engineering proceedings

MDPI

Proceeding Paper

Robustness Levels of Critical Infrastructures Against Global Navigation Satellite System Signal Disturbances †

André Bos [1,2,*], Merle Snijders [2,3], Alexandra Zevenbergen [2,4], Kirsten Drost [1,2], Hein Zelle [2,3] and Bas van der Hoeven [2,4]

1 S[&]T BV, 2616 LR Delft, The Netherlands
2 EGNSS Centre of Excellence, 2201 DK Noordwijk, The Netherlands; merle.snijders@nlr.nl (M.S.); alexandra.zevenbergen@cgi.nl (A.Z.); hein.zelle@nlr.nl (H.Z.); bas.van.der.hoeven@cgi.nl (B.v.d.H.)
3 Netherlands Aerospace Center (NLR), 1059 CM Amsterdam, The Netherlands
4 CGI, 3068 AX Rotterdam, The Netherlands
* Correspondence: andre.bos@stcorp.nl
† Presented at the European Navigation Conference 2023, Noordwijk, The Netherlands, 31 May–2 June 2023.

Abstract: Resilience against signal disturbances is an important characteristic of GNSS-based PNT solutions. In particular, for critical infrastructures, failure to provide correct PNT information in these domains may have a major societal impact. The Resilience Framework by the Department of Homeland Security (DHS) provides a set of requirements and guidelines to design a PNT solution of a certain level of resilience. Over the lifetime of the applications, it will be of prime importance to assess the resilience of the PNT solutions on a regular basis. Given how often GNSS-based solutions are being applied, partly automating the assessment process will be needed to make this task feasible. To automate the generative process, a machine-readable structure with well-established meaning is required. In this work, the use of fault trees as a formal system to encode the resilience framework is investigated.

Keywords: resilience; PNT solutions; jamming; spoofing; assessment; questionnaire generation

Citation: Bos, A.; Snijders, M.; Zevenbergen, A.; Drost, K.; Zelle, H.; van der Hoeven, B. Robustness Levels of Critical Infrastructures Against Global Navigation Satellite System Signal Disturbances. *Eng. Proc.* **2023**, *54*, 21. https://doi.org/10.3390/ENC2023-15443

Academic Editors: Tom Willems and Okko Bleeker

Published: 29 October 2023

1. Introduction

Global navigation satellite systems (GNSS) have become immensely popular for providing positing, navigation, and timing (PNT) information to a wide range of applications. The popularity has a downside as well. It has been well documented (see, e.g., [1]) that GNSS-based PNT information can be easily compromised, either intentionally or accidentally. However, this kind of vulnerability knowledge of GNSS-based PNT information is not very well known outside the community of GNSS specialists. Especially for applications that control critical infrastructures, this lack of knowledge may lead to less effective operation and maintenance of the infrastructure and eventually to the potential loss of essential services and resources.

In order to better inform designers and operators of critical infrastructures, the knowledge of robustness should be better disseminated. This study describes the first results of an attempt to make this information more readily available: The resilience of applications that use PNT information for their correct operation is investigated. The assessment will be based on a resilience framework pioneered by the US Department of Homeland Security (DHS) [2]. Various ways of assessing resilience are foreseen, from questionnaires to automated test approaches. The proposed approach in this study is to largely generate the assessment methods automatically using a computer program that uses a computer-readable and formalized description of the resilience framework. Resilience is obtained by the robustness of the GNSS receiver and the additional equipment to determine the PNT information. Various signal disturbances are considered, including natural radio frequency interference (RFI), jamming, and spoofing. There are many different formalisms

for describing the (lack of) resilience knowledge. This study considers the "fault tree" formalism to capture the resilience knowledge.

2. GNSS Basics, Disturbances, and the Potential Effect on Critical Infrastructures

2.1. GNSS Basics

A GNSS receiver tracks the signals of all the GNSS satellites in view. One of the indicators of the quality of the tracking process is the carrier-to-noise density (C/N0), which is expressed in decibel-Hertz (dB-Hz). Too low a value of C/N0 (typically < 25 dB-Hz) usually renders the receiver to lose its lock on the signal. The higher the values of the C/N0, the better the receiver estimates the pseudo range.

