# Information security in critical transport systems: Case studies and lessons learned

Alessandro Cantelli-Forti[1], Michele Colajanni[2]

[1] RaSS National Laboratory, CNIT and with University of Pisa, Pisa, Italy
alessandro.cantelli.forti@cnit.it

[2] University of Modena and Reggio Emila, Modena, Italy
michele.colajanni@unimore.it

**Abstract.** Any critical infrastructure for transportation relies on safety-critical systems that have to meet stringent requirements. System performance and operations are continuously monitored by means of multiple sensors producing large amount of data. Relevant information is preserved in so called "event data recorders". We evidence some present limitations in the exploitation of recorded data that are fundamental for the legal reconstruction of the scenario in case of serious malfunctions and incidents. Real examples are related to investigations referring to the Costa Concordia and Norman Atlantic accidents. We then indicate some possible ways to guarantee information security in terms of data integrity and availability that are essential to identify and attribute human and/or machine responsibilities.

**Keywords.** Transportation systems, event data recorder, accident forensics, human and machine attribution, data integrity and availability.

- "Event data recorders", namely *black boxes*, of critical transportation systems are designed to comply with current regulations although they present several limitations in reconstructing the data semantic scenario in case of serious incidents.
- Some examples of drawbacks are reported in the case of naval transportation incidents where it is necessary to legally reconstruct the scenario and to attribute human and/or machine responsibilities.
- We evidence the main areas for improvements in terms of data integrity, data availability and synchronization of the events related to several sub-systems of the transportation system.

## 1 Introduction

Critical transportation systems, such as air and naval vectors, may lead to people's death or serious injury, loss or severe damage to equipment or environmental harm in case of failure or malfunction. Both US (since 1996 and then the Patriot Act in 2001)

and Europe (EPCIP program) have a critical infrastructure protection program in place for transportation (DHS, 2018). Any modern critical system is controlled by some software components where a correct process engineering and management is essential. Standards and certifications require precise codification, inspection, documentation, test, verification and analysis of the system (Bowen and Stavridou, 1993). Unfortunately, many safety improvements in transport systems are realized by "learning the hard way" from incidents MCIB, 2013, (Clinch, 2013). Accidents' reconstruction and analysis is another important method to mitigate potential life threats in a transport critical infrastructure, where multiple sensors continuously monitor systems' performance and operations and produce large amount of data that is continuously used for proper real-time functioning. The most relevant data is registered in the so called "event data recorders", that should allow the technical and legal reconstruction of the scenario in case of serious malfunctions and incidents. For these reasons, data integrity and availability of "event data recorders" are essential for a solid attribution of human and/or machine responsibilities.

### 1.1 Data recording requirements

Typical event data recorders are hardened, specifically designed and embedded devices that are controlled by a software running on some general-purpose CPU or microcontroller. Since this controlling software is not considered life-critical, the typical directives for critical infrastructures are not applied. Specific legal and regulatory requirements of data collection and preservation are addressed by so called "minimum requirements". Every transport system category has to follow specific "minimum requirements" transposed into national and or international laws issued by FAA and EU for aviation (EUROCAE ED-112), International Convention for the Safety of Life at Sea (IMO Res.A.861/20) for navigation, NHTSA's ruling and for automotive (49 CFR Part 563) and U.S. regulations (CFR 49 Ch II 229.5) or UK and Ireland GM/RT 2472 regulations for railway transport system. These requirements are less stringent than those related to life critical system and do not indicate formal methods of producing software nor standard verification systems.

The exploitation of recorded data is fundamental for the legal reconstruction of the scenario in case of serious malfunctions and incidents. Unfortunately, regulations are drawn up to be inspirational and future proof in the perspective of technological progress. For example, it is not taken into consideration how the internal logic of the programs determines the format and the semantics of the information produced by sensors [6-9]. Hence, the event data recorders producers are free to implement the characteristics required by regulations as they fit, but some architectural choices, trade-offs and limitations are common in the design of any event recorders of every transportation system. The drawbacks of this situation are highlighted in the Concordia and Norman Atlantic accidents, where the forensics analysis for the precise reconstruction of the scenario was restricted by the limited possibility of exploiting recorded data from "event data recorders" [5-9]. Another problem is represented by the fragmentation of the written data that usually occur when the sensors detect many anomalous events at the same time and time synchronization protocols are not implemented. We claim that urgent and practicable solutions are necessary to guarantee

information security in terms of data integrity and availability because they are essential for forensic analysis in critical transportation systems with the goal of attributing human and/or machine responsibilities.

