessarily include all the above elements. Also, the order of the elements in the chain of the data handling is differentiated according to the purpose of the monitoring system, the available data sources, the type of the data and the selected architecture.

The implementation of the monitoring elements is a composition of various modules either hardware or software. The most typical modules of a data flow and analysis chain are presented in table 2.

*Table 2 Typical Modules of Monitoring System – (for detailed definitions of each item see chapter 5)*

| Data Acquisition | Data Processing | Data Transfer & Storage | Data Analysis and Business Intelligence | Information Flow |
|---|---|---|---|---|
| Sensors | Filtering | Relational DBs | Data Mining | Dashboards |
| Transducers | Formatting | Non-Relational DBs | Text Mining | Visualization |
| Signal Converters | Event Detection | Backup devices | Complex Event Processing | Natural Language Interfaces |
| Measurement Instruments | Statistical Analysis | Storage Systems | Online Analytical Processing | WEB Apps |
| Control Units | Signal Features Analysis | Data Streaming | Process mining | Mobile Apps |
| Data Loggers | Estimation of Uncertainty | Compression, Decompression | Analytics | Collaboration Platforms |
| M2M Interfaces | Classification | Data Transfer Protocols | Predictive Analytics | |
| Applications for Insertion Manual Data | Synchronization | Messaging Bus Systems | Reporting | |
| Interfaces to Data Bases | | Wireless Networks | Benchmarking | |
| Interfaces to Applications | | Satellite Networks | Learning Machines | |
| | | Optical Networks | Simulation Tools | |
| | | Wired Networks | CFD | |

According to the served purpose of the monitoring system, the solution can be synthesized using multiple modules of each category. Also, most of the modules can serve several monitoring systems eliminating the duplications of the data and acquisition systems. This is crucial for optimization, cost, homogenization, and efficiency of the monitoring structure inside an organization as union of all the monitoring systems. The main precondition for that is the interoperability of all monitoring systems and their modules. Interoperability means that each system must provide standardized interfaces (e.g., API) to share data and services with other systems.

## 2.1 Data Transfer

Measurements collected by the data acquisition component that have been converted into digital values must be aggregated for monitoring and analysis purposes. Data transfer either through point-to-point links or across data networks must address security threats, communication latencies, bandwidth limitations, communication interruptions as well as data alteration and corruption. All such aspects of interest must be considered in relation to the selected communication protocols and physical layers. Data transfer paths all the way from system sensors onboard to one or multiple backend analysis systems onshore, fall into either one of the following three categories:

- On board monitoring data network
- Vessel to shore or cloud data transfer
- Data transfer among backend systems

In the sections that follow, all aspects of data transfer deemed to be of interest are covered for each one of these categories.

### 2.1.1 On board monitoring data network

The purpose of monitoring data networks onboard a vessel is to interconnect control and/or monitoring systems with data acquisition systems, enabling collection of measurements. The main features to be considered are:

- **Security** – One might argue that, since access onboard vessels is tightly controlled, elaborate security measures may not be required. Nevertheless, encryption and threat detection mechanisms are recommended, especially for wireless networks that can be compromised from a distance. ISO16425 [5] and IEC62443 [6] provides guidelines for the cybersecurity measurements of any information network onboard the vessels.
- **Latencies** – The latencies observed on point-to-point links, such as the ones between sensors and data acquisition nodes, are insignificant in comparison to the sampling rate of the signals being observed. Uncertainties in timing do accumulate when interconnecting various data networks, however, with potentially significant effects on analysis. An effective mitigation method is to record a timestamp for each measurement as close as possible to the data source. To synchronise the clocks of different data sources it is recommended to install a Network Time Protocol (NTP) server.
- **Bandwidth** – The bandwidth of point-to-point links is generally not a concern but aggregating multiple measurement streams may cause network traffic bottlenecks. High frequency sampling employed by some condition monitoring systems may need careful consideration for the links in question. In addition, physical interfaces selected for interconnection must be capable of running at sustained speeds exceeding the maximum sampling rates desired.
- **Communication Interruptions** – Interruptions in communication onboard may indicate failures either in the monitored systems or in the data acquisition system or both. In rare occasions, interruptions may also point to mechanical issues in the interconnecting cabling or in (usually intermittent) wireless channel interference. Wired installations should employ marine approved cabling and follow comprehensive fastening guidelines. Wireless networks should be based on industrial standard technologies, hardened appropriately for increased levels of noise and interference.
- **Data Corruption and Alteration** – Corruption of data onboard is relatively rare and standard measures, such as parity checking for serial communication or checksum calculation for protocols implemented over serial lines, will generally be enough. It is recommended, however, to employ industrial grade physical interfaces using balanced transmission for cancelling inductively coupled electrical noise.

  Alteration of data, on the other hand, may become an issue when measurements are provided in a form that cannot be transferred using data communication protocols available. In such case, care must be taken so that any required translation or transformation does not result in loss of precision. Detrimental data alteration may also occur when the system being monitored filters its data output in a non-standard or, in some cases, undocumented way.

