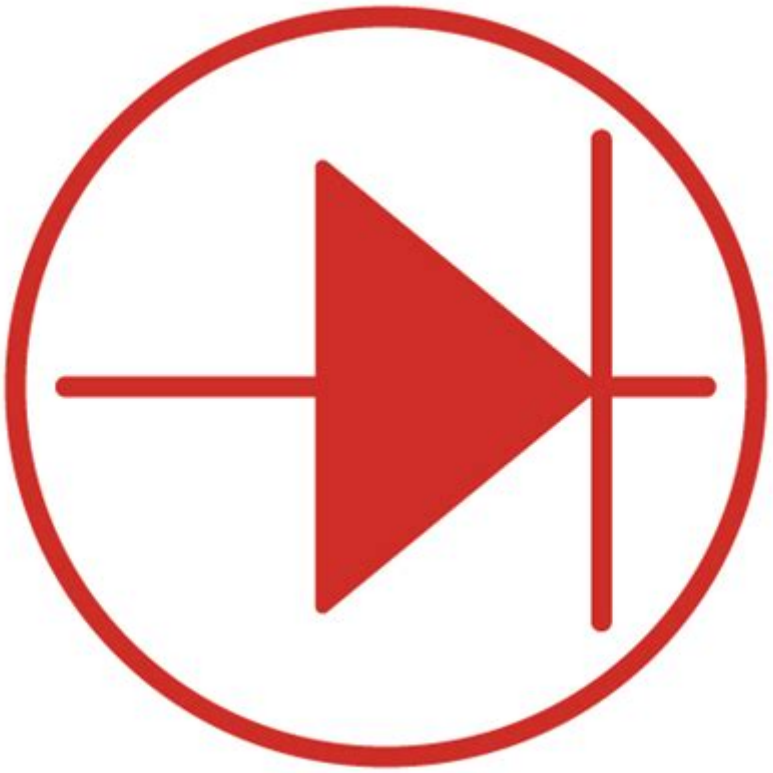
Data-Diode Report

Management of Security



- Croche Loïc - 000502435
- Cochez Benjamin - 000490159
- Hanquin Benjamin - 000495418

Table of Contents

1. Introduction

1.1 Context

On board a ship the watchstanding officer uses an "Electronic Chart Display and Information System" (ECDIS), which is a type of "Geographic Information System" (GIS) that is used for nautical navigation and that complies with the regulations of the "International Maritime Organization" (IMO) and therefore is a legally valid alternative to paper nautical charts. Alongside its on-board radar and depth sounder, a ship's ECDIS relies on information from the "Automatic Identification System" (AIS) for providing situation awareness to the officer(s) on the bridge. The AIS system on-board a ship consists of a standardized VHF transceiver combined with a positioning system such as a GPS receiver, as well as other electronic navigation sensors.

Nowadays satellites equipped with AIS receivers are typically used for monitoring maritime traffic. ORBCOMM is for instance operating a global satellite network that includes 18 AIS-enabled satellites. The AIS information is accessible to the general public through a number of free portals, like on https://www.vesselfinder.com/.

AIS was originally developed for "collision avoidance" but since then a number of other applications are heavily relying on AIS as a source of information, such as fleet and cargo tracking, fishing fleet monitoring, search and rescue, accident investigation, and underwater infrastructure protection. For that reason AIS is nowadays considered to be a "critical infrastructure".

A number of high profile incidents in the recent past have shown that critical infrastructure is an increasingly popular target for cyber-attacks. A number of security researchers have furthermore pointed out some security issues with the current AIS protocols and implementations.

For the purpose of this exercise we will consider that a "Global Agency for Ship Tracking" (GAST) is to be created that will operate a number of AIS receivers on-board satellites , fuse the information with other sources of information, and will provide the obtained information to the authorities, to industry and to the general public.

1.2 Project

Following the context, we are playing the role of the GAST, and we must secure the network in order to assure to the end users that incoming data from AIS Server (high

level network) are real and has not been altered. These data are sensible and so we must ensure I.A. (Integrity , Availability) principles which are properties of secure information.
The possibility that the trajectory of some boats are diverted is real and therefore, the consequences that would be binded to them could be devastating, like as collisions and so one.
That's why we have to design and implement a component of the GASP security architecture , this component is the **Data Diode** and it must be a certified one.

1.3 Data diode

Data diode solves the secure data transfer by one-way communication channel.
That's allows to solve communication between the insecure network to the secure network without allowing any data to leave these secure network. In fact, Data Diode allow to separate a level 2 network (access by business employee) and a level 3 network (just read only from level 2 network).
In the data diode there are two servers, the "pitcher" and the "catcher".
The pitcher is the server the sender and the "catcher" is the receiving one. In this case, the catcher server can't send any data to the pitcher server.
To achieve this , the 'pitcher' will send information through an optical fiber connected in a one-way maner (cfr Figure 1.2) to the 'catcher'.
Light is a nice choice because it avoids electromagnetic perturbations and it's faster than copper cable.

The communication protocol used in the data diode is UDP (User Datagram Protocol) because of the one-way communication, as the TCP (Transmission Control Protocol) needs a bidirectional communication (send and wait for response).

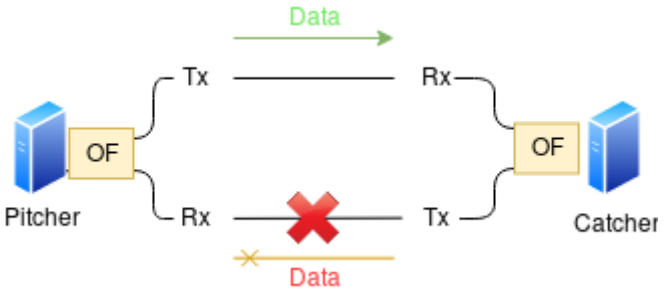


Figure 1.1 : Scheme of the data-diode.
OF = Optical Fiber | Tx = Optical Transceiver |Rx = Optical Receiver

2. Risk analysis report (NIST SP 800-30 based)

Risk analysis is very important to protect a network against malicious guy but a lot of businesses do not perform risk assessment because it is too long to prepare and it isn't cost-effective. For help companies, frameworks exists to supervise and accelerate process. For data diode, we use a part of these different frameworks as NIST, ISO 27K series and SANS CSC.

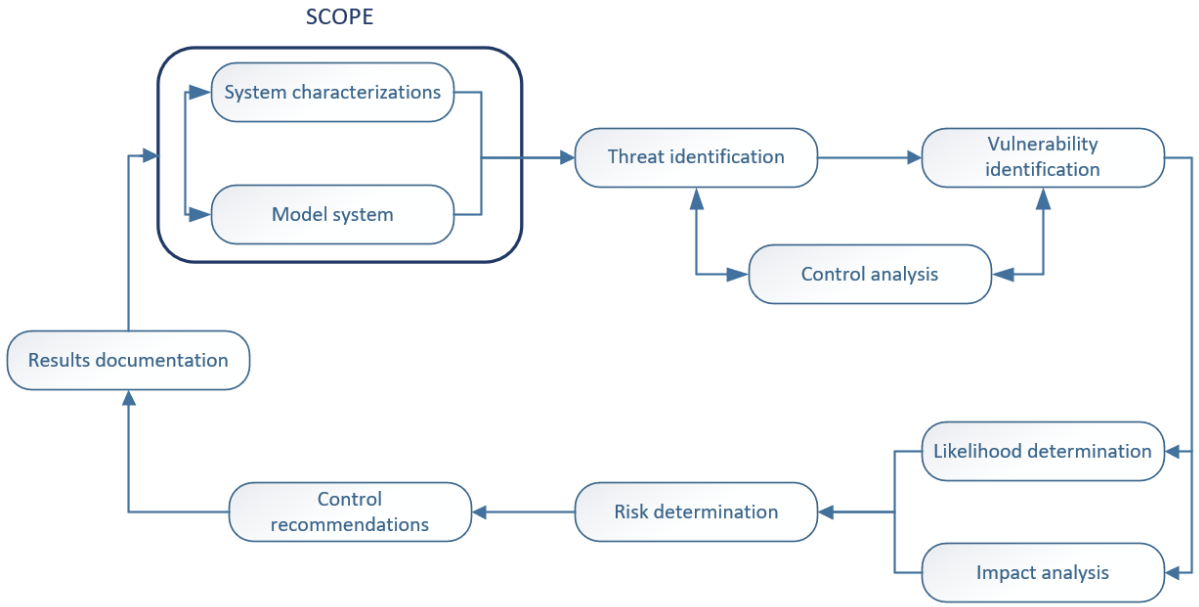


Figure 2.1 : Risk analysis diagram

Risk analysis is composed of several steps. Certain steps can be made in parallel with other one.

2.1 Define the scope

In first time, we must determine the scope of our project before we make the risk assessment.

We assume that we performed security only on Data Diode in network architecture. All data that arrive on AIS server are assumed secure. All the "private network" (c.f.r. Figure 2.2) are determined insecure.

During scope step, we will define system characterizations (assets and what's scope must be able to implement). Modeling system part is designed in chapter 3 which called "Design documentation".