### 1.2 Event Data Recorders

The reconstruction of events occurred to a critical transport system and, more specifically, to a means of transport, is typically recorded by on board devices and/or is transmitted through a terrestrial or satellite link to a base station (US Patent 6,677,888 B2, 2014). This paper focuses on the former devices that are called *event data recorder* or *black boxes*. These hardened devices include read and write memories and exist for any transportation system: “Event Recorder" (EDR) in terrestrial vehicles, “Flight Data Recorder” (FDR) and “Cockpit Voice Recorder” (CVR) in aviation, “Train Monitoring Recorder” (OTMR) in railways, and “Voyage Data Recorder” (VDR) in naval transportations.

On-board data recording is not affected by transmission problems nor by information-carrying capacity and guarantees high confidentiality, because its data is not continuously monitored. On the other hand, local storage, which suffers from physical space limitations must be resistant even to serious accidents and depends on the energy source of the transport vector. Any planned and unplanned maintenance must be carried out on board. In the event of a catastrophic accident, the black box can be designed to remain anchored or disengaged in order to be more easily found.

### 1.3 Authors’ Contribution

Both authors took care of conceptualization, original draft preparation, review and editing. A.C.F carried out experiments, data curation, investigation, software development and validation. M.C. led the analyzes of the results, devised and supervised the main conceptual ideas and the methodology.

This paper is organized as follows. Section 1 is introductory to different Event Data Recorder technologies. This section contains some data integrity and availability requirements common to EDRs. Section 2 is the literature review and describes the bibliographical and experimental sources of the case studies. This section motivates the research to focus on the data recorders of naval transport systems Section III describes Voyage Data Recorders’ operations and current limitations. Section IV summarizes lessons learned from case studies. Section V presents suggestions for improvement. Section VI is the concluding one.

## 2 Literature Review

The present manuscript extends some of the topics of the paper presented by first author at 2018 IEEE International Conference on Smart Computing (Cantelli-Forti, 2018), which was limited to a single use-case study and focused on forensic analysis and regulations. Technical and legal investigative reports from aviation, naval and rail investigation commissions was collected and considered the most reliable sources of information for this research. Any data recorder instruction and maintenance manual

included in these reports have been taken into consideration. The possibility of consulting the archives of Accident Investigation, Tri Branch data recorder group of UK and Transport Accident Investigation Commission of New Zealand was requested and granted. Every international technical reports of the mentioned naval accidents have been consulted. The research within those archives has identified twenty-one cases in which the Event Data Recorder failed to provide some or all of the information for the investigation in aircraft, train or naval accident investigations. Authors made this documentation publicly available online through a cloud platform (RaSS.Cloud, 2018). The analysis of these reports shows that the investigative approach to the failures of the Event Data Recorders is not epistemic and that failures are mentioned but not studied in deep. Incident reports of Costa Concordia and Norman Atlantic ships are the only ones found that devote relevant sections to fault analysis. It is also evident that the VDRs are extremely less reliable than the Event Data Recorders of Trains and Airplanes. This is confirmed by Marine Accident Investigation Branch of the Marine Casualties Investigative Body in UK: In 2016 stated that over 230 data recorders had been analyzed and 90% of the data sets evidenced issues in exploiting its content (Clinch, 2013). On the other hand, all the reported malfunctions about the train and aircraft Data Reorders are indicated as inadequate maintenance. Furthermore, literature review shows that airplanes' FDRs and CVRs seem to suffer from the lack of redundant power in the event of an emergency, which needs also to be considered as external cause. In addition to an alarming percentage of malfunctioning VDRs, accidents in the maritime field have specific needs. The amount of time useful for investigations, in which it is advisable to record the greatest amount of information, is wider due to latency in maneuvering ships. Moreover, while in the event of an air or rail disaster a violent impact represents the final moment of the accident, in case of a naval one, it can represent its initial event. If a ship is seriously damaged in its structure, its sensor networks keep generating a huge quantity of useful data for a long time essential to identify and attribute human and/or machine responsibilities and these data are not always correctly preserved in the analyzed case studies. [5-10]. Naval VDR systems, therefore, deserve the focus of this paper.