2.2. Disturbances

Unintentional interference mainly comprises natural, inter- and intra-, out-of-band, and in-band interference. Such interference can come from faulty machinery. Also, a multipath is one of the major contributors of error to satellite positioning, especially in urban canyons.

Jamming: Jamming is the process of purposefully disturbing the reception of GNSS signals by receivers in a targeted geographic—the jammed—region. In case of jamming, a powerful signal is applied to the target receiver's antenna, such that the front end will need to handle the high-power signal, thereby reducing the capability to handle the low-power authentic GNSS signal. Usually, the front end will adjust the automatic gain control (AGC) so that the processor can handle the powerful jamming signal. The effects of jamming are [3]: potential loss of tracking, decrease in measured signal strength (C/N0), adjustment of AGC values, increase in noise on pseudo range measurements (code phase and carrier phase) and position, and increase in cycle slips.

A rather new jamming technique is called systematic jamming and uses measurements of the signal-to-be-distorted to jam the signal in an intelligent way. Systematic jamming relies on a standard receiver that determines at which points in time jamming is most effective and only jams the signal briefly, e.g., to deny reception of the time of week indicator.

Spoofing: Spoofing is the transmission of forged GNSS-like signals, with the purpose of producing a false position or time at the victim's receiver without seemingly disrupting GNSS operations and thus effectively taking control of the receiver. With the advent of software-defined radio (SDR) technology, it has become a practical method to implement a spoofing system and thus could pose a real threat to the trustworthiness of GNSS-based PNT information.

2.3. Example of Critical Infrastructure Applications and Electricity Networks

Applications within critical infrastructures often require reliable and accurate PNT information. Just relying on a simple GNSS receiving system for this PNT information may not be enough to satisfy the availability and safety requirements that are imposed on the applications running in the critical infrastructures domain.

Some example applications from the electrical energy sector domain include [4]:

- Sequence of Event (SoE) recording is a data logging system that stores timestamped event information. The exact order of events is essential in quickly finding the real cause of the problem in electricity systems. A fault in one system may result in a whole avalanche of events at the subsystems connected to the source of failure. These events happen so fast that it almost seems like one instantaneous event with too coarse a time resolution for the SoE recorder. The timing accuracy requirement is < 1 ms;
- A phasor measurement unit (PMU) is a device used to estimate the magnitude and phase angle of an electrical phasor quantity in the electricity grid. The timing accuracy requirement is < 1 μs;
- Wire fault localization using the traveling wave method. Such methods calculate fault locations by measuring the arrival times of the naturally occurring traveling waves caused by a transmission line fault. The timing accuracy requirement is < 100 ns.

GNSS-disciplined clocks are used in such applications to obtain these strict time constraints. The basic principle of these clocks is that the GNSS time information controls a local oscillator. The basic principles actually being used are often not disclosed, but in general, the frequency of the local oscillator is kept within strict bounds by one or more servo loops, such as a Phased Locked Loop (PLL). After a GNSS disturbance has occurred, the clock will still continue to operate, but the clock stability parameters will degrade over time. In case the disturbance occurs for a longer period, the clock might not meet the application's requirements. It may take minutes to hours before the clock is degraded such that it fails to meet the accuracy requirements, depending on the quality of the local oscillator.

3. Resilience Framework

In the previous section, the various ways to disturb GNSS signals were introduced, as well as how these can affect various applications within the electricity-critical infrastructure. There is great interest in the development and analysis of resilient implementations. One of the approaches is the Resilience Framework by the US Department of Homeland Security (DHS) [2]. This framework could be seen as a set of very useful guidelines to achieve a certain level of resilience during the implementation of PNT sources for applications. The framework defines the following concepts:

PNT System: The components, processes, and parameters that collectively produce the final PNT solution for the consumer. Note that this is not necessarily restricted to GNSS components.

PNT Source: A PNT system component that is used to produce a PNT solution. Examples include GNSS receivers, networked and local (stable) clocks, inertial navigation systems (INS), and/or timing services provided over a wired or wireless connection.

PNT Solution: The full solution provided by a PNT system or source, including time, position, and velocity. A PNT system or source may provide a full PNT solution or a part of it. For example, a GNSS receiver with a clock may provide a full PNT solution, while a local clock only provides a timing/frequency solution.