### 2.1.2 Vessel to shore or cloud data transfer

- **Security** – Data transfers from vessels to shore- or cloud-based infrastructure must be secured by using more than one layer of protection. Measurements must be packaged, compressed, and encrypted. Compression must be applied in a fashion that ensures minimal loss of data when a record is lost due to corruption, e.g., saving parameter sets in separate files and compressing sets of files in compound archives. This allows delimiting individual files in an archive, enabling recovery of all files except the one(s) affected by corrupted compressed data. Encryption applied during data transfer must support state of the art ciphers as typically employed in Virtual Private Networks (VPNs) over the public Internet. In addition, only cryptographically authorized vessel endpoints must be allowed to connect and push data to the backend analysis system.

- **Latencies** – All measurement data should already be time-stamped at this point, so communication latencies affect how data packages are re-sequenced and ingested onshore. Measurement sets covering same or similar periods may happen to be split over numerous packages. This is an important consideration when, after receiving an "out of sequence" package, databases may need to be updated for time periods already being processed.
- **Bandwidth** – Data transfer bandwidth has been traditionally scarce and expensive for vessel to shore communications. In recent years, the number of offerings and available options from providers have increased. Nevertheless, minimizing data rates and/or volumes is still important. Use of efficient compression standards and protocol stacks designed for the long round-trip propagation delays typical of satellite channels is crucial.
- **Communication Interruptions** – Challenging weather conditions causing vessel (and by consequence, antenna) movement that greatly complicates satellite tracking, mechanical vibration and detrimental interference from co-located communication equipment are just a few factors causing issues with data communications. Assumptions regarding outages for the satellite connection used to transfer data from vessel to shore will directly impact local data buffering requirements. Onboard storage must guarantee data retention for at least the duration of the worst-case outage plus an ample safety margin.
- **Data Corruption and Alteration** – Alteration of data is not an issue at this stage; there is no translation of individual values, only packetization, compression and encryption of entire data sets. Data corruption during transfer over satellite, on the other hand, may be rare but is entirely possible. For this reason, every file transferred must include means for validating integrity, e.g., a cryptographic checksum, enabling validation after being delivered to the backend system, just prior to data ingestion.

### 2.1.3 Data transfer among backend systems

- **Security** – Safeguarding sensitive vessel and company data is of highest priority at this level. Apart from state-of-the-art perimeter tools for protecting data and services from unauthorized access, the entire backend system must be designed from the ground up with security in mind. Individual services must not have direct access to databases, but only through dedicated, internal services that expose a standards-compliant interface such as REST over the HTTPS protocol. Intra-service access must be granted on an "as needed" basis, following a "zero trust" model on the backend system cluster. Accounts defined in the cluster for enabling granular access options, may be secured further by employing Role-Based Access Control (RBAC). In this way, access is restricted to certain users, groups and applications, at the right scope. Finally, a cryptographically protected gateway must be provided as a single point of entry for all outside service requests.

- **Latencies** – Communication delays internal to a properly designed, state-of-the-art backend analysis system are expected to be negligible. Latencies affecting database access, analysis services, and visualization will depend on numerous factors such as proper platform dimensioning, georedundancy support and, to a lesser extent, networking bandwidth. If the backend system is implemented on cloud infrastructure, all parameters of interest can be benchmarked and fine-tuned according to any desired optimization criteria.
- **Bandwidth** – In a properly designed backend analysis system, communication bandwidth is directly related to capacity parameters selected the for physical or virtual infrastructure provisioned. For the case of cloud infrastructure, bandwidth can be throttled according to need and/or system load, based on appropriate profiling metrics.
- **Communication Interruptions** – Interruptions during data transfer among backend systems may be rare but always a possibility. Services and data delivery must provide mechanisms to recover from such interruptions. Achievable availability figures for service consumers must factor in minimum availability guaranteed by design in the case of an inhouse data centre, or by applicable Service Level Agreements (SLAs) in the case of a cloud infrastructure on which backend systems are deployed.
- **Data Corruption and Alteration** – Data alteration will generally not be an issue of concern in backend systems if proper analysis methodologies and software development patterns are in place. It is also reasonable to expect that data integrity is guaranteed by operating software running on cloud or inhouse infrastructure. It is however advisable to retain cryptographic checksums, where already available, as an extra layer of protection.

### 2.1.4 Interfaces

Interfacing subsystems supplied by different vendors in order to collect as much data as possible for monitoring purposes can become a daunting task due to the different and often proprietary interfaces that each subsystem exposes to allow interconnectivity.

Machine to machine interconnectivity is facilitated by the adoption of communication protocols that incorporate information modelling, i.e., a standardised way of describing the machine and the data it provides, so that communication can easily be established without prior knowledge of which services and data the machine can provide.

Furthermore, due to the increased complexity of hybrid propulsion systems, and the ever-increasing complexity associated with the progressive implementation of distributed intelligence that each subsystem brings with it, it is recommended to adopt protocols that support publish/subscribe patterns, to facilitate the way the systems “talk” to each other.