2.1.1 Scheme of scope

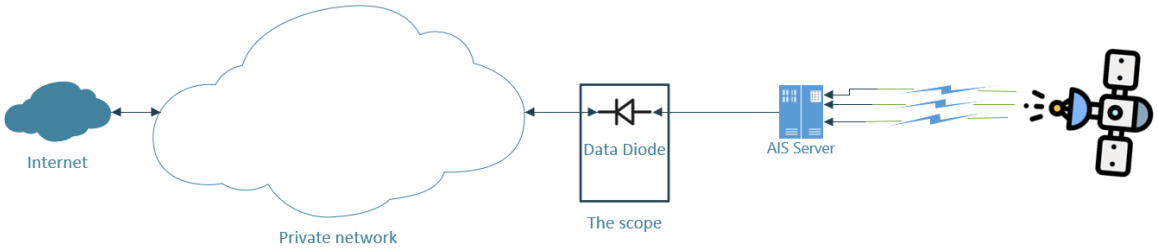


Figure 2.2 : Scheme of the Network

2.1.2 System characterizations

In the Scope :

We have two main parts in our scope, catcher and pitcher servers with data flow management.
We must ensure different points in scope like this :

- **I**ntegrity, we will assure that the data that flow through our data diode , from the *pitcher* to the *catcher* , will not be modified by an external/internal actor. As so we'll be sure that the data received by the catcher have not been altered during transport.

- **N**on-**R**epudiation, we'll make sure that the data received by the catcher is really coming from the pitcher. As so we'll be sure that the message is coming from the pitcher before reading it and then transfer it securely .

- **A**vailability, we'll make sure that the flow through our data diode will be assured no matter which problem happen (in our scope) . The diode being a bottleneck to the network , and so this availability is vital to the whole structure.

- **A**ccess control for the diode, we'll ensure that only authorized *user* will be able to access to the management console of the diode severs. As so the diode could not be modified by an attacker without proper access.

- **A**udit, we'll ensure that each action done within the servers are well written in log files. It allow to check what happened on the servers anytime.

Out of the Scope :

- General topology of the network, the DMZ and the local network must be well designed with security devices as firewall, IDS, IPS, … We assume that local network is segmented.

- Update system, we cannot ensure the frequency, stability and overall the content of updates on our data diode. We'll assume that the system is always up to date and so we don't have to worry about them neither of flaws repaired by them.

- Electricity supply management/Availability (More than few hours), we cannot assure the constancy of the electric supply management delivered by the company/power supplied. So we'll assume that the electric management is stable and will never be down more than few hours.

- Integrity of received data, we cannot ensure the data that come from the AIS server are not corrupted. This depend of the data received from the satellites. So we assume that incoming data are not corrupted and are fully readable.

- Physical access, we cannot ensure that no one will have access to ou data diode via the building where it is placed. This depend of the physical security level of the company. So we assume the diode is placed in a secure shelf within a secured room where only authorized personnel "the administrator" have access.

Implementation of Integrity and Non-repudiation

Asymmetric key will be used to ensure the **non-repudiation and integrity** by signing the hash of the encrypted message.

The hash function we choose is SHA with a key of size 256 bits.

For the asymmetric key we'll be using RSA for signing as our algorithm and a key size of 2048 bits .

We decided to choose RSA over ECDSA (Elliptic curve digital signature algorithm) for its efficiency in power consumption and speed despite of the key length problem in RSA . This problem is based in the fact that RSA keys are 9 to 30 times bigger than ECDSA and so signatures are bigger and so packet are as well, with RSA (n bits key = n bits signatures in RSA). In our case, this data length problem is null because we got an optical fiber and no relay between the two actors.

Each week a update process will begin, this process role is to renew asymmetric keys and it is initiated by the ‘pitcher’ . We did not implement it here.

Theses algorithms and key size have been chosen based on NIST recommendation (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5-draft.pdf). This combination give the minimum security level required to be ‘secure’ until 2030.

Message transfer scheme :

The message received from the high network combined with the current time will be hashed using SHA-256. The hash now have to be signed using the ‘pitcher’ private key. We send the message combined once again with the signed hash through the fiber.

The ‘catcher’ will receive both of signed hash and message. The signed hash will be verified and compared to the received message hash using the public key certificate of the ‘pitcher’ present in the ‘catcher’. If the hash is successfully identified as coming from the ‘pitcher’ and if the two hash matches , the time in the message can be compared to the current one . If the two times are less than 5 seconds different , the message is retransmitted to the low network.

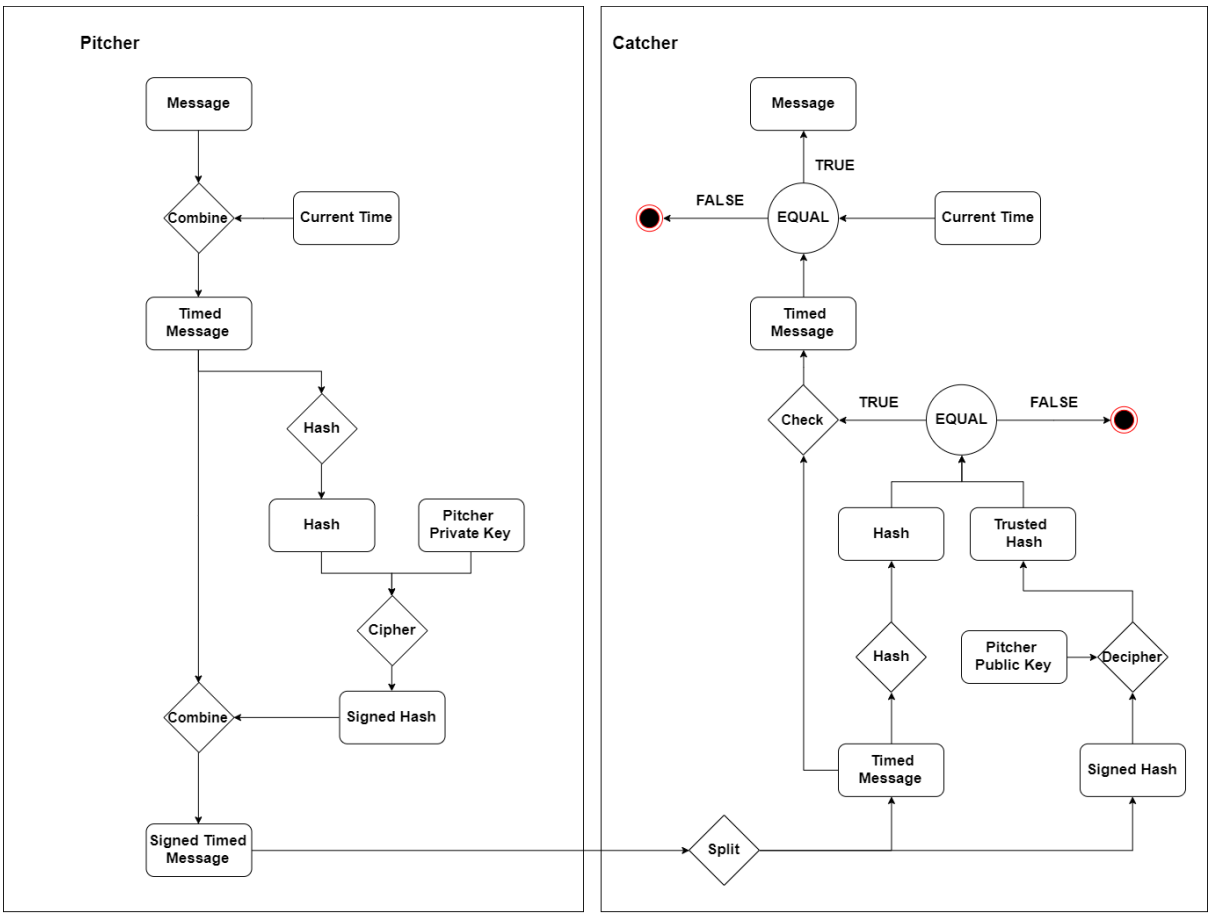
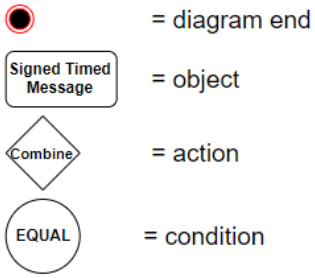


Figure 2.3 : Scheme of message transfer



Implementation of the Audit

We will generate logs to cover anomalies detection during Data Diode processes. It's very important because we will be able to know if there is a problem when we receive Data from AIS server and when data is transferred from pitcher to catcher. Therefore, we implement log generation into several parts of our Data Diode. If the packet has been sent more than 5 seconds ago or if signature verification is incorrect, we generate an alert with an error log and drop this packet. If signature verification is correct, an information log is generated.

When message is received by catcher, an info log is generated just as packet is transferred to AIS receiver.

Implementation of Availability

We assume that availability is ensure by an UPS (Uninterruptible Power Supply) when there is a power failure for a certain time. Moreover, availability is also ensure by optic fiber cable which allows a large debit and which will be not perturbed by electromagnetic field as copper cable.

Implementation of Access Control

We restrict access to AIS server with Data Diode (one-way communication). We assume that business network is segmented and Data Diode is in a secure environment. We can also assume that Data Diode has not a VPN access. So management is only possible through physical access and by administrator.
For system access control, only administrator can change configuration into catcher and pitcher servers. In addition, it is impossible to delete our log file because it's in write append (can only write to the end of the file) privilege.