Component: A part or element of a larger PNT system with well-defined inputs and outputs and a specific function. Examples may include individual PNT sources or subsystems of PNT sources, discrete software functions that implement resilient PNT processing algorithms, hardware modules providing a supporting function internal to the PNT system, antennas, firewalls (between antenna and receiver), and external detectors such as those based on SDR technology.

Recover from atypical errors to return to a proper working state and defined performance.

Then, the framework identifies four levels of resilience (see Table 1).

The framework is not necessarily geared towards GNSS-PNT in particular but is agnostic with respect to a particular technology that is being used. Furthermore, although the framework provides guidelines to assess the resilience of PNT solutions, in reality, the assessment will not be straightforward. For example, the effectiveness of identifying compromised PNT sources (point 4 in Table 1) will vary from one implementation to another. By further detailing the conditions for the resilience levels (as can be part of the formalization process), one can better identify why a certain solution fails to qualify for a certain resilience level.

Table 1. Resilience level requirements overview (from [2]).

Level	Minimum Requirements
Level 1 Ensures recoverability after removal of the threat.	1. Must verify that stored data from external inputs adheres to values and formats of established standards; 2. Must support full system recovery by manual means, making all memory clearable or resettable, enabling a return to a proper working state, and returning the system to the defined performance after removal of the threat; 3. Must include the ability to securely reload or update firmware.
*Level 2 ** Provides a solution (possibly with unbounded *** degradation) during a threat.*	Includes capabilities enumerated in Level 1 plus: 4. Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions; 5. Must support automatic recovery of individual PNT sources and systems without disrupting system PNT output.
Level 3 Provides a solution (with bounded degradation) during a threat.	Includes capabilities enumerated in Levels 1 and 2 plus: 6. Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source; 7. Must cross-verify between PNT solutions from all PNT sources.
Level 4 Provides a solution without degradation during a threat.	Includes capabilities enumerated in Levels 1, 2, and 3 plus: 8. Must have a diversity of PNT source technology to mitigate common-mode threats.

Notes: Level 0 indicates a source or system that does not meet the criteria in Level 1 and thus is considered a non-resilient system or source. ** Critical infrastructure applications will likely require Level 2 resilience at a minimum. *** The output can deviate within a manufacturer-defined envelope.

Reference Architectures

The framework [2] also describes a reference architecture for acquiring Level 1 and Level 2 resilience. For Levels 3 and 4, no reference architecture is given yet. A PNT solution with resilience Level 3 may experience a bounded level of degradation when operating in a threat environment, whereas a Level 4 solution should not experience that degradation. The framework also provides guidelines for assessing the resilience level of a particular solution and defining testing procedures compliance for a certain level. The objective of the study presented in this paper is to largely automate these tasks, as described in the next section.

4. Formal Description of PNT Resilience

The following section will focus on the formalization of the framework. Such a formalization will ease the automatic processing by a computer as such a formalization can be used to generate computer programs performing a certain analysis task. One of the goals is to construct a computer-assisted resilience assessment and an automatic testing system that is able to generate test data to test resilience.

There are various types of formalisms that describe events (failures and exceptional conditions) and their impact on system behavior. One of these formalisms (and, maybe, conceptually, one of the simplest to comprehend) is the modeling of system behavior by fault trees [5]. This section briefly describes the fault tree (FT) formalism and then how it can be used to capture the resilience knowledge.

4.1. Fault Trees

One of the possible formalisms that can capture the failed operation of system components and, to a certain level, the sequence of occurrence of those failures is fault trees. Fault tree analysis (FTA) is a type of failure analysis in which an undesired state of a system is examined. This analysis method is mainly used in safety engineering and reliability engineering to understand how systems can fail, identify the best ways to reduce risk, and determine (or obtain a feeling for) event rates of a safety accident or a particular system-level (functional) failure. The main elements of a fault tree are a TOP event, which is the description of the critical system event, such as the tracking loss lock; Basic events

are the lowest level of identified causes, such as excessive RFI or atmospheric scintillations; and Logic gates, such as OR or AND gates, which give the logical relationship between the TOP event and the basic events.