## 3 Voyage Data Recorders' operations and current limitations

The capacity of the data stored depends on the adopted technology and the physical dimensions of the hardened compartment called "capsule". Depending on the use case, the minimum registration time required by the regulations must be sufficient for a timely reconstruction of the event that needs to be analyzed.

In every transport system, events are recorded using a circular memory paradigm (Cavo-Dragone, 2012) which is an implementation strategy for any queue that has fixed maximum size. This means that a block of new events is logged overwriting the oldest block in memory. When a maximum size is adopted for a queue, a circular buffer is a completely ideal implementation. Safety standards indicate the minimum time that should be reconstructed by recorded data before the end of recording (Cavo-Dragone, 2012), (Carpinteri, 2017). In order to prevent overwriting of specific events' data, a manually operating command can be given to protect a portion of the circular memory from overwriting. Each time this function is activated, the overall memory for recording

new events is reduced. It is possible to speculate that after a first event to be reconstructed due to a human error, it is necessary to deepen the correct reaction and functionality of the emergency critical systems in order to mitigate the event. The opposite can also be hypothesized: as a consequence of a transport system failure, it might be necessary to verify if the personnel have fully respected their liability. In order to cover more non-consecutive time periods, the personnel in charge should carefully activate the aforementioned system while managing a serious emergency. This is assumed to be unlikely feasible (Carpinteri, 2017).

Unfortunately, in the case of an accident, a physical damage to a means of transport, as well as to the sensors connected to an Event Recorder, will also increase the density of data sent per unit of time by several orders of magnitude (Cavo-Dragone, 2012), (Carpinteri, 2017). This constraint is not always considered as demonstrated by the reconstruction of the two most serious accidents to passenger ships in Europe (since the mandatory introduction of the VDRs) has been much more complex or less successful than expected [5-7], (Carpinteri, 2017). In the case of the Costa Concordia cruise ship (Capsized and sank in 2012 off Isola del Giglio, Tuscany), the data of the Safety Management System, valuable for the investigations, required the rewriting of part of the raw data parsing software that did not provide for this such a great number of events per minute (Cavo-Dragone, 2012). In the case of the passenger ferry Norman Atlantic (destroyed by fire in 2014 in the Strait of Otranto), the VDR, the Ship Automation System and the Fire System have completely failed in providing useful data to the Investigation. The main reason was due to the overwriting of the data concerning the origin of the fire (Carpinteri, 2017). A concomitant reason for these shortcomings was the granularity of the type of circular memory of the fire alarm system: no less than a quarter of the oldest memory could be erased during standard operations. The solid-state memory of the fire alarm critical system was divided into few partitions; without a real file system, the minimum erase unit was an entire partition.

The choice of the subset of data to be sent to the VDR is described in (Cavo-Dragone, 2012) and (Carpia, 2012). Before being saved in the hardened capsule, that is resistant to catastrophic events, the data can go through “Data Concentration” systems and optional "Replay Systems" enabling the on-board review of events. The data concentrators are used to contain the largest quantity of data chosen by the sensors and to decimate them in time sampling. In the Costa Concordia investigation, the capsule was damaged due to a bad block in the solid-state memory containing the Real Time Operating System [5-8]. The data were taken from the Replay System that luckily remained on the emerged side of the ship. On the other hand, for the similar reasons, data were unavailable in the Norman Atlantic investigation because they had been overwritten. The copy of the data of the Norman Atlantic’s VDR was too general and did not indicate the specific fire sensors but only the general alarms. The most complete source of information was sent to a small printer connected to the Fire System Panel which reported the data about the intense fire on thermal paper.