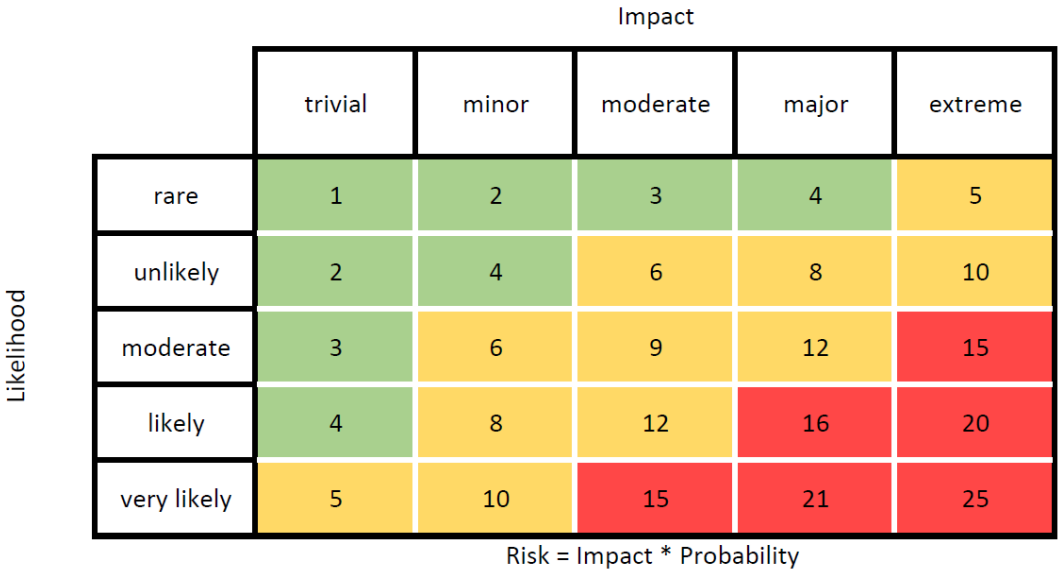
2.2 Threat and vulnerability identification

We identify threats in a STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege) grid. This process allows to map types of threats with a risk to define a vulnerability. Each type of threats has a corresponding vulnerability. Here is the corresponding list of threat and property impacted.

#	Threat	Property impacted
A	Spoofing	Authenticity
B	Tampering	Integrity
C	Repudiation	Non Repudiation
D	Information of disclosure	Confidentiality
E	Denial of service	Availability
F	Elevation of privilege	Authorization

2.3 Risk determination

We determine risk with multiplication of impact and likelihood numbers to give us a specific wafer of risk. Risk determination could have 3 valors. The different one are “low”, “medium” and “high” risks. It is defined by result of multiplication.
For example, if we take a minor (2) impact with a moderate likelihood (3), we obtain six which gives a middle risk (from 5 to 12).



2.3.1 Likelihood determination

Likelihood can be determined by several ways. And it is altered by several concepts as exposure to the threat and frequency. We must therefore ask ourselves these questions :

- Does this vulnerability is easy to exploit ?
- What is this exploit happening likelihood ?

We use a simple average mathematical calcul to have final likelihood :
Likelihood = ((exposure + frequency)/2).
We use 5 sections to classify these 2 concepts.

For exposure :

➔ rare (1) : in a secure physical/logical environment with strict policies and there is only one way to exploit it.
➔ unlikely (2) : in a secure physical/logical environment with policies.
➔ moderate (3) : in a secure physical/logical environment without policies.
➔ likely (4) : in a non-secure physical/logical environment with policies.
➔ very likely (5) : in a non-secure physical/logical environment (anyone can reach vulnerability) with no policies (anyone can exploit vulnerability).

For frequency, we assume that's an estimation per year in percentage[1] :

➔ rare (1) : < 2 %
➔ unlikely (2) : 2 - 7%
➔ moderate (3) : 7 - 20%
➔ likely (4) : 20 - 70%
➔ very likely (5) : > 70%

2.3.2 Impact analysis

To determine the impact, two questions arise :

- What damage would be caused ?
- How long the system would be impacted (the time taken by the reverse control) ?

We use a simple average mathematical calcul to have final impact :
Impact = ((damage importance + reverse control time)/2).

Sometimes we round up impact and likelihood according to type of actor (hacker, hackers group, hacktivist, competitive compagnie, malicious employee or even script kiddies) and their ability to exploit attack.

We use also 5 sections to classify impact:

➔ trivial (1) : small damage without consequences.
➔ minor (2) : moderate damage with almost no consequences.
➔ moderate (3) : moderate damage with some consequences.
➔ major (4) : irreversible damage with big consequences.
➔ extreme (5) : irreversible damage with terrible consequences.

We use also 5 sections to classify time to do reverse control :

➔ trivial (1) : < 5 minutes.
➔ minor (2) : between 5 and 29 minutes.
➔ moderate (3) : between 30 minutes and 1 hour.
➔ major (4) : between several hours and 2 days.
➔ extreme (5) : > 2 days.

2.4 Risk assessment

Risk types are divided into 5 categories. They are human, natural, hardware, software and hacking risks.

[1]https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf

When risks are determined through likelihood and impact, we use NIST (National Institute of Standards and Technology) framework to perform control base. It's divide into 5 large categories. NIST framework is implemented by several companies around the world because it's a general basis which is possible to combine with other frameworks like ISO 27000 series, CIS Critical Security Controls, PCI DSS , … . Moreover, NIST is scalable and it's a very important aspect because it can adapted in different environments.
We use also ISO 27000 of fact that it's an international standard but it's more a list of requirements such as CIS CRC (Critical Security Controls) controls which help us to define security management in us information system. We normally don't have access to other ISO 27000 standards for the simple reason that standards aren't free but we got student access on a web platform to look at them. The last framework that we decide to implement is CIS CRC.
So, we sometimes refine certain NIST categories with ISO 27000 and CIS CRC if we have a specific control to apply. We select categories and subcategories that we think appropriate in our scope and we reject controls that we don't need. We will identify as many vulnerabilities as possible. Here is the list of risky elements classified with NIST framework where, we explain for each element the vulnerability corresponding and the corrective approach to mitigate risk.

2.4.1 Human risks

2.4.1.1 Fiber cable cutting

It's possible that fiber cable is cut intentionally or not. Malicious employee or administrator could have been manipulated by an external malicious guy or do that deliberately.

For likelihood:
We estimate that exposure is moderate (3), because we assume that data diode is in a secure environment and is only reachable by authorized administrators.
We estimate that frequency is moderate (3) since it's a critical environment and some people from other governments could be interested in putting down the availability of this service.
So (3 + 3)/2 = 3 (moderate).

For impact:
We estimate that damages are moderate (3) because availability will be impacted.
We estimate that reverse control would take between 1 day and 2 days so its time is major (4).
So (3 + 4)/2 = 3,5 and we round up to 4 (major) because we assume that actors (as a competitive company, a hacker or a group of hackers) could be able to perform this attack.

Controls to apply:
According to NIST controls about Security Continuous Monitoring, it's important that physical and network activities are monitored to detect potential cybersecurity event. We assume that physical activity monitoring, setting aside fiber cables and protected cabinet are applied.
According to ISO controls about Logging and Monitoring, event logs are recording user activities , exceptions, faults, and information security events shall be produced, kept and regularly reviewed.
You could buy and put aside an optic fiber cable to avoid the shipping time and replace directly the cutted cable and also place the Data Diode in a secure cabinet.

Vulnerability	Fiber cable
STRIDE threat	Denial of service
Risk determination	Medium (12)

Actor(s)	Malicious employee or administrator
Likelihood	Moderate (3)
Impact	Major (4)
Risk goal after correction	Low
Corrective approach	Use continuously monitoring and put Data Diode into a protected cabinet. Set aside some fiber cables.
ISO/NIST/CSC controls	NIST DE.CM-1, 2, RS.MI-2; A.12.4

2.4.1.2 Fiber connectors destruction

It's possible that fiber connectors are destroyed intentionally or not. Malicious employee or administrator could have been manipulated by an external malicious guy or do that deliberately.

For likelihood:
We estimate that exposure is moderate (3), because we assume that data diode is in a secure environment and is only reachable by authorized administrators.
We estimate that frequency is moderate (3) since it's a critical environment and some people from other governments could be interested in putting down the availability of this service.
So (3 + 3)/2 = 3 (moderate).

For impact:
We estimate that damages are moderate (3) because availability will be impacted.
We estimate that reverse control takes between 1 day and 2 days so it's time it's major (4).
So (3 + 4)/2 = 3.5 and we rounded to 4 (major) because we assume that actors (as a competitive compagnie, a hacker or a group of hackers) could be able to perform this attack.

Controls to apply:
According to NIST controls about Security Continuous Monitoring, it's important that physical and network activities are monitored to detect potential malicious

event. We assume that physical activity monitoring, setting aside fiber connectors and protected cabinet are applied.
According to ISO controls about Logging and Monitoring, event logs recording user activities , exceptions, faults, and information security events shall be produced, kept and regularly reviewed.
You could set aside some fiber connectors to replace bad ones and put Data Diode in a secure cabinet.

Vulnerability	Fiber connectors
STRIDE threat	Denial of service
Risk determination	Medium (12)
Actor(s)	Malicious employee or administrator.
Likelihood	Moderate (3)
Impact	Major (4)
Risk goal after correction	Low
Corrective approach	Use continuously monitoring and put Data Diode into a protected cabinet. Set aside some fiber connectors.
ISO/NIST/CSC controls	NIST DE.CM1, 2, RS.MI-2 ; ISO A.12.4

2.4.1.3 Bad configuration

Bad configuration could conduct to availability problems or worse, to exploit which hacker would use. It's very important that our Data Diode configuration is correct. We assume that bad configuration can be from a deliberate or unconscious origin. For example, it's possible, that an Iptables configuration is wrong, an open port abnormally opened.

For likelihood:
We estimate that exposure is unlikely (2) because it's not very often that an administrator access the diode to configure it. Neither an administrator being corrupt and access the diode to deliberately modify the configuration We estimate

that frequency is unlikely (2) because administrator can be absent-minded when he configures Data Diode. Moreover, it's possible that he forgets a configuration.
So (2 + 2)/2 = 2.

For impact:
We estimate that damages are major (4) because if a malicious guy steal critical information and exploit them, it would be catastrophic for business.
We can estimate time to reverse control at more than 2 days (extreme) because it could take a while in the case that OS is completely wiped to reinstall everything, reconfigure, etc… Moreover by the nature of the diode (no usable available USB ports) to access the diode hardware.