In a publish/subscribe pattern, whichever system generates the data publishes it on the network on a specific topic, and authorised receivers that have subscribed to that particular topic get it whenever available and process it at their own convenience. This greatly simplifies the integration of communication among various subsystems, as in the case of ship automation and control, it significantly reduces the required bandwidth, and it improves scalability of the system.

The physical interface must also be chosen adequately. The very popular Ethernet protocol/network gives a very high throughput with its potential bandwidth. But these networks are difficult to use in situations where real time communication is required because they are based on CSMA (Carrier Sense Multiple Access) that permits each peer to start “speaking” (send data over the transmission medium) without a moderator, in a nondeterministic way. To overcome this limitation, a common standard was introduced in real-time industrial automation: Time-Sensitive Networking (TSN) is a set of standards under development by the Time-Sensitive Networking task group of the IEEE 802.1 working group, which define mechanisms for the time-sensitive transmission of data over deterministic Ethernet networks.

The majority of projects define extensions to the IEEE 802.1Q – Bridges and Bridged Networks, which describes Virtual LANs and network switches. These extensions in particular address the data transmission of very low latency and high availability.

Interfacing the on-board monitoring systems with an onshore server (either on-premises or in the cloud) can be done using standard and well-established internet technologies and protocols. Even in this case, the choice of a publish/subscribe protocol simplifies the way monitoring systems on board communicate with the remote server. Choice of protocol depends on available bandwidth, quality of service required (i.e., can some messages be lost? Is it required to have acknowledged confirmation of message receipt? Is it acceptable to receive the same message more than once?), and data security requirements.

The diversity of digital interfaces, the fragmentation of the systems, the lack of IT networks across the vessel and the low quality of them are significant barriers that must be overcome by any monitoring system.

To access data of navigational equipment, a data exchange standard, the IEC 61162 [7] series can be used. However, access of data from other on-board components and systems (e.g., machinery, safety equipment and hull) have not yet been standardised. Exchanging non-standardised data between and/or among applications requires name-based aggregation and format mapping. However, this requires a large amount of labour, which hinders the use of such data. To improve these situations, the ISO19848 [8] series defines unified rules for developing machine and human-readable identifiers and data structures for shipboard machinery and equipment, with the objective to facilitate exchange and processing of sensor data from ships. Additionally, the ISO16425 [5] series provides guidelines for the installation of ship communication networks for shipboard equipment and systems. Any installed monitoring system is highly recommended to provide interfaces according to these standards. The monitoring system could act also as the shipboard data server, for sharing information to any other system. In this case, the monitoring system should be designed according to ISO19847 [9] recommendations.

| Standards | Scope |
|---|---|
| **ISO61162** | Digital interfaces for navigational equipment within a ship |
| **ISO16425** | Guidelines for the installation of ship communication networks for shipboard equipment and systems |
| **ISO19847** | Shipboard data servers to share field data at sea |
| **ISO19848** | Standard data for shipboard machinery and equipment |

## 2.2 Data Processing

Digital values collected from a multitude of sources in a monitoring system will, in general, require further processing. This may take place at various stages, all the way from the edge (e.g., onboard) to the core (e.g., the cloud backend infrastructure). Processing at all stages must include provisions for propagating measurement uncertainty, manifested in the Data Acquisition component as measured value error. Processing requirements will vary widely depending on consumers defined for processed data and may depend on features implemented for specific stakeholders. In most cases, data volumes will increase along a processing chain, with non-trivial implications for intermediate storage and latency.

### 2.2.1 Requirements

All digital values from quantities monitored have an associated confidence interval (or uncertainty) resulting from the transfer characteristic of the sensor employed, manifested as a statistically distributed numerical error. Data processing at any stage in the system must include means for accepting an input error and for generating an output error for use by any subsequent stage.

Depending on the time and/or frequency characteristics of measured quantities, filtering of various types may be applied. This may include application-specific windowing in either time or frequency domain. Context-specific windowing may also be applied for removing outliers with the purpose of improving data quality. Such functionality may be crucially important, e.g., when using filtered data for training sensitive machine learning models at a later stage.

Data formatting and synchronization assures that value representation and signal time-base are unambiguously defined across internal and external monitoring system interfaces. Fulfilling this requirement enables interoperability and modularity across components and can be applied not only during measurement collection onboard, but also in processing and reporting stages throughout the monitoring system.

Event detection and signal feature extraction may be applied across the data processing chain. Requirements may vary from low-level operating range-checking to high-level trend and/or pattern validation. Low-level event detection enables flagging of malfunctioning sensors and/or system connectivity issues. Monitoring high-level trends and validating operating profiles can be used for preventive and/or condition-based maintenance. The sophistication and resulting value of a monitoring system shall be a function of its capacity to extract features of interest and to predict imminent failures, providing early warnings that enable preventive mitigation.

## 2.3 Data Storage

Data may be stored for short or long time-intervals, at various levels in a monitoring system. Interval lengths shall depend on design parameters such as measurement availability and latency, as well as requirements for offline post-processing and cost of storage.