The AND gate is used to model redundancy in a system design or alternative test methods. A redundant system's function will only not be realized if all the alternatives fail. The OR gate is used to model serial dependencies in a system design or test method. If one of the components fails, then the overall system functionality fails to be realized. Given system components 1, 2, and 3 for a hypothetical system, then layer (i) of Figure 1 depicts the OR gate of these components, layer (ii) the AND gate of these components, and layer (iii) a combination of the OR and AND gates.

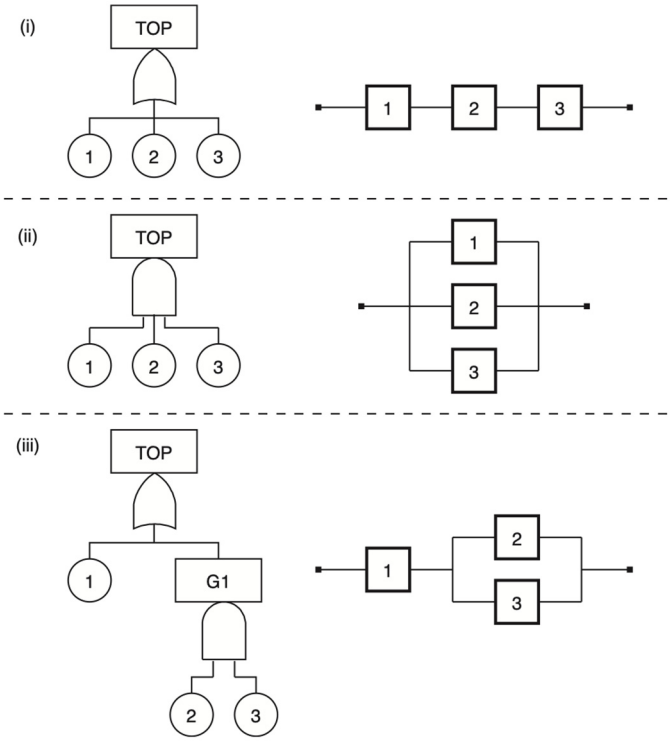

Figure 1. Construction of a fault tree.

There are several analysis methods that can be applied to the FT structure. One such method is the dependency analysis, or the estimation of the minimal set (minimal: deletion of one element from the minimal set invalidates the defining property) of Basic Events, causing the Top Event to be True. Such a minimal set gives the combination of events that renders the resilience to be invalid. Thus, it will be important to check that this combination will not happen during the lifetime of the PNT system. A well-known graph algorithm, the minimal cut set algorithm, exactly corresponds to solving this dependency analysis problem. Another analysis is the computation of the Probability of a Failure (PoF). If the probability of the Basic events can be determined and independence of events is assumed, the probability of the Top Event can be determined by propagating the probabilities in a bottom-up fashion.

4.2. Formalisation of the Resilience Framework

The fault tree method will not be applied to a particular system design (as in the usual case of applying fault trees) but will be used to encode the requirements of the resilience framework. One could say that the fault tree will basically model the robustness behavior of a reference architecture for a certain resilience level. Each of the resilience levels of the framework has attached a number of requirements that must be satisfied in order to qualify the PNT system to the corresponding resilience level. Furthermore, the resilience

framework contains various high-level requirements for which the formalization may need to be made more specific to allow the automatic and effective generation of assessment applications (questionnaire and test program generation). Different fault trees can be defined for these requirements. For example, the framework specifies the rather high-level Requirement 4 of Level 2: "Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions." For this the concept of "compromised PNT sources" and "prevent them from contributing" must be specified. Compromised PNT can mean various things, for example, Compromised by Jamming, Compromised by Spoofing, and Compromised by Antenna position. Concentrating further on the case of "Compromised by Jamming", the basic events would include, for example, "lock lost" and "increased code and carrier noise". However, these events can also come from other than jamming events. Jamming detection can be performed by inspecting the RF samples or monitoring the receiver observations, such as the carrier-to-noise density (C/N0). Once jamming has been detected, the effects of jamming can be mitigated using, e.g., signal processing techniques (such as the adaptive notch filter (ANF)) or spatial filtering (such as the controlled reception pattern antenna (CRPA)). The "Loss of Lock" fault tree for the Jamming Case could look like the one given in Figure 2.