So (4 + 5)/2 = 4,5. We round up to 5 (extreme) because we assume that actors (as a competitive compagnie, a hacker or a group of hackers) are capabilities to perform this attack.

Controls to apply:
According to NIST controls about Asset Management, it's important that organizational communication and data flow are mapped.
About Data Security, data-in-transit must be protected by cryptography and integrity checking mechanisms are used to verify information integrity.
About Security Continuous Monitoring, it's important that network activities are monitored to detect potential abnormal event. All monitoring comes configured logs on pitcher and catcher.
According to CSC controls about Controlled Use of Administrative Privileges, Minimize administrative privileges and only use administrative accounts when they are required is an idea to avoid some problems.
About Limitation and Control of Network Ports, you must ensure that only useful ports are open on Data Diode system. About Secure configuration of Network, you must use standard secure configurations.
According to ISO controls about Responsibility of assets, assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
About Media handling, media containing information shall be protected against unauthorized access, misuse or corruption during transportation.
About Access Control, an access control policy shall be established, documented and reviewed based on business and information security requirements to know who is responsible that part of information security.
About Key Management, a policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented.

About Logging and Monitoring, event logs recording user activities , exceptions, faults, and information security events shall be produced, kept and regularly reviewed.
We assume that network is segmented and that all communication of sensitive information over less-trusted networks is encrypted.
According to ISO controls about Equipment, equipment shall be correctly maintained to ensure continued availability and integrity.

Vulnerability	Catcher or pitcher configuration
STRIDE threat	S,I,D,E
Risk determination	Medium(10)
Actor(s)	hacktivist, hacker, hacker group, government spies or competitive company.
Likelihood	Unlikely (2)
Impact	Extreme (5)
Risk goal after correction	Low
Corrective approach	Use continuous monitoring. Use cryptography.
ISO/NIST/CSC controls	NIST ID.AM1, 2, 3, PR.AC4, PR.DS-2, 6, DE.CM-1, RS.MI-2; CSC 5, 9, 11; ISO A.8.1, A.8.3, A.9.1, A.10.1, A.11.2, A.12.4

2.4.1.4 Voluntary fire

It's possible that a malicious administrator or employee ignites voluntary Data Diode. It's also possible that administrator or employee are manipulated by external people as hacktivist, hacker, hacker group or government spies.

For likelihood:
We estimate that exposure is unlikely (2) because only employee or administrator could access to Data Diode. We assume that Data Diode is normally in a safe place.
We estimate that frequency is unlikely (2) since it's a critical environment and some people from other governments could be interested in putting down the availability of this service.

So (2 + 2)/2 = 2.

For impact:
We estimate that damages are extreme (5) because it's expensive to buy a new Data Diode and pay anyone to configure it. Moreover, Data Diode will be shut down. So, Denial of Service will cause perturbations.
We estimate that reverse control takes more than 2 days to to buy new devices and recreate a functional Data Diode. So reverse control time is extreme (5).
So (5+5)/2 = 5.

Controls to apply:
According to NIST controls about Awareness and Training, physical and information security personnel understand roles & responsibilities.
About Security Continuous Monitoring, it's important that network and physical activities are monitored to detect potential abnormal event.
According to CSC controls about Data Recovery Capability, it's important to ensure that pitcher and catcher systems are automatically backed up each week.
We can assume that there is a security system in data diode place which get out oxygen to stop fire.
According to ISO controls, about Secure Areas, physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
You could set aside components to recreate a Data Diode.

Vulnerability	Data Diode
STRIDE threat	Denial of service
Risk determination	Medium(10)
Actor(s)	hacktivist, hacker, hacker group or government spies.
Likelihood	Unlikely (2)
Impact	Extreme (5)
Risk goal after correction	Low
Corrective approach	Use continuously monitoring and set aside components to recreate a Data Diode.
ISO/NIST/CSC controls	NIST PR.AT-5, DE.CM-1, 2, RS.MI-2; CSC 10; ISO A.11.1

2.4.1.5 Malicious social engineering

An employee or administrator which have access to Data Diode could be manipulated (blackmail) by external people as hacktivist, hacker, hacker group or government spies, competitive company. But it's also possible that employee or administrator are victim of phishing.

For likelihood:
We estimate that exposure is moderate (3) because only authorized staff could access to Data Diode. We assume that Data Diode is in a safe place.
We estimate that frequency is moderate (3) because it's a critical environment and most people as other governments or other one is interested by critical information.
So (3 + 3)/2 = 3 (moderate).

For impact:
We estimate that damages are extreme (5) because this may conduct to business credibility and financial losses. This may also conduct to bankruptcy.
We estimate that reverse control takes more than 2 days and even impossible to reverse if damages are too important. Therefore, time to reverse control is extreme (5).
So (5 + 5)/2 = 5 (extreme).

Controls to apply:
According to NIST controls about Awareness and Training, physical and information security personnel understand roles & responsibilities.
About Data Security, data-in-transit must be protected by cryptography and integrity checking mechanisms are used to verify information integrity.
About Security Continuous Monitoring, it's important that network and physical activities are monitored to detect potential abnormal event.
According to CSC controls about Controlled Use of Administrative Privileges, Minimize administrative privileges and only use administrative accounts when they are required is an idea to avoid some problems.
About Limitation and Control of Network Ports, you must ensure that only used ports are open on pitcher and catcher systems.
About Secure configuration of Network, you must use standard secure configurations.
According to ISO controls, about Access Control, an access control policy shall be established, documented and reviewed based on business and information security requirements to know who is responsible that part of information security.
We assume that network is segmented.

Vulnerability	Employee or administrator
STRIDE threat	S,I,D,E
Risk determination	High (15)
Actor(s)	hacktivist, hacker, hacker group, government spies or competitive company.
Likelihood	Moderate (3)
Impact	Extreme (5)
Risk goal after correction	Low
Corrective approach	Use continuously monitoring
ISO/NIST/CSC controls	NIST DE.CM-1, 2, PR.AC-4, PR.AT-5, PR.DS-2, 6, RS.MI-2 ; CSC 5,9,11; ISO A.9.1

2.4.2 Natural risks

2.4.2.1 Data Diode perturbated by a flood

A flood could occur but normally we assume that Data Diode is in a secure environment and it isn't in a place where there is a water supply or a place at risk.

For likelihood:
We estimate that exposure is rare (1), because we assume that data diode is in a securely environment. A flood from too much rain isn't possible because Data Diode is in a secure environment.
We estimate that frequency is rare (1) because we assume that a tsunami is almost impossible in Belgium.
So (1 + 1)/2 = 1 (rare).

For impact:
We estimate that damages are extreme (5) because all network device will shut down and to buy new devices it would be very expensive.
We estimate that reverse control takes more than 2 days, so it's time it's extreme (5).
So (5 + 5)/2 = 5 (extreme).

Controls to apply:
According to NIST controls about Security Continuous Monitoring, it's important that network and physical activities are monitored to detect potential abnormal event.
According to CSC controls about Data Recovery Capability, it's important to ensure that pitcher and catcher systems are automatically backed up each week.
You could put Data Diode in an high place and in a secure waterproof cabinet.
According to ISO controls, about Secure Areas, physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

Vulnerability	Data Diode
STRIDE threat	Denial of service
Risk determination	Medium (5)
Actor(s)	None
Likelihood	Rare (1)
Impact	Extreme (5)

Risk goal after correction	Medium
Corrective approach	Use continuously monitoring. Otherwise, no specific correction except keep Data Diode in a raised and watertight place.
ISO/NIST/CSC controls	NIST DE.CM-1, 2, RS.MI-2; CSC 10; ISO A.11.1

2.4.2.2 Data Diode perturbated by an earthquake

It's possible that an earthquake perturbs network infrastructure and therefore, Data Diode which contains fragile cables.

For likelihood:
We estimate that exposure is rare (1), because we assume that a earthquake that could affect the data diode is from magnitude 7+ and this kind of earthquake never happened in Belgium[2].
We estimate that frequency is rare (1) because we assume that an earthquake is almost very rare in Belgium.
So (1 + 1)/2 = 1.

For impact:
If we consider a 7+ magnitude earthquake on richter scale , we estimate that damages are major (4) because all network devices will be disturbed, and services provided by Data Diode will be stopped. So, it will cost a lot of money.
We estimate that reverse control takes between 1 day and two days (major) to refurbish network devices and specially Data Diode.
So (4 + 4)/2 = 4 (major).

Controls to apply:
According to NIST controls about Security Continuous Monitoring, it's important that network and physical activities are monitored to detect potential abnormal event.
According to CSC controls about Data Recovery Capability, it's important to ensure that pitcher and catcher systems are automatically backed up each week.
According to ISO controls, about Secure Areas, physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
You could attach Data Diode with stabilizer and shock-absorber to avoid damages and put it in a secure cabinet.

[2] https://earthquaketrack.com/p/belgium/recent?mag_filter=5

Vulnerability	Data Diode
STRIDE threat	Denial of service
Risk determination	Low (4)
Actor(s)	None
Likelihood	Rare (1)
Impact	Major (4)
Risk goal after correction	Low
Corrective approach	Use continuously monitoring. Use stabilizer and shock-absorber to avoid damages.
ISO/NIST/CSC controls	NIST DE.CM-1, 2, RS.MI-2; CSC 10; ISO A.11.1

2.4.3 Hardware risks

2.4.3.1 Pitcher or catcher hard drive failure

It's possible that catcher and pitcher hard drive head is disturbed by external magnetic fields or other things which can break or damage hard drive.

For likelihood:
We estimate that exposure is unlikely (2), because we assume that data diode is in an securely environment but it's reachable by an authorized staff and we assume that Data Diode is in an environment which works as a Faraday cage, so magnetic field could only come from internal devices or employee/administrator (not deliberately).
We estimate that frequency is moderate (3) because it's a common vulnerability.
So (2 + 3)/2 = 2,5. We round down to 2 (unlikely) because we assume that actors are not going to do it intentionally.