### 3.1 Voyage Data Recorder’s data sources

This section describes how data are generated by the multiple sensors of a critical system, then defined and translated. Every received event is contained in a line of text,

called *sentence* or *telegram*. The header declares the beginning of an event, the sensor(s) that originated it, and the type of content. For instance, a data coming from a satellite-based radio navigation system receiver can be flagged either of time or position type and can embed details such as type or reception quality as in GPS, GLONASS, GALILEO, Standard or Augmented.

After the header or the identification tag, each line of text contains the payload consisting of strings separated from each other. The payload is composed by a specific apparatus that receives sampled sensors' data. Accident investigation experiences have shown that a timestamp should be attached as soon as the data is collected, before storing a *telegram*. After being generated, the telegram is sent to a *data concentrator*. If relevant, it is also sent to the event data recorder. Only a receipt timestamp is generated and recorded by the data concentrator in a first-come-first-served order. Data generation timestamp is not required by the regulations, but it would improve investigators' ability to reconstruct events [5-9], (Clinch, 2013). Reception timestamp can be a prefix or suffix to each line; the creation timestamp, when provided, would be part of the payload.

Data from sensors is received simultaneously from different transmission channels (by a point-to-point link or network), and an indication of the channel number is part of the telegram structure. In order to verify the correct operation of the sentence generator and its subsequent re-transmissions, an errors detection algorithm adds a checksum control characters at the end of each sentence. It is actually calculated as an XOR of all the bytes in the sentence, excluding prefixes and suffixes. The final exploitation of this data should be an easily readable graphic system, usually called Replay System, in order to retrospectively reconstruct the events of interest [Fig.2].

In none of the analyzed case studies it was possible to use these replay systems as they were inconsistent when trying to reproduce the same event (Cavo-Dragone, 2012), (Carpinteri, 2017). Some data was not reproduced at all.

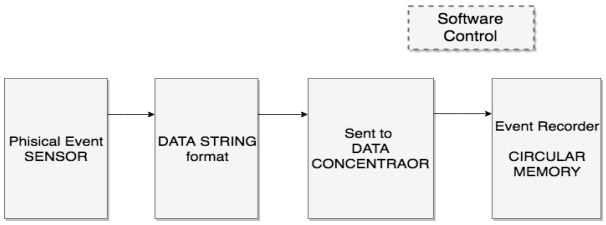


**Fig. 1** - Example of data flow from physical event to Event Recorder

### 3.2 The NMEA format

This model is the basis of some data formats including NMEA 0183 and NMEA 2000. The NMEA is a standard that is defined and controlled by the National Marine Electronics Association (NMEA, 2012). It specifies the electrical interface and data protocol for communications among marine instrumentation such as echo sounders, sonars, anemometers, gyrocompasses, autopilots, GPS receivers and other kinds of instruments. All data is transmitted in the form of simple ASCII sentences, also called telegrams, passing from one *talker* to multiple *listeners* at a time, serial communications protocol or LANs. Intermediate expanders allow a unidirectional

conversation with an unlimited number of listeners. Multiple sensors can communicate to a single computer port through multiplexers. Other event recorders like IDR and EDR are not required to follow a standard format, but they observe similar approaches. Very few car makers have published their custom standard (Kean, 2014).

### 3.3 Assemblage of subsystems

Ships are a peculiar critical transport infrastructure as they are not usually mass produced. The biggest ones, like the Costa Concordia, are real floating cities hosting thousands of people. All the subsystems, starting from the most important ones, like the engines, to the critical ones, like the automation systems, are not the result of a holistic design approach of the whole ship, but it is an assemblage of independent parts, like most consumer-grade personal computers (Cantelli-Forti, 2016). For this reason, a data paradigm, such as the one described, risks of being a limiting factor.

When a transport system is an integration of subsystems, a proper documentation regarding every single data recorded by the Event Recorder becomes of primary importance (Cavo-Dragone, 2012). In addition to the significance of the physical recorded value, it is necessary to be sure of its location in the payload area which contains several measurements referred to the same identification tag. In addition, the range, the metric system and the possible non-linearity of a digitized analog value (for instance, the aerodynamic shipping surfaces of an aircraft or a rudder of a ship) need to be clearly documented. This is a complicated task if we consider the project dimensions and the number of suppliers and systems integrators.