Local storage must be available onboard (in the field) according to requirements for the Data Transfer component (see “Data Transfer – Requirements and Definition). Additional storage may be provided on hosts in the field, either for backup purposes or for local processing and visualization.

Backend storage may be provided across a multitude of database engines, messaging, and streaming platforms, and is specific to modules and services offered and their corresponding requirements.

The selection of the storage system must be based on the following criteria (figure 5):

| Type of Data | Scope | Hardware |
| --- | --- | --- |
| • Structured<br>• Unstructured<br>• Timeseries | • Short term analysis<br>• Long term analysis<br>• Backup Storage | • Embedded Systems<br>• Local Servers<br>• Cloud Based Systems |

*Figure 5 Criteria for Storage Selection*

## 2.4 Information Flow and Reporting

Considering the complex configuration in marine hybrid systems, end users may need a comprehensively structured representation of the information of each equipment. Hence, the scope of a monitoring system, in addition to collecting data, is to convert available data into relevant information for the different stakeholders.

For presenting the information and recommendations, reporting can be based on different technologies – ranging from regularly generated status report documents to dashboard solutions that are accessible e.g., via mobile apps or collaboration platforms.

The content that is made available by the reporting process, strongly depends on the purpose and the observation level for which the monitoring system has been designed, as well on the end users' interest for the results of each system. Therefore, it might be necessary to establish more than just a single reporting system to meet the requirements of various stakeholders for complex systems.

Ideally, the entire reporting process shall be designed to optimally support all beneficiaries in any commercial and strategic decision-making process regarding the main monitoring purpose. From this perspective, it is required that the reporting process allows the end users to improve the performance and efficiency of the marine hybrid system as well as performing condition monitoring towards efficient fault diagnosis and asset management. Therefore, the end user should get the possibility - based on the reporting system - to use the offered information to perform individual optimization studies, examine how the vessel engine performs in regimes it had not operated in the past, and aim to optimize vessel operation.

An example of a reporting system structure for a marine hybrid propulsion system is presented in figure 6, and can include:

- **Data logging** – Equipment data can be obtained online through the monitoring system, including data from engines, motors, and the energy storage system.
- **Trend analysis** – Operators can see operation of the engine over time compared to both measured and reference values, thus allowing early detection of abnormalities. It is possible to choose any period of time for a more detailed performance analysis by staff.
- **Monitoring** – An overview of engine performance data, from any period of time, can be produced from plant-specific customised displays and reports. Data and readings from offline equipment can be added into reports directly. This allows operators to easily manage regular reporting, for example, to the home office.

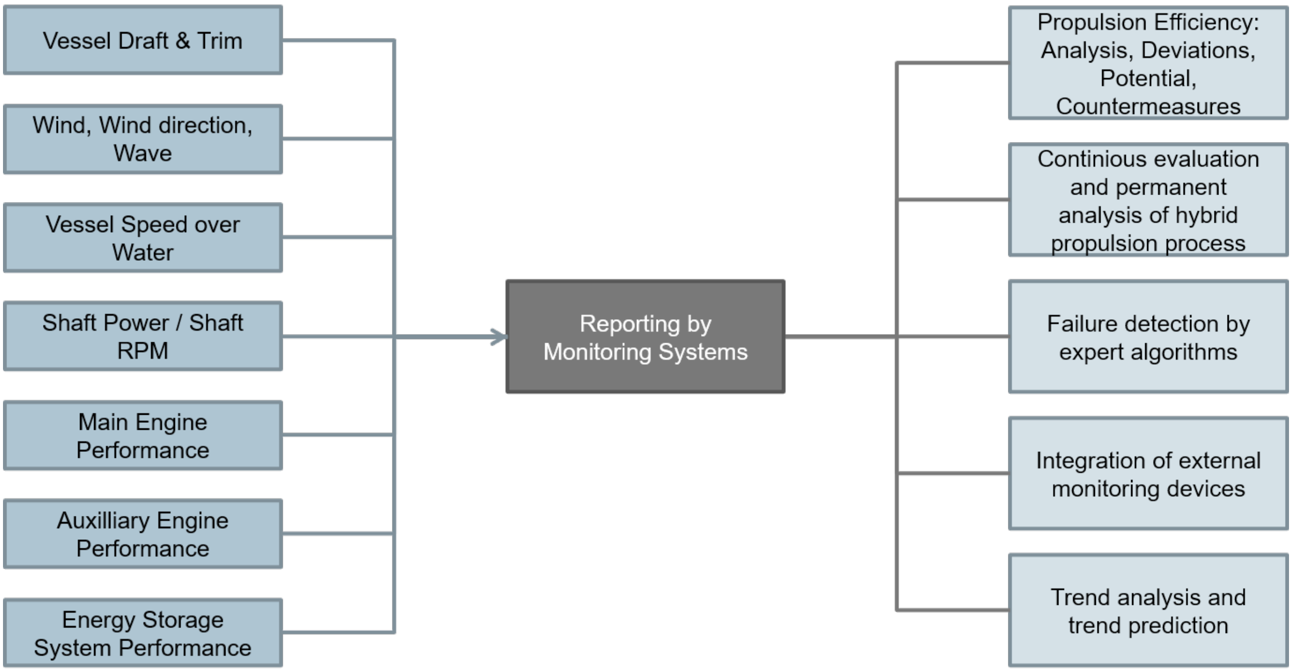


*Figure 6 Reporting System Structure of a Marine Hybrid Propulsion System*

## 2.5 Data Quality Assurance & Reliability

The ability to create, collect, store, maintain, transfer, process and present information and data to support business processes in a timely and cost-effective manner requires both an understanding of the characteristics of the information and data that determine its quality, and an ability to measure, manage and report on information and data quality.