For impact:
We estimate that damage is moderate (3). Services aren't available during a certain time, but it isn't very dangerous for business.
We estimate that reverse control takes approximately 1 hour to reinstall Data Diode system and configure it on a new hard drive. So reverse control time is major(4).
So (3 + 4)/2 = 3,5. We round down to 3 (moderate) because we assume that there aren't actors.

Controls to apply:
According to NIST controls about Security Continuous Monitoring, it's important that network and physical activities are monitored to detect potential abnormal event.
According to CSC controls about Data Recovery Capability, it's important to ensure that pitcher and catcher systems are automatically backed up each week.
According to ISO controls about Equipment, equipment shall be correctly maintained to ensure its continued availability and integrity.
About backup, backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.
About Redundancies, information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
You could set aside 1 or 2 hard drives. If it's possible, use a cluster to have high availability.

Vulnerability	Pitcher and catcher hard drive

STRIDE threat	Denial of service
Risk determination	Medium (6)
Actor(s)	None
Likelihood	Unlikely (2)
Impact	Moderate (3)
Risk goal after correction	Low
Corrective approach	Use continuously monitoring. Set aside 1 or 2 hard drives. Plan a backup every day to deploy faster Data Diode system. If it's possible, use a cluster to have high availability or use RAID technology to maintain redundancies.
ISO/NIST/CSC controls	NIST PR.MA-1, DE.CM-1, 2, RC.RP-1, RS.MI-2; CSC 10; ISO A.11.2, A.12.3, A.17.1

2.4.3.2 Data Diode overheating

It's possible that Data Diode shut down because there is an overheating caused by fans failure or bad heat dispersion because of lack of thermal paste.

For likelihood:
We estimate that exposure is unlikely (2), because normally system is thought to avoid overheating. We assume that Data Diode is in an air-conditioned place.
We estimate that frequency is unlikely (2) because we assume that it isn't common.
So (2 + 2)/2 = 2 (unlikely).

For impact:
We estimate that damages are moderate (3) because availability will be impacted.
We estimate that reverse control takes between 1 and 2 days to buy components (fan, thermal paste) and replace them. So reverse control time is major (4).
So (3 + 4)/2 = 3,5. We round down to 3 (moderate) because we assume that there aren't actors.

Controls to apply:
According to NIST controls about Security Continuous Monitoring, it's important that network and physical activities are monitored to detect potential abnormal event.
According to ISO controls about Equipment, equipment shall be correctly maintained to ensure its continued availability and integrity.
You could set aside fans to replace bad ones and keep thermal paste to change it each two years for example.

Vulnerability	Data Diode hardware
STRIDE threat	Denial of service
Risk determination	Medium (6)
Actor(s)	None
Likelihood	Unlikely (2)
Impact	Moderate (3)
Risk goal after correction	Low
Corrective approach	Use continuously monitoring. Set aside fans to replace bad ones and thermal paste to increase heat dispersion of CPUs.
ISO/NIST/CSC controls	NIST PR.MA-1, DE.CM-1, 2, RS.MI-2; ISO A.11.2

2.4.3.3 Short circuit into Data Diode

It's possible that an over voltage or a failure electronic component which cause a short circuit into Data Diode electronic.

For likelihood:
We estimate that exposure is unlikely (2), because we assume that electronic components protect is ensured at most by manufacturer.
We estimate that frequency is unlikely (2) because we assume that it isn't current.
So (2 + 2)/2 = 2 (unlikely).

For impact:

We estimate that damages are moderate (3) because because availability will be impacted.

We estimate that reverse control takes between 1 and 2 days to recreate a functional Data Diode or buy components to replace failure components. So reverse control time is major (4).
So (3 + 4)/2 = 3,5. We round down at 3 (moderate) because isn't actor with specific capabilities that we could consider.

Controls to apply:
According to NIST controls about Security Continuous Monitoring, it's important that network and physical activities are monitored to detect potential abnormal event.
According to ISO controls about Equipment, equipment shall be correctly maintained to ensure its continued availability and integrity.
You could set aside some Data Diode components to replace bad ones.

Vulnerability	Data Diode electronic
STRIDE threat	Denial of service.
Risk determination	Medium (6)
Actor(s)	None
Likelihood	Unlikely (2)
Impact	Moderate (3)
Risk goal after correction	Low
Corrective approach	Use continuously monitoring. Set aside Data Diode components.
ISO/NIST/CSC controls	NIST PR.MA-1, DE.CM1, 2, RS.MI-2; ISO A.11.2

2.4.3.4 Power failure

It's possible that there is a power failure which shut down Data Diode. It's a problem if availability is interrupted and if Data Diode doesn't stop properly.

For likelihood:

We estimate that exposure is very likely (5) because power supply is provided from outside and is accessible by everyone, but we assume that security about this and power supply availability isn't managed by us.
We estimate that frequency is likely (4) because general power failure is usual.
So (5 + 4)/2 = 4,5. We round down at 4 (likely) because there isn't actor with specific capabilities that we could consider.

For impact:
It depends that power failure time, but we can estimate impact is moderate (3) because availability is important.
We estimate that reverse control takes approximately 1 hour to restart Data Diode, so impact is moderate (3).
So (3 + 3)/2 = 3 (moderate).

Controls to apply:
According to NIST controls about Security Continuous Monitoring, it's important that network and physical activities are monitored to detect potential abnormal event.
According to ISO controls about Equipment, equipment shall be protected from power failure and other disruptions caused by failures in supporting utilities.
About Logging and Monitoring, event logs recording user activities , exceptions, faults, and information security events shall be produced, kept and regularly reviewed.
You could use an UPS to maintain critical infrastructure and switch off properly if power failure is too long.

Vulnerability	Data Diode
STRIDE threat	Denial of service
Risk determination	Medium (12)
Actor(s)	None
Likelihood	Likely (4)
Impact	Moderate (3)
Risk goal after correction	Low
Corrective approach	Use continuously monitoring. Use an UPS to maintain critical infrastructure and switch off

	properly Data Diode if power failure is too long.
ISO/NIST/CSC controls	NIST PR.MA-1, DE.CM-1, 2, RS.MI-2; ISO A.11.2, A.12.4

2.4.4 Software risks

2.4.4.1 Data congestion

It's possible that there is data congestion between catcher and pitcher at certain moments because of the size of certains packets due to long cryptographic key and signatures.

For likelihood:
We estimate that exposure is rare (1) because fiber cable debit is high and UDP protocol accelerate debit considering it is a unidirectional protocol.
We estimate that frequency is rare (1) because AIS sender can send a lot of data at a certain moment but most of the time, it is not the case.
So (1 + 1)/2 = 1 (rare).

For impact:
We estimate that damages are moderate (3) because availability is important.
We estimate that reverse control would automatically take between 5 minutes and 29 minutes, so reverse control time is minor (2).
So (3 + 2)/2 = 2,5 and we round down to 2 (minor) because we assume that there aren't malicious actors.

Controls to apply:
According to NIST controls about Security Continuous Monitoring, it's important that network activities are monitored to detect potential abnormal event. All monitoring comes configured logs on pitcher and catcher.
According to ISO controls about Logging and Monitoring, event logs recording user activities , exceptions, faults, and information security events shall be produced, kept and regularly reviewed.
There aren't many solutions, just wait to catcher stabilize data management.

Vulnerability	catcher server
STRIDE threat	Denial of service
Risk determination	Low (2)
Actor(s)	None
Likelihood	Rare (1)
Impact	Minor (2)

Risk goal after correction	Low
Corrective approach	Use continuously monitoring.
ISO/NIST/CSC controls	NIST DE.CM1, RS.MI-2; ISO A.12.4

2.4.4.2 Data loss

It's possible that data are loss during data transferring because of UDP protocol which does not verify if packet has been sent.

For likelihood:
We estimate that exposure is unlikely (2) because UDP protocol can loss packet normally with fiber cable debit and small distance, data should arrive at destination.
We estimate that frequency is rare (1).
So (2 + 1)/2 = 1,5. We round down at 1 (rare) because we assume that there isn't malicious actor.

For impact:
We estimate that damages are moderate (3) because availability is important.
We estimate that they aren't specific reverse control because if a packet is lost, packet is definitely lost but we assume that it isn't a big problem. We estimate impact on this criterion at 3 (moderate).
So (3 + 3)/2 = 3 (moderate).

Controls to apply:
According to NIST controls about Security Continuous Monitoring, it's important that network activities are monitored to detect potential abnormal event. All monitoring comes configured logs on pitcher and catcher.
We assume that some packets are lost during transferring because normally transferring is almost instant.
According to ISO controls about Logging and Monitoring, event logs recording user activities, exceptions, faults, and information security events shall be produced, kept and regularly reviewed.

Vulnerability	Data transferring
STRIDE threat	Denial of service
Risk determination	Low (3)

Actor(s)	None
Likelihood	Rare (1)
Impact	Moderate (3)
Risk goal after correction	Low
Corrective approach	Use continuously monitoring.
ISO/NIST/CSC controls	NIST DE.CM1, RS.MI-2; ISO A.12.4

2.4.5 Hacking risks

2.4.5.1 Malicious code injection

It's possible that a malicious guy finds a breach a after that inject a malicious code like a ransomware, spyware, trojan horse, malware, worm, virus into pitcher, catcher, administrator laptop or system which has access to Data Diode.

For likelihood:
We estimate that exposure is unlikely (2) because we assume that only some employees and Data Diode administrator could be a physical access to Data Diode. Logical access is normally restricted by network segmentation, protocols and policies.
We estimate that frequency is unlikely (2) because hacktivist, hacker, hacker group, government spies or competitive company must find in first an exploit or perform an attack against a target, like an employee or Data Diode administrator. Moreover, we assume that actor's capabilities can also be large.
So (2 + 2)/2 = 2 (unlikely).