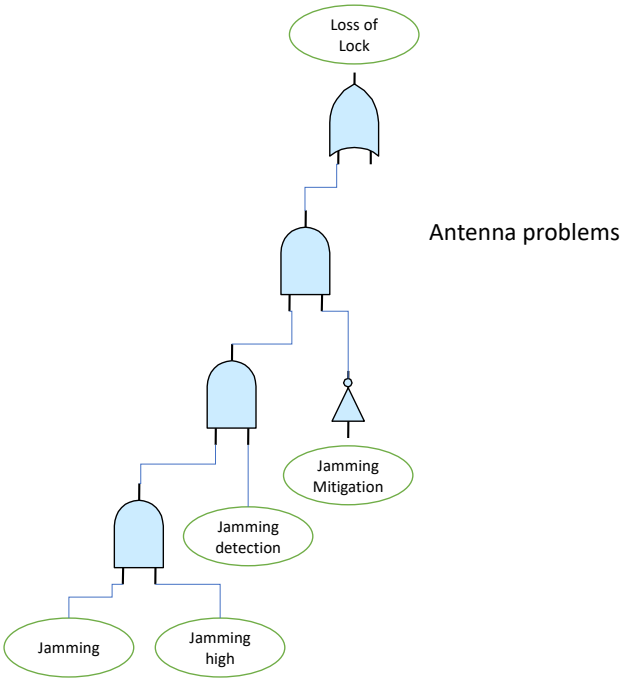

Figure 2. Fault tree for jammed signal.

"Loss of lock" can also be caused by the antenna position, due to the fact that the line of sight to the satellite is obscured. This can be caused by buildings that block the view. A similar fault tree can be constructed. For Compromised by Spoofing, the basic events would include "tracking of encrypted signals" (such as Galileo PRS [6]) and cryptographic checking of the navigation data (such as in OSNMA [7]). By correctly combining these basic events, one can encode the satisfaction conditions for this requirement.

In general, there can be several detection methods to recognize jamming, spoofing, or other disturbances. These methods will have, in general, different detection characteristics and will, therefore, trigger alarms under different conditions.

4.3. Generating a Resilience Questionnaire

The formalization of resilience knowledge can be used for various analysis techniques, such as the computer-assisted evaluation of resilience levels. The FT will be further attributed with evaluation questions. That is, for each of the "basic events", a question about

the presence of the events can be assigned such that the truth value of these basic events can be established, as is depicted in Figure 3.

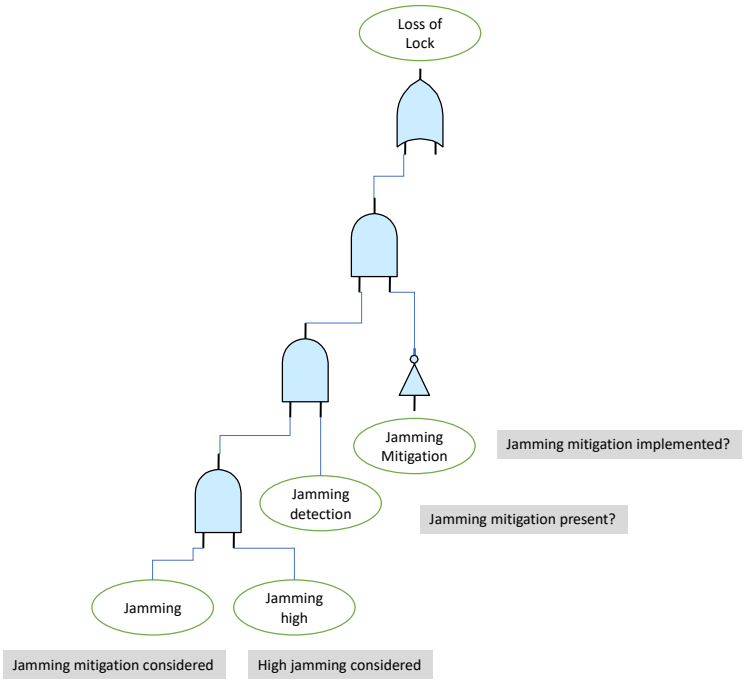

Figure 3. Fault tree augmentation with questions.

Now, as according to Figure 4, the FT can be evaluated as either "bottom up" or "top down". Top down starts at the TOP event and evaluates the value of the tree by descending the nodes of the tree and keeping track of the truth value of the basic events and the sub-trees.