In an IoT and/or sensor system, information and data quality are defined and measured according to the following three categories [ISO8000-8, ISO/IEC 2382:2015]:

- **Syntactic quality:** the degree to which data conforms to their specified syntax, i.e., requirements stated by the metadata; metadata is data that defines and describes other data [12].
- **Semantic quality:** the degree to which data corresponds with that which it represents [13]. For example, if a temperature sensor measures 45 degrees C, the temperature at the point of measurement must be 45 degrees C, otherwise these is some degree of semantic error.
- **Pragmatic quality:** the degree to which data is appropriate and useful for a particular purpose [14].

**Data quality** is the measurement to which degree data meet the implicit or explicit expectations and requirements of users or systems utilizing the data. Information and data quality are defined and measured according to syntactic, semantic, and pragmatic quality. Syntactic and semantic quality is measured through a verification process, whereas pragmatic quality is measured through a validation process [1] [2].

**Verification** is the evaluation of whether data complies with requirements, specifications, or imposed conditions. This generally involves a digital model (or twin) of the actual physical entity from which the data is being sampled.

**Validation** is the assurance that data meets the needs of its consumers. As intuitively expected, this involves acceptance and suitability tests with external parties.


*Figure 7 The ISO 8000-8 assessment model [DNVGL-RP-0497, 2017]*

| Syntactic Quality | Semantic Quality | Pragmatic Quality |
| --- | --- | --- |
| Verify data according to technical requirements | Verify if the data corresponds to what it represents in the real world | Validate if all data needed for the intended use is available |

The Monitoring System must be aligned to the Data Quality Management Process of the company. Of all the lower-level processes, as described in [14], the Data Quality and Control process is part of the Monitoring System, automating in high degree the verification and validation procedures.