For impact:
We estimate that damages are extreme (5) because this may conduct to business credibility and financial losses. This may also conduct to bankruptcy.
We estimate that reverse control takes more than 2 days and even impossible to reverse if damages are too important and not repairable. Therefore, time to reverse control is extreme (5).
So (5 + 5)/2 = 5 (extreme).

Controls to apply:
According to NIST controls about Data Security, data-in-transit must be protected by cryptography and integrity checking mechanisms are used to verify information integrity.
About Security Continuous Monitoring, it's important that network activities are monitored to detect potential abnormal event.
According to CSC controls about Controlled Use of Administrative Privileges, Minimize administrative privileges and only use administrative accounts when they are required is an idea to avoid some problems.
About Limitation and Control of Network Ports, you must ensure that only ports are open on Data Diode system.
About Secure configuration of Network, you must use standard secure configurations. Moreover, latest stable version of security updates must be installed.

According to ISO controls, about Access Control, users shall only be provided with access to the network and network services that they have been specifically authorized to use.
About protection from malware, Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
We assume that network is segmented.

Vulnerability	Pitcher, catcher, administrator laptop or any access to Data Diode.
STRIDE threat	S,I,D,E
Risk determination	Medium (10)
Actor(s)	hacktivist, hacker, hacker group, government spies or competitive company.
Likelihood	Unlikely (2)
Impact	Extreme (5)
Risk goal after correction	Low
Corrective approach	Use continuously monitoring.
ISO/NIST/CSC controls	NIST DE.CM1, PR.AC4, PR.DS-2, 6, RS.MI-2; CSC 5, 9, 11; ISO A.9.1, A.12.2

2.4.5.3 Breach exploit

An unclassified asset could conduct to let persist several breaches into network which can exploited by hackers. Here, the asset is Data Diode.

For likelihood:
We estimate that exposure is unlikely (2) because we assume that only some employees and Data Diode administrator could be a physical access to Data Diode. Logical access is normally restricted by network segmentation, protocols and policies.
We estimate that frequency is moderate (3). Exploit an unknown breach is probable because forget to classify an asset is current in a business.
So (2 + 3)/2 = 2,5. We round up at 3 (moderate) because we assume that they are several actors.

For impact:
We estimate that damages are extreme (5) because this may conduct to business credibility and financial losses. This may also conduct to bankruptcy.
We estimate that reverse control takes more than 2 days and even impossible to reverse if damages are too important and not repairable. Therefore, time to reverse control is extreme (5).
So (5 + 5)/2 = 5 (extreme).

Controls to apply:
According to NIST controls about Asset Management, it's important that organizational communication and data flow are mapped.
About Data Security, data-in-transit must be protected by cryptography and integrity checking mechanisms are used to verify information integrity.
About Security Continuous Monitoring, it's important that network activities are monitored to detect potential abnormal event.
According to CSC controls about Inventory of Authorized and Unauthorized Devices, you could maintain an asset inventory of all systems present in secure network.
About Controlled Use of Administrative Privileges, Minimize administrative privileges and only use administrative accounts when they are required is an idea to avoid some problems.
About Limitation and Control of Network Ports, you must ensure that only ports are open on Data Diode system.
About Secure configuration of Network, you must use standard secure configurations. Moreover, latest stable version of security updates must be installed.
We assume that network is segmented and that network access control through device is limited 802.1x authentication.

According to ISO controls about Responsibility of assets, assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
About Access Control, users shall only be provided with access to the network and network services that they have been specifically authorized to use.
About Logging and Monitoring, event logs recording user activities , exceptions, faults, and information security events shall be produced, kept and regularly reviewed.
We assume that network is segmented and that all communication of sensitive information over less-trusted networks is encrypted.

Vulnerability	Unclassified asset (Data Diode)
STRIDE threat	S,I,D,E
Risk determination	High (15)
Actor(s)	hacktivist, hacker, hacker group, government spies or competitive company.
Likelihood	Moderate (3)
Impact	Extreme (5)
Risk goal after correction	Low
Corrective approach	Use continuously monitoring.
ISO/NIST/CSC controls	NIST ID.AM1, 2, 3, PR.AC4, PR. DS-2, 6, DE.CM1, RS.MI-2; CSC 1, 5, 9, 11; ISO A.8.1, A.9.1, A.12.4

2.4.6 NIST categories on risk and vulnerability corresponding

Risk	Vulnerability	Identify	Protect	Detect	Respond	Recover
Human						
Cut	Fiber Cable			X	X	
Destroy	Fiber Connectors			X	X	
Bad configuration	Pitcher or catcher OS	X	X	X	X	
Voluntary fire	Data Diode		X	X	X	
Malicious social engineering	Data Diode admin or employee		X	X	X	
Natural						
Flood	Data Diode			X	X	
Earthquake	Data Diode			X	X	
Hardware						
Failure	Hard drive		X	X	X	X
Overheating	Data Diode		X	X	X	
Short Circuit	Data diode electronic		X	X	X	
Power failure	Data Diode power		X	X	X	
Software						
Data congestion	catcher server			X	X	
Data loss	Data transfer			X	X	
Hacking						

Malicious code injection	Administrator laptop, catcher or Pitcher OS		X	X	X	
Sniffing data	catcher or pitcher flows		X	X	X	
Breach exploit	Unclassified asset	X	X	X	X	

2.4.7 Attenuated risks table

Risk	Importance	Importance after controls
Human		
Fiber cable cutting	Medium (12)	Low
Fiber connectors destruction	Medium (12)	Low
Bad configuration into catcher and pitcher server	Medium (10)	Low
Voluntary fire against Data Diode	Medium (10)	Low
Malicious social engineering against Data Diode Admin or employee	High (15)	Low
Natural		
Flood on Data Diode	Medium (5)	Medium
Earthquake on Data Diode	Low (4)	Low
Hardware		
Hard drive failure	Medium (6)	Low
Data Diode overheating	Medium (6)	Low
Short Circuit into data diode electronic	Medium (6)	Low
Data Diode power failure	Medium (12)	Low
Software		
Data congestion into catcher server	Low (2)	Low
Data loss during data transferring	Low (3)	Low

Hacking		
Malicious code injection to Administrator laptop, catcher or pitcher OS	Medium (10)	Low
Breach exploit through unclassified asset	High (15)	Low

2.4.8 Stride threads summary

Element	S	T	R	I	D	E
Human						
Fiber cable cut					X	
Fiber connectors destruction					X	
Bad configuration into catcher and pitcher server	X			X	X	X
Voluntary fire against Data Diode					X	
Malicious social engineering against Data Diode Admin or employee	X			X	X	
Natural						
Flood on Data Diode					X	
Earthquake on Data Diode					X	
Hardware						
Hard drive failure					X	
Data Diode overheating					X	
Short Circuit into data diode electronic					X	
Data Diode power failure					X	
Software						
Data congestion into catcher server					X	
Data loss during data transferring					X	
Hacking						

Malicious code injection to Administrator laptop, catcher or pitcher OS	X			X	X	X
Breach exploit through unclassified asset	X			X	X	X