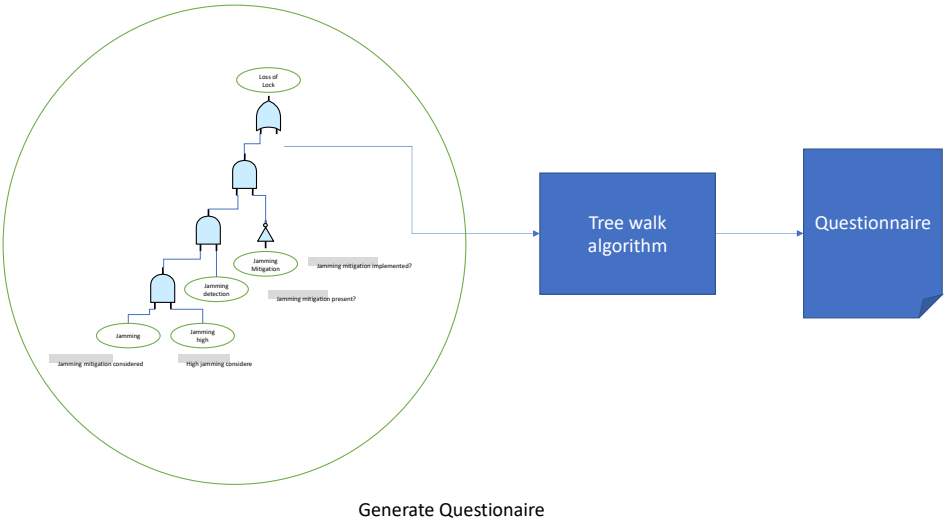

Figure 4. Automatic assessment method generation.

The formalization process is rather labor intensive, but once the knowledge is formalized, the generation of questionnaires is rather straightforward. Having a formal model allows various types of analyses, including the generation of test data.

5. Concluding Remarks

As the usage of GNSS-based PNT information for applications within critical infrastructures is present, it becomes of vital importance to keep an eye on the resilience of these

systems. In this study, the partly automatic generation of questionnaires, and eventually test programs, is researched. This approach requires the cumbersome formalization of a resilience framework into a form that a computer can process. The formalization work ideally has to be performed once. Still, this formalization task is laborious and prone to errors. Alternative methods will be investigated in further research. The current popularity of generative Artificial Intelligence (AI) [8] seems to suggest that this technique would provide an alternative to questionnaire generation. Much more research is needed in this direction as well.

Author Contributions: Conceptualization, A.B.; methodology, writing—review and editing, A.B., M.S., A.Z., K.D., H.Z. and B.v.d.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors thank the reviewers for their valuable comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ioannides, R.T.; Pany, T.; Gibbons, G. Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques. *Proc. IEEE* **2016**, *104*, 1174–1194. [CrossRef]
2. DHS, Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture. V2.0, The Department of Homeland Security (DHS) Science and Technology Directorate (S&T). 2022. Available online: https://www.dhs.gov/sites/default/files/2022-06/22_0609_st_resilient_pnt_ra.pdf (accessed on 13 December 2023).
3. Jansen, P. The Impact of Jamming and Spoofing on GNSS Signals. Master's Thesis, Delft University of Technology, Mekelweg, The Netherlands, 2022.
4. Dagle, J.; O'Neil, L.R.; Tuffner, F.; Bonebrake, C.; Engels, M.; Dindlebeck, G.B. *Energy Sector Position, Navigation, and Time Profile*; Technical Report, PNNL-30780; Pacific Northwest National Laboratory: Richland, WA, USA, 2021.
5. Fovino, I.; Masera, M.; De Cian, A. Integrating cyber attacks within fault trees. *Rel. Eng. Syst. Saf.* **2009**, *94*, 1394–1402. [CrossRef]
6. PRS. Available online: https://www.euspa.europa.eu/european-space/galileo/services/prs (accessed on 12 May 2023).
7. Galileo Open Service Navigation Message Authentication (OSNMA). Available online: https://www.gsc-europa.eu/galileo/services/galileo-open-service-navigation-message-authentication-osnma (accessed on 12 May 2023).
8. The AI writing on the wall. *Nat. Mach. Intell.* **2023**, *5*, 1. [CrossRef]