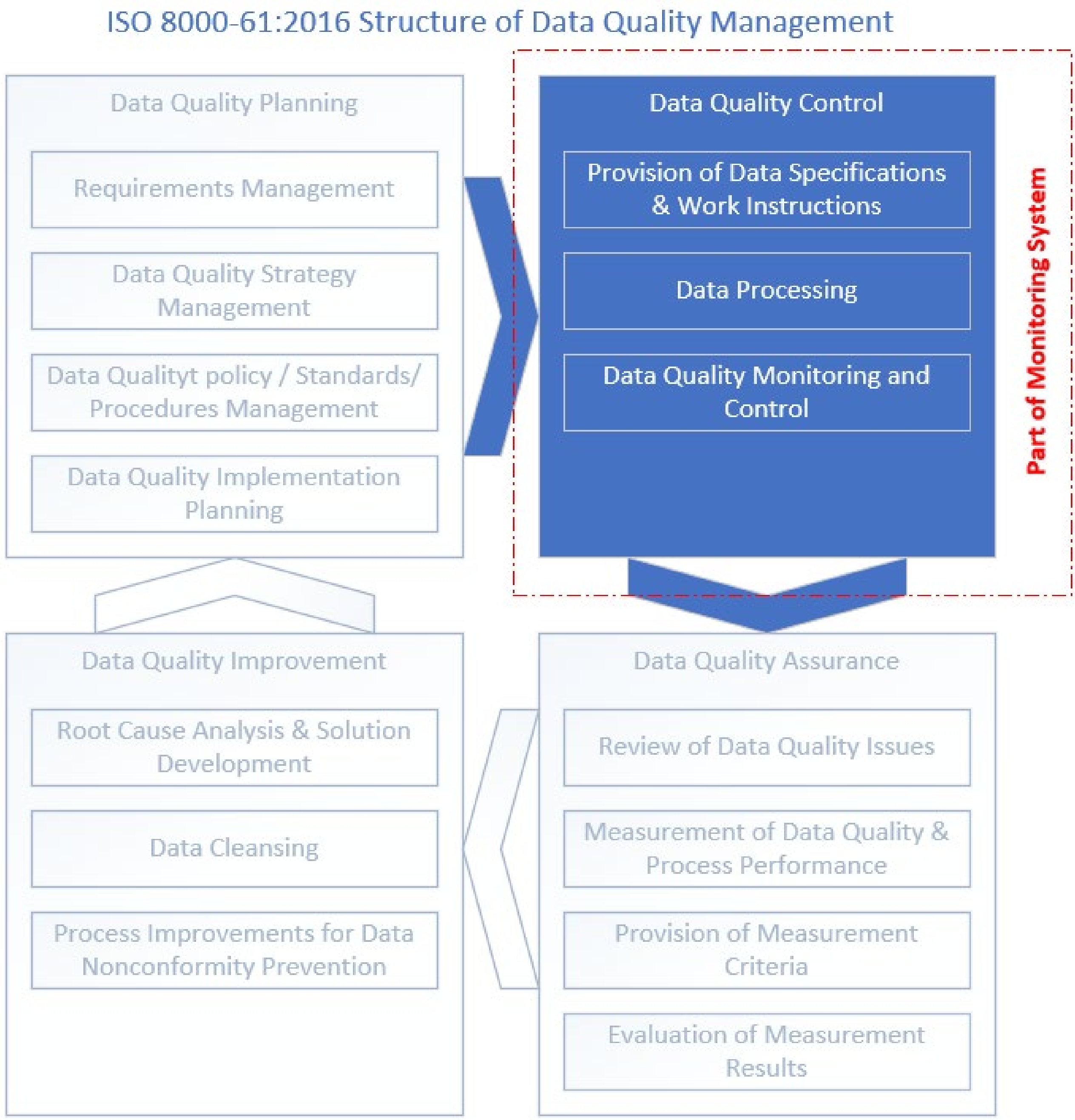


*Figure 8 Data Quality Control Process*

# 3 Recommendations

The task of this paper is to provide guidance and an overview of the tasks required to implement a performance monitoring system/equipment on marine hybrid propulsion systems. Due to the wide range of monitoring system variabilities, the following task list is a mandatory guideline to define the main requirements and can be seen as a conclusion from the former chapters:

**What are the required features of the monitoring system?**

- Define main monitoring system targets
- Are Business intelligence, condition monitoring and remote control mandatory or optional?

**Who are the actors and what is the information to be shared with them?**

- Classify beneficiaries/ ecosystem
- Classify acc. to purpose/ main scope
- Classify acc. to observation level

**What are the minimum requirements?**

- Identify mandatory systems and sub-subsystems
- Define minimum data requirements
- Define common interfaces acc. to ISO standards

**How does the system level architecture look like?**

- Define primary unit, (sub-) system and system integration levels
- Define modularity requirements and dependencies between systems and subsystems
- Clarify 3rd party system inclusions

**What is the content of the required monitoring system elements?**

- Data acquisition
- Data transfer (see chapter 2.1.)
- Data processing (see chapter 2.2.)
- Data storage (see chapter 2.3.)
- Reporting (see chapter 2.4.)

**What are the requirements on data assurance and reliability?**

- Provide data verification and validation processes
- Align monitoring system to the data quality management process of the company

**How to secure all monitoring system information?**

- Data storage strategy/system
- Data exchange standards
- Data transfer onboard
- Data transfer to shore/cloud
- Data transfer among backend-systems

Defining all requirements at an early stage is often not possible. More important in this context is an architecture with standard interfaces for future data processing and reporting. Interface protocols incorporating information modelling tend to be more future proof.

# 4 Abbreviations

| | |
|---|---|
| API | Application Programming Interface |
| BI | Business Intelligence |
| CFD | Computational Fluid Dynamics |
| CSMA | Carrier Sense Multiple Access |
| DB | Database |
| HTTPS | HyperText Transfer Protocol Secure |
| IEC | International Electrotechnical Commission |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| KDD | Knowledge Discovery in Databases |
| LAN | Local Area Network |
| M2M | Machine to Machine |
| MQTT | MQ Telemetry Transport |
| NTP | Network Time Protocol |
| RBAC | Role-Based Access Control |
| REST | REpresentational State Transfer |
| RPM | Revolutions Per Minute |
| SLA | Service Level Agreement |
| SQL | Structured Query Language |
| TSN | Time Sensitive Networking |
| VPN | Virtual Private Network |

# 5 Glossary

***Analytics.*** The systematic computational analysis of data or statistics used for the discovery, interpretation, and communication of meaningful patterns in data.

***API.*** Application Programming Interfaces are computing interfaces which define interactions between multiple software intermediaries. They define the kinds of calls or requests that can be made, how to make them, the data formats that should be used, the conventions to follow, etc., and can also provide extension mechanisms so that users can extend existing functionality in various ways and to varying degrees. APIs enable modular programming, which allows users to use the interface independently of the implementation.

***Backup Device.*** A permanent storage device that is used to store in a different location from the original a copy of computer data so that it may be used to restore the original after a data loss event

***Benchmarking.*** The practice of comparing business processes and performance metrics to industry bests and best practices from other companies. Dimensions typically measured are quality, time and cost.

***CFD.*** Computational Fluid Dynamics is a branch of fluid mechanics that uses numerical analysis and data structures to analyse and solve problems that involve fluid flows.

***Classification.*** Process of sorting data into clusters, or classes, of homogeneous content.

***Complex Event Processing.*** A set of concepts and techniques developed for processing real-time events and extracting information from event streams as they arrive with the goal of identifying meaningful events (such as opportunities or threats) in real-time situations and responding to them as quickly as possible.