3. Design documentation

3.1 Physical network infrastructure

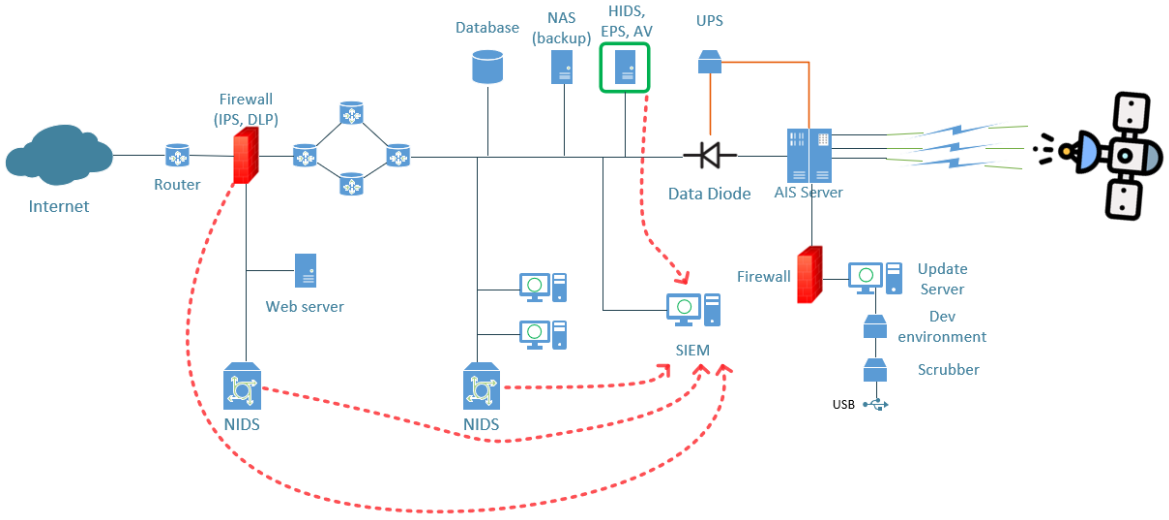


Figure 3.1 : Scheme of the physical network infrastructure

3.2 Logical network infrastructure

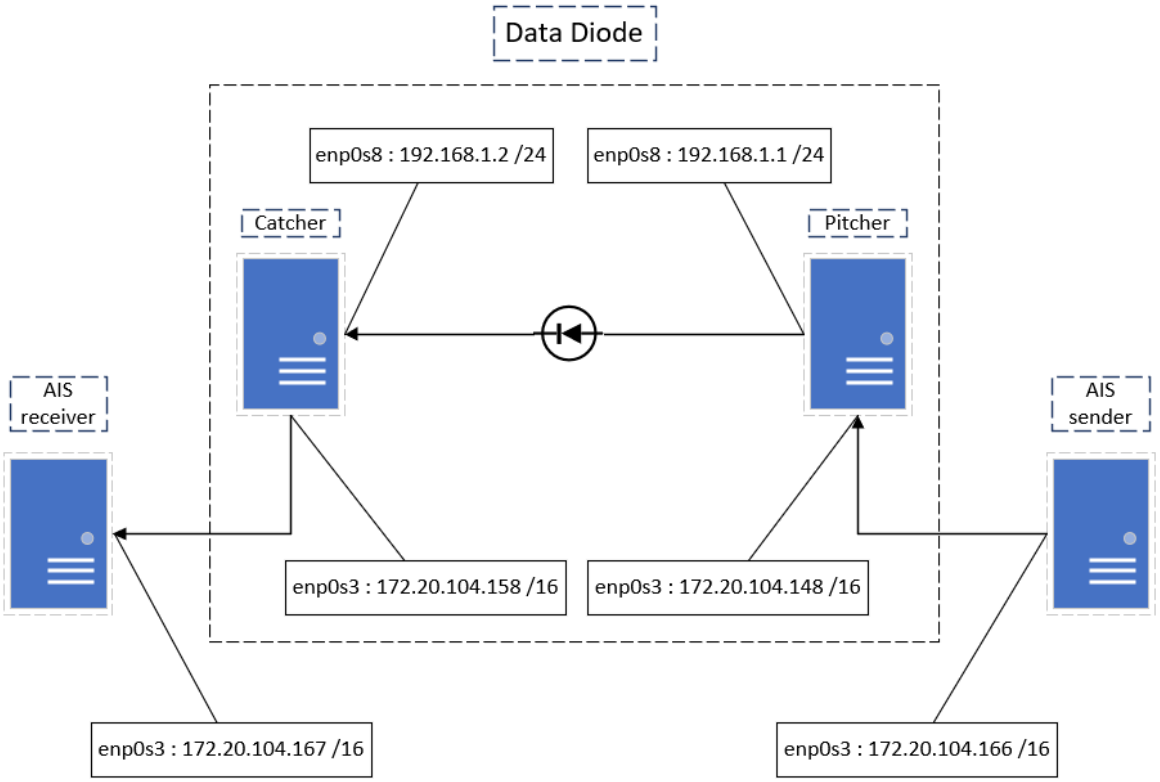


Figure 3.2 : Scheme of the logical network infrastructure

3.3 Data flow diagram

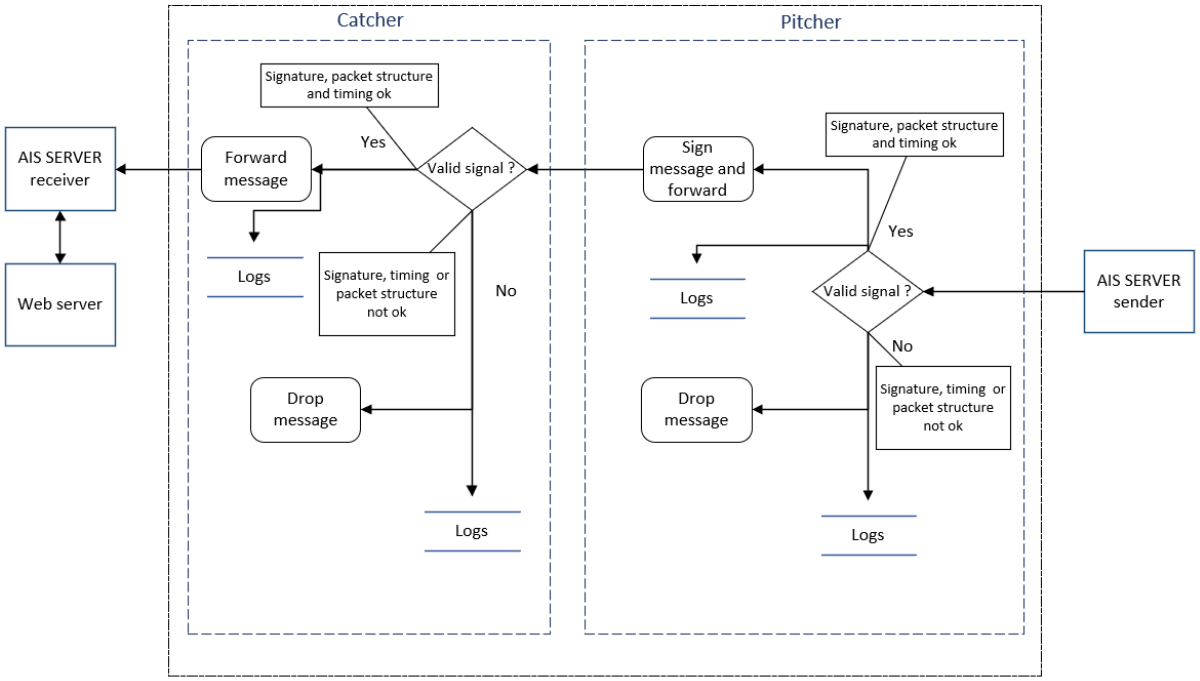


Figure 3.3 : Scheme of the network infrastructure

4. Operational documentation

4.1 Configure network interfaces

Firstly, configure the interfaces on the both servers interfaces (the ones between pitcher and catcher).

In the file /etc/network/interfaces

```
auto enp0s8
iface enp0s8 inet static
        address 192.168.1.1 (on catcher it is 192.168.1.2)
        netmask 255.255.255.0
```

Then restart networking service :

```
$sudo service networking restart
```

And check IP addresses:

```
$ip a
```

It should looks like this :

Pitcher

```
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 08:00:27:4a:a1:14 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/24 brd 192.168.1.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe4a:a114/64 scope link
       valid_lft forever preferred_lft forever
```

catcher

```
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 08:00:27:a0:53:0f brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.2/24 brd 192.168.1.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea0:530f/64 scope link
       valid_lft forever preferred_lft forever
```

4.2 Configure firewall

The first thing to do in this scope, is to DROP all packets incoming from the catcher to the pitcher. In order to do that, the Output packets from catcher (to pitcher) and the Input packets To pitcher (from catcher) are dropped.

On pitcher :

```
$sudo iptables -I INPUT 1 -i enp0s8 -j DROP
```

On catcher :

```
$sudo iptables -I OUTPUT 1 -o enp0s8 -j DROP
```

And then configure the firewall :

- Deny everything
  Putting DROP as default policy on all packet is safer. Because the administrator will only accept the packets which need to pass. There is no possibilities for the administrator to "forget" to close a port.

  ```
  $sudo iptables -P INPUT DROP
  $sudo iptables -P OUTPUT DROP
  $sudo iptables -P FORWARD DROP
  ```

- Allow SSH on 172.20.104.x interfaces (on both machines) (Only on the scope of this project, in real case it would not be here). For an actual management purpose.

  ```
  $sudo iptables -A INPUT -i enp0s3 -p tcp --dport 22 -j ACCEPT
  $sudo iptables -A OUTPUT -o enp0s3 -p tcp --sport 22 -j ACCEPT
  ```

- Pitcher
  - Allow incoming UDP packets on port 5005 from AIS Sender

    ```
    $sudo iptables -A INPUT -i enp0s3 -p udp --dport 5005 -j ACCEPT
    ```

  - Allow outgoing UDP packets on port 5005 to catcher

    ```
    $ sudo iptables -A OUTPUT -o enp0s8 -p udp --sport 5005 -j
    ACCEPT
    ```

  - Save configurations to keep data persistent. Just before, i must create a file and change these rights to save into.

    ```
    $sudo touch /etc/iptables.rules
    $sudo chmod 722 iptables.rules
    $sudo iptables-save > /etc/iptables.rules
    ```

- Catcher
  - Allow incoming UDP packets on port 5005 from pitcher

    ```
    $sudo iptables -A INPUT -i enp0s8 -p udp --dport 5005 -j ACCEPT
    ```

  - Allow outgoing UDP packets on port 5005 to AIS Receiver

    ```
    $sudo iptables -A OUTPUT -o enp0s3 -p udp --sport 5005 -j
    ```

```
ACCEPT
```

- Save configurations to keep data persistent. Just before, i must create a file and change these rights to save into.

```
$sudo touch /etc/iptables.rules
$sudo chmod 722 iptables.rules
$sudo iptables-save > /etc/iptables.rules
```

Now that only the port 5005 is open, the arp doesn't work anymore, we have to put a static address in the arp table. Using on the pitcher (supposing that 08:00:27:a0:53:0f is the @MAC of the catcher to pitcher interface on catcher):

```
$sudo arp -s 192.168.1.2 08:00:27:a0:53:0f
```

4.3 Signature and integrity

https://gitlab.cylab.be/mos-19/group02/blob/master/Pitcher/Pitcher.py
https://gitlab.cylab.be/mos-19/group02/blob/master/Catcher/Catcher.py

First ,we need to get the certificate (public key) of the AIS Sender from cylab.

```
$wget https://filetray.net/files/cylab.be/management-of-security/certificate.pem
```

```
vagrant@pitcher:~$ wget https://filetray.net/files/cylab.be/management-of-security/certificate.pem
--2019-11-22 11:25:17--  https://filetray.net/files/cylab.be/management-of-security/certificate.pem
Resolving filetray.net (filetray.net)... 5.39.78.97
Connecting to filetray.net (filetray.net)|5.39.78.97|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3926 (3.8K) [text/html]
Saving to: 'certificate.pem'

certificate.pem          100%[=================================>]   3.83K  --.-KB/s    in 0s

2019-11-22 11:25:17 (50.1 MB/s) - 'certificate.pem' saved [3926/3926]
```

Pitcher.py :
This Python code wait for incoming packets from AIS sender, check their signatures and forward them, with a timestamp and a signature, to the catcher if the signature and the format are ok.
Logs are written in the file Pitcher/activity.log

Catcher.py :

This Python code wait for incoming packets from the catcher, check the signatures and timestamp added by the pitcher then forward the original packet to the AIS receiver if everything matched.
Logs are written in the file Catcher/activity.log

Start up the programs :

```
pitcher$sudo python ~/group02/Pitcher/Pitcher.py &
```

```
catcher$sudo python  ~/group02/Catcher/Catcher.py &
```

5. Test results

5.1 Connection blocked

To check if the connection is well blocked between the two machines. We will begin with the easiest way : the PING.
As the connection should be blocked the ping should not be successful.