### 3.4 Data sentences fragmentation

Existing solutions suffer from fragmentation problems that are internal and external to the sentences. The industrial sub-systems generate sentences starting from their internal logs that are not intended for data integration. In addition to the semantic limits, when there is a lack of documentation (and this is the typical case) there is a problem of format size.

NMEA messages have a maximum length of 82 characters on one line including the $ or ! starting and the ending Line Feed character. Minimum time resolution is one second. Hence more lines may be necessary to represent some data like alarms. The position within the sentence defines the type of data. Fragmentation can cause wrong positioning in the payload space at critical moments when many alarms are received (NMEA, 2012). Moreover, the raw logs of some subsystems are often transposed in NMEA format by specific modules. When the module detects too much information in the same second, then it acts to divide logs in more sentences. The combination of these two fragmentation behaviors might requires complex reverse engineering process and writing of specific parsers for each analyzed case (Cavo-Dragone, 2012), (Carpinteri, 2017).

### 3.5 Clock synchronization

The system is when every sentence is an atomic and independent information that indicates one sensor read, such as the temperature of a component or the wind direction. Understanding more complex data describing an event requires more than one sentence

and the integration of data coming from multiple sensors. In this case, it is important to know the exact order of events with a precision that should be defined a priori. Accordingly, a synchronization system needs to be provided, such as Network Time Protocol or IEEE standard 1588v2 since every real-time clock will shift. In the considered accidents, the shift has been measured to be of few days.

### 3.6 Push and Pull architectures

When the alarms condition or other measurements are distinguished only by *high and low* states, it is fundamental to decide whether to use a *push* or *pull* architecture on data. In the former case, all status changes are recorded while they are occurring whereas in the latter case they are retrieved at regular intervals. In the case of a push architecture, the time accuracy of the status change detection can be defined in the project, whereas in the pull cases the refresh time generates an interval of uncertainty.

In the survey of Costa Concordia disaster, it was understood that the watertight doors were monitored by a system that sent the data both directly to the VDR system and to an emergency system called the Safety Management System (SMS) that each time redirected them to the VDR MCIB, 2013. These systems were generating data with pull technologies in the first case and with push architecture when processed a priori by the SMS system. The data received in near real-time in push mode did not consider the actual state of the *fully open* sensor, but they expressed only the positions of complete or incomplete shutting given from the *fully closed* sensor. The data received in pull mode is aware of booth sensors could distinguish complete closing, partial opening which meant movement, full open with a delay of up to 16 seconds (Cavo-Dragone, 2012). Some events in the latter case could be misses when status changes were short.

As a further complication, it is important to evidence that the two ways of receiving data were recorded independently by the VDR based on the time they were received. They were not received with a fixed delay that depends on the type of transmission medium: serial link for push, Ethernet LAN for the pull. After the incident, because of the water flood and damages, data traffic increased uncontrollably and serial multiplexers generated delays due to congestion, different delays were from the data transmitted over LANs (Cavo-Dragone, 2012). As a consequence of the lack of the telegram generation timestamp, the only way to align “push” and “pull” based data was to find shared patterns for alignment. This alignment required that short status changes were not recorded via pull and the alarms were only detailed in the pull data. Indeed, in the push cases, there was only an indication of general alarm and not related to specific doors.

The alarms related to the *Hydraulic Power Pack*, representing the hydraulic energy reserves indispensable in the event of a blackout for the running of the watertight doors, are not detected in the event of a power outage. Such alarms, such as low oil, low oil pressure, blackouts, obviously trigger off only in the absence of electricity. This design limit is present in many ships and it is an evident result of the regulations interpretation that does not provide for the connection of the weathertight doors to the Emergency Diesel Generator, as the doors are too *power hungry* (Cavo-Dragone, 2012). These regulations do not even account the use of UPS which in that position, under the main deck, would be flooded. For these reasons, during the criminal investigation, it was

very difficult to decipher both the state of the doors at the time of the accident and their actual closure during the capsize.