***Compression/Decompression.*** The process of transforming data into a format that requires less transmission/storage capacity than the original format but is not directly accessible in such format (compression) and, vice versa (decompression).

***Control Units.*** Any electronic device that is tasked with keeping a specific process under control. In order to do so, the control unit needs to measure the parameters to be controlled to compute the error with respect to the target and to drive the actuators that operate to minimise the error. As such, control units are also means of data acquisition, and they can share the measured values with the monitoring system.

***Dashboard.*** An organised layout of tools for data visualisation aimed at giving a comprehensive overview of the monitored system status and performance.

***Data Acquisition Devices.*** The devices that perform the process of sampling signals that measure real world physical conditions and converting the resulting samples into digital numeric values that can be manipulated by a computer. They typically convert analog waveforms into digital values.

***Data Analysis.*** Process of deriving information from data, enabled by a series of mathematical tools and techniques.

***Data Mining.*** The gathering of information from pre-existing data stored in a database. The difference between data analysis and data mining is that data analysis is used to test models and hypotheses on the dataset, while data mining uses machine learning and statistical models to uncover clandestine or hidden patterns in a large volume of data.

***Data Streaming.*** Data that are continuously generated by different sources at high speed, and therefore require dedicated techniques for analysing them, which are known as stream processing.

***Data Transfer Protocol.*** System of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. The protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods, and can be implemented by hardware, software, or a combination of both.

***DB.*** A database (DB) is an organized collection of data, generally stored and accessed electronically from a computer system. It is managed by a DB management system, which provides various functions that allow entry, storage and retrieval of large quantities of information and provides ways to manage how that information is organized.

***Estimation of Uncertainty.*** The process of evaluation of the measurement error associated to the measured data.

***Event Detection.*** Capability to detect a significant variation in process parameters, which is linked to a change in system status, and which may be used to trigger a reaction (i.e., even driven response)

***Filtering.*** In signal processing, a filter is a device or process that removes some unwanted components or features from a signal, such as some frequencies or frequency bands. Filtering improves signal quality and the accuracy of the calculations that data analysis algorithms perform on such signal.

***Formatting.*** Process aimed at converting data in a format that is compatible with the expectation of the application that needs to receive and process the data, so that data exchange between producer and consumer can be done in an automatic and reliable way.

***Learning Machines.*** Machines that execute algorithms that improve automatically through experience. Machine learning algorithms build a mathematical model based on sample data, known as "training data", in order to make predictions or decisions without being explicitly programmed to do so, and they are used in a wide variety of applications where it is difficult or infeasible to develop conventional algorithms to perform the needed tasks.

***M2M Protocols.*** Machine to Machine protocols are protocols that allow machines to talk directly to each other and exchange data, using any communications channel, including wired and wireless. MQTT is an example of such protocols.

***Manually Inserted Data.*** Data that the operators collect from readings of on-board instruments not connected to the data acquisition system and that therefore need to be manually inserted into the database to be taken into consideration by the data analytics algorithms.

***Measurement Instruments.*** Any instrumentation equipped with means of measuring a given quantity and reporting the measured value directly to the operator (e. g., multimeter, manometer etc.) by means of an analog display; the term is meant here as opposed to sensors, which are instead interfaced to data acquisition systems.

***Messaging Bus System.*** A hardware/software architecture model where a shared communication channel facilitates connections and communication between software modules. Messages (command/data) travel on the bus and reach all connected devices

***Mobile App***. A computer program or software application designed to run on a mobile device such as a phone, tablet, or watch.

***Monitoring System***. Methodology that enables the user to have an informed overview of the operation and performance of the process being monitored. This is achieved through operation data collection, analysis, storage and interpretation according to specific business intelligence rules.

***Natural Language Interface.*** A type of computer-human interface where linguistic phenomena such as verbs, phrases, and clauses act as user interface controls for creating, selecting and modifying data in software applications

***Non-Relational DB.*** A database that provides a mechanism for storage and retrieval of data that is modelled in means other than the tabular relations used in relational databases. These databases have a simpler structure and are increasingly used in big data and real time web applications due to their higher scalability and possibility of performing certain operations faster than in relational DBs.

**Online Analytical Processing.** An approach to quickly answer multi-dimensional analytical queries. It allows performing analytical operations of *consolidation*, i.e., aggregation of data, *drill-down*, i.e., navigating through details of data, and *slicing and dicing*, i.e., extraction of a subset of coherent data – e.g., of all ships with the same engine – for analysis.

***Optical Network.*** A wired network that uses signals encoded in light to transmit information along fibre-optic cables. Due to its capability of achieving extremely high bandwidth it is the technology of choice for the internet.

***Predictive Analytics.*** A variety of statistical techniques from data mining, predictive modelling, and machine learning, that analyse current and historical facts to make predictions about future or otherwise unknown event (i.e., failure prediction)

***Process Mining.*** A family of techniques in the field of process management that support the analysis of business processes based on event logs. Specialized data mining algorithms are applied to event log data with the aim of improving process efficiency and understanding.

***Relational DB.*** A digital database based on the relational model of data, which organizes data into one or more tables (or "relations") of columns and rows, with a unique key identifying each row. Generally, each table/relation represents one "entity type". The rows represent instances of that type of entity and the columns representing values attributed to that instance. Relational databases have an option to be queried using the SQL (Structured Query Language).

***Reporting.*** The process of collecting and submitting data which gives rise to accurate analyses of the facts on the ground. Different from data analysis that transforms data and information into insights, data reporting is the previous step that translates raw data into information.

***Satellite Network.*** A wireless computer network that uses satellite bridges to connect nodes that are so geographically distant that other wireless technologies cannot reach them.

***Sensor.*** Literally, any device, such as a steel membrane, photoelectric cell, etc. that receives a signal or stimulus and responds to it. In practice, the term is used to define the object that is used to measure a physical quantity by generating a corresponding electrical signal.

***Signal Feature Analysis.*** A series of techniques of signal processing aimed at identifying significant features/patterns of a signal. It includes classical signal processing techniques as well as machine learning algorithms.

***Simulation Tools.*** Computer programs that can simulate the operation of a component or system through the solution of the system of equations that make up the mathematical model of the component or system under investigation.

***Statistical Analysis.*** Also known as statistical inference, it is the process of using data analysis to deduce properties of a population on the basis of observation of the properties of a sample of the same population.

***Storage System.*** A system made up of computer components and recording media aimed at retaining digital data. While memory generally refers to volatile storage (i. e. it is lost when the system is powered off), storage refers to persistent technologies that can retain data even in absence of power.

***Synchronisation.*** Technique aimed at ensuring that data generated by different sources refers to the same actual time instant.

***System.*** A set of elements which interact according to design, where an element of a system can be another system, called a sub-system, which maybe a controlling system or a controlled system and may include hardware, software and human interaction (IEC 61508)

***Text Mining.*** A branch of data mining that aims at deriving high-quality information from text, i.e., turning text into data for analysis, via application of natural language processing, different types of algorithms and analytical methods

***Transducer.*** A device that converts energy from one form to another. In case the conversion is from physical quantity to electrical signal, the transducer is known as a sensor. In the opposite direction the transducer is termed an actuator. In both cases the electrical signal involved can be used for monitoring the process.

***Visualisation.*** In this context, it indicates the graphic representation of data, aimed at human interpretation and analysis.

***Web App.*** An application software that runs on a web server. The user only needs a web browser with an active internet connection to access the app. This differs from computer-based apps that need to be installed on the user's computer and use its computing power.

***Wired Network.*** A computer network that uses cabled data connections between network nodes.

***Wireless Network.*** A computer network that uses wireless data connections between network nodes.

# 6 References


[1] ISO8000-8:2105 Data quality Part 8: Information and data quality: Concepts and measuring.

[2] ISO/IEC 2382:2015 Information Technology

[3] DNVGL-RP-0497, 2017 Data quality assessment framework

[4] Fayyad, U.; Piatetsky-Shapiro, G.; Smyth, P.; From Data Mining to Knowledge Discovery in Databases; AI Magazine, Vol. 17 No 3, 1996

[5] ISO16425:2013 Ships and marine technology - Guidelines for the installation of ship communication networks for shipboard equipment and systems

[6] IEC62443:2018 Industrial communication networks - IT security for networks and systems

[7] IEC 61162:2016 Maritime navigation and radiocommunication equipment and systems - Digital interfaces

[8] ISO19848:2018 Ships and marine technology - Standard data for shipboard machinery and equipment.

[9] ISO19847:2018 Ships and marine technology - Shipboard data servers to share field data at sea

[10] ISO/IEC 11179-1:2004 Information technology — Metadata registries (MDR) — Part 1: Framework

[11] DAMA – Data Management Body of Knowledge, 2nd Edition, ISBN 9781634622349, http://www.technicspub.com

[12] ISO 8000-61:2016 Data quality Part 61: Data quality management: Process reference model.

## Imprint

CIMAC e. V.
Lyoner Strasse 18
60528 Frankfurt
Germany

President: Prof. Dr. Donghan, Jin
Secretary General: Peter Müller-Baum

Phone +49 69 6603-1567
E-mail: info@cimac.com

## Copyright



CIMAC is the International Council on Combustion Engines, a worldwide non-profit association consisting of National and Corporate Members in 27 countries in America, Asia and Europe. The organisation was founded in 1951 to promote technical and scientific knowledge in the field of large internal combustion engines (piston engines and gas turbines) for ship propulsion, power generation and rail traction. This is achieved by the organisation of Congresses, CIMAC Circles, and other (including local) CIMAC events, and by Working Group activities including the publication of CIMAC Recommendations and other documents. CIMAC is supported by engine manufacturers, engine users, technical universities, research institutes, component suppliers, fuel and lubricating oil suppliers, classification societies, and several other interested parties.

For further information about our organisation please visit our website at http://www.cimac.com.