One of the aspects of the Norman Atlantic investigation referred to the Fire System that similarly sent data to the Event Logger with two distinct paths. Even though they were both *push*, they suffered from different and unpredictable delays to the extent that alignment was necessary through the comparison between the recorded alarms (Carpinteri, 2017). The problem in that case also regarded data semantics: one of the two paths considered the manual reset of the command and control panel of the general error to be sent whereas the other did not.

## 4. Lessons Learned

Overall, we can conclude that these VDRs, critical recording systems, fail their primary purpose because they are not designed to detect anomalies related to an emergency. The choice of the most relevant data to be preserved in hardened memories should be evaluated carefully. When this is not foreseen, it becomes of primary importance to decide when to suspend the circular registration as evidenced in (Cavo-Dragone, 2012), (Cantelli-Forti, 2016). The actual solution is to trigger a timeout that nowadays is forced by regulations in the case of blackout events. Any Event Recorder can easily recognize the lack of tension even because a UPS can operate as a buffer supply and communicate the lack of main power to the recording system through a serial link. Any critical transport system is provided with an Emergency Electric Generator that feeds the utilities required by the regulations for a certain period of time in the event of a blackout. In ships and trains this is called the Emergency Diesel Generator, while the planes are equipped with a small wind turbine called RAT (Ram Air Turbine) which, however, in some use cases studied, was not expected to power the data recorders. Their entry into service indicates an emergency and the loss of propulsion and services. Therefore, every Event Recorder should have an independent continual power system and monitor the main power line and not the emergency line. Other serious shortcomings are a widespread lack of documentation and the lack of an integrated approach to the configuration of the Event Data Recorders components and sources of information. In particular case studies analysis bring out the lack of attention to synchronization problems, effective timestamping, protection against data fragmentation and an effective paradigm for managing the data sampling and representation.

## 5 Proposed Solutions

In a critical transport system, some not immediately visible aspects can make a sensor network's data recorder ineffective in case of incidents (Cantelli-Forti, 2016), (Carpinteri, 2017). Most issues are caused by a difficult integration of sub-systems designed for more generic purposes and lack of proper documentation. The other limitations identified could be solved with the use of information security technologies.

### 5.1 Understanding and exploitation of data

Future regulations and technologies should include a qualitative approach that can evaluate the type of data recorded on the basis of a data taxonomy. This solution would facilitate a cognitive decimation, thus mitigating the problem of the data burst during emergencies.

From an event data recorder operation prospective, all system clocks should be synchronized to avoid ambiguities by mean of specific protocols. The documentation of how the information should be exploited has to consider complex dynamics of synchronization, integration, semantics and worst-case data generation throughput (Cavo-Dragone, 2012). The choice of the data format could be formalized in the format of a single message per event. This approach generates the least possible overhead, but it is dependent on a correct documentation. Unfortunately, the current implementation requires the support of the provider companies that may have not kept the necessary know-how during time. A markup language could allow each piece of information to carry material regarding its semantics and not be bound to its position within a message to be understood (RaSS.Cloud, 2018). This approach has not been pursued yet either due to the low speed with which the rules are updated (IMO, 2018) or the technological limits of the hardened storage systems that is necessary for the survival to a catastrophic event. Although the density of storage on solid state memories grows, it is also verified that these messages could only partially survive an accident and lose the self-descriptive content (Cantelli-Forti, 2016), (Carpinteri, 2017). A memory corruption that is both logical (as in the case of overwriting) and physical, could damage a dense and self-descriptive data logical format based on markup language. Moreover, many electronic devices, without an operating system, still transmit via serial interface and do not have computational resources of a markup language.

### 5.2 Data integrity and availability

From an event data recorder technology prospective, through the use of Copy-On-Write cryptographic system that with the Merkle tree such as btrfs or OpenZFS it is possible to verify the integrity of the data, enforce anti-tampering as of, digitally sign the maintenance operations performed and give redundancy to critical equipment such as recording medium.

OpenZFS (as btrfs) is designed for long term storage of data by means of hierarchical checksumming of all data and metadata, in order to ensure that the entire storage system can be verified on use, and confirmed to be correctly stored, or remedied if corrupt. Checksums are stored with a block's parent block, rather than with the block itself. This contrasts with many file systems where checksums (if held) are stored with the data so that if the data is lost or corrupt, the checksum is also likely to be lost or incorrect.

With the send/receive operations included in OpenZFS, by means of *Copy-On-Writ*e technology, a “forensically sound” approach could be ensured without further technical complications. Anomaly detection algorithms might be used to make the data recorder system aware of an accident in progress to automatically avoid useful data overwrite. In such a case, cryptographic file system’ primitives such as snapshotting and cloning could preserve useful recorded intervals, on the fly.

### 5.3 Forensically sound procedures

Moreover, a suitable approach to a criminal investigation requires repeatable data extraction procedures. For this reason, we propose that the internal memories of crash survival modules should enforce a specific forensic procedure that is not implemented yet. Companies fail, the know-how is dispersed, and the retrofits imposed by the regulations complicates the readings which currently take place with custom procedures. On the other hand, specific read only mode could allow a forensic, bit-by-bit copy that is guaranteed by cryptographic hash functions. A standardization based on open formats would further benefit the entire critical transport infrastructure industry (Cantelli-Forti, 2018).

## 6. Conclusions

This paper exposes main reasons for Event Data Recorder's issues and the reasons why the maritime industry's event recorders are the least reliable in exploiting its contents for legal and technical reconstruction of the incident scenario. This paper also proposes some ways for solutions that can leverage recent technological advancements. Due to the high percentage of failures, we expect that event recorder manufacturers will make a joint effort to harmonize their attempts and improve future standards also through the transfer of information technologies that guarantee information security.

## 5 References

US Department of Homeland Security (2018). *Critical Infrastructure Security*. [online] DHS official site, https://www.dhs.gov/critical-infrastructure-sectors [Accessed 14 May. 2018].

International Maritime Organization, Maritime Knowledge Centre (MKC), 1974-2018. [online] *Resolutions Online Archive*. www.imo.com [Accessed 14 May. 2018].

Bowen, J. and Stavridou, P. (1993). *Safety-critical systems, formal methods and standards.* Software Engineering Journal. 8 (4). IEE/BCS. Victoria. pp. 189–209.

United States Patent 6,677,888 B2 (2014). *Secure Aircraft Communications Addressing and Reporting System* (ACARS).

Cavo-Dragone, G., Dalle-Mese, E., Maestro, M. and Carpinteri, F. (2012). *Technical Report for the Court of Grosseto*, Italy.

Cantelli-Forti, A. (2016). *Evidence recovery and analysis from the Costa Concordia's digital data by means of forensic techniques: turning data into information, European Maritime Safety Agency Seminar on Voyage Data Recorders and Electronic Evidence*. Cranfield University, UK.

Marine Casualties Investigative Body (2013). *Cruise Ship Costa Concordia Marine casualty on January 13th, 2012 Report on the safety technical investigation.* Ministry of Infrastructure and Transport, Rome.

Carpinteri, F. et al. (2017) *Norman Atlantic shipwreck, 28 December 2014, Technical*

*Report for the Court of Bari*, Italy

Capria, A. (2012). *Costa Concordia shipwreck, 13 January 2012, Technical Report for the Court of Grosseto*, Italy

Kean, T (2014). *Event Data Recorder, An Overview*. Virginia State Police, Virginia, USA

Serrano, J (CERN) et al (2013). *The White Rabbit project*. Proc. of the 2nd International Beam Instrumentation Conference, Oxford, UK.

National Marine Electronics Association (2012). *The NMEA 0183 V 4.10 Standard*. Severna Park, Maryland, USA

Clinch, S. (2013). *VDRs the most important tool?*. European Marine Accident Investigators International Forum, Santa Margherita Ligure, Italy.

RaSS-Cloud public archive on EDRs failures during accident investigations, https://rass.cloud/index.php/s/XxGww8iRY8e3mtz [Accessed 10 Sep. 2018]

Cantelli-Forti, A. (2018). Forensic Analysis of Industrial Critical Systems: The Costa Concordia's Voyage Data Recorder Case. *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2018, 458-463.