Ping from pitcher to catcher

```
$ping 192.168.1.2
```

```
vagrant@pitcher:~/group02/Pitcher$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 192.168.1.2 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3023ms
```

Ping from catcher to pitcher

```
$ping 192.168.1.1
```

```
vagrant@catcher:~/group02$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
```

As we can see, the both ping command doesn't work. So it proves that the ICMP packet are well blocked.
Then we should try to forward a packet on another port than the 5005. To prove that it is not only the ICMP protocol that is blocked.

5.2 Packet format on pitcher & catcher

Pitcher :
Packets incoming from the AIS sender are accepted if they have the right structure (well splitted " A , B , C ") . The packet is then forwarded to the catcher.

```
Socket: ('172.20.104.148', 5005)
(forwarded)Packet from : ('172.20.104.166', 37429) Sign:??
(forwarded)Packet from : ('172.20.104.166', 37429) Sign:??
(forwarded)Packet from : ('172.20.104.166', 37429) Sign:??
(forwarded)Packet from : ('172.20.104.166', 37429) Sign:??
(forwarded)Packet from : ('172.20.104.166', 37429) Sign:??
```

Therefore if a packet is received but the structure is not right , the packet is not (**forwarded**) to the catcher.

```
vagrant@pitcher:~/group02/Pitcher$ sudo python Pitcher.py
Socket: ('172.20.104.148', 5005)
Packet from : ('172.20.104.166', 37429) MALFORMED PACKET !
Packet from : ('172.20.104.166', 37429) MALFORMED PACKET !
Packet from : ('172.20.104.166', 37429) MALFORMED PACKET !
Packet from : ('172.20.104.166', 37429) MALFORMED PACKET !
Packet from : ('172.20.104.166', 37429) MALFORMED PACKET !
Packet from : ('172.20.104.166', 37429) MALFORMED PACKET !
```

In both cases , forwarded or not , the action taken is written in the logs.

```
2019-12-20 22:42:29,035 :: INFO :: (forwarded)Packet from : ('172.20.104.166', 37429) Sign:??
2019-12-20 22:44:50,341 :: INFO :: (forwarded)Packet from : ('172.20.104.166', 37429) Sign:??
2019-12-20 22:44:51,354 :: INFO :: (forwarded)Packet from : ('172.20.104.166', 37429) Sign:??
2019-12-20 22:44:52,360 :: INFO :: (forwarded)Packet from : ('172.20.104.166', 37429) Sign:??
2019-12-20 22:44:53,367 :: INFO :: (forwarded)Packet from : ('172.20.104.166', 37429) Sign:??
2019-12-20 22:44:54,373 :: INFO :: (forwarded)Packet from : ('172.20.104.166', 37429) Sign:??
2019-12-20 22:53:50,237 :: ERROR :: Packet from : ('172.20.104.166', 37429) MALFORMED PACKET !
2019-12-20 22:53:51,245 :: ERROR :: Packet from : ('172.20.104.166', 37429) MALFORMED PACKET !
2019-12-20 22:53:52,250 :: ERROR :: Packet from : ('172.20.104.166', 37429) MALFORMED PACKET !
2019-12-20 22:53:53,256 :: ERROR :: Packet from : ('172.20.104.166', 37429) MALFORMED PACKET !
2019-12-20 22:53:54,266 :: ERROR :: Packet from : ('172.20.104.166', 37429) MALFORMED PACKET !
2019-12-20 22:53:55,287 :: ERROR :: Packet from : ('172.20.104.166', 37429) MALFORMED PACKET !
```

Catcher :

Packets incoming from the pitcher are accepted if they have the right structure (well splitted " A , B ") . The packet is then forwarded to the AIS receiver.

```
Socket: ('192.168.1.2', 5005)
(forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
```

Therefore if a packet is received but the structure is not right , the packet is not (**forwarded**) to the AIS receiver.

```
Socket: ('192.168.1.2', 5005)
Packet from : ('192.168.1.1', 60905) MALFORMED PACKET !
Packet from : ('192.168.1.1', 60905) MALFORMED PACKET !
Packet from : ('192.168.1.1', 60905) MALFORMED PACKET !
Packet from : ('192.168.1.1', 60905) MALFORMED PACKET !
Packet from : ('192.168.1.1', 60905) MALFORMED PACKET !
Packet from : ('192.168.1.1', 60905) MALFORMED PACKET !
```

In both cases , forwarded or not , the action taken is written in the logs.

```
2019-12-20 22:19:38,049 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
2019-12-20 22:19:39,059 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
2019-12-20 22:19:40,069 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
2019-12-20 22:19:41,078 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
2019-12-20 22:19:42,083 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
2019-12-20 22:19:43,100 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
2019-12-20 22:19:44,116 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 60905) , Sign:OK|Time:OK
2019-12-20 22:21:16,105 :: ERROR :: Packet from : ('192.168.1.1', 60905) MALFORMED PACKET !
2019-12-20 22:21:17,121 :: ERROR :: Packet from : ('192.168.1.1', 60905) MALFORMED PACKET !
2019-12-20 22:21:18,124 :: ERROR :: Packet from : ('192.168.1.1', 60905) MALFORMED PACKET !
2019-12-20 22:21:19,143 :: ERROR :: Packet from : ('192.168.1.1', 60905) MALFORMED PACKET !
2019-12-20 22:21:20,156 :: ERROR :: Packet from : ('192.168.1.1', 60905) MALFORMED PACKET !
2019-12-20 22:21:21,162 :: ERROR :: Packet from : ('192.168.1.1', 60905) MALFORMED PACKET !
```

5.3 AIS sender signature

We were not able to check the signature of the AIS sender on the packet. This is due to the lack of info on what is hashed and signed and encoded.

5.4 Pitcher signature + packet integrity

Packets incoming from the pitcher are accepted if they have the right signature (If B is the signed hash of the message A : " A , B ") . The packet is then forwarded to the AIS receiver if the signature match the pitcher public key.

```
Socket: ('192.168.1.2', 5005)
(forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
```

Therefore packets incoming from the pitcher are not accepted if they do not have the right signature (If B is not the signed hash of the message A : " A , B ") . The packet is not (**forwarded**) to the AIS receiver if the signature / hash does not match the pitcher public key / message.

```
vagrant@catcher:~/group02/Catcher$ sudo python Catcher.py
Socket: ('192.168.1.2', 5005)
Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
```

In both cases , forwarded or not , the action taken is written in the logs.

```
2019-12-20 21:36:27,795 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
2019-12-20 21:36:28,802 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
2019-12-20 21:36:29,811 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
2019-12-20 21:36:30,826 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
2019-12-20 21:36:31,832 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
2019-12-20 21:36:32,838 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
2019-12-20 21:36:33,855 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
2019-12-20 21:36:34,861 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 57120) , Sign:OK|Time:OK
2019-12-20 21:38:08,834 :: ERROR :: Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
2019-12-20 21:38:09,839 :: ERROR :: Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
2019-12-20 21:38:10,843 :: ERROR :: Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
2019-12-20 21:38:11,851 :: ERROR :: Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
2019-12-20 21:38:12,858 :: ERROR :: Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
2019-12-20 21:38:13,862 :: ERROR :: Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
2019-12-20 21:38:14,868 :: ERROR :: Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
2019-12-20 21:38:15,875 :: ERROR :: Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
2019-12-20 21:38:16,880 :: ERROR :: Packet from : ('192.168.1.1', 50137) , Sign:!!NOK!!
```

5.5 Time check

Packet incoming from the pitcher , within a time span of 5 second from the current time , are accepted by the catcher and (**forwarded**) to the AIS receiver.

```
vagrant@catcher:~/group02/Catcher$ sudo python Catcher.py
Socket: ('192.168.1.2', 5005)
(forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
(forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
```

Therefore if a packet is received but the time difference between the current time and the time in the packet is more than 5 second , the packet is not forwarded.

```
vagrant@catcher:~/group02/Catcher$ sudo python Catcher.py
Socket: ('192.168.1.2', 5005)
Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
```

In both cases , forwarded or not , the action taken is written in the logs.

```
2019-12-20 21:20:34,906 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
2019-12-20 21:20:35,911 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
2019-12-20 21:20:36,919 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
2019-12-20 21:20:37,926 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
2019-12-20 21:20:38,933 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
2019-12-20 21:20:39,939 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
2019-12-20 21:20:40,946 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
2019-12-20 21:20:41,952 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
2019-12-20 21:20:42,959 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
2019-12-20 21:20:43,968 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
2019-12-20 21:20:44,973 :: INFO :: (forwarded)Packet from : ('192.168.1.1', 37519) , Sign:OK|Time:OK
2019-12-20 21:27:31,658 :: ERROR :: Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
2019-12-20 21:27:32,663 :: ERROR :: Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
2019-12-20 21:27:33,681 :: ERROR :: Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
2019-12-20 21:27:34,687 :: ERROR :: Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
2019-12-20 21:27:35,693 :: ERROR :: Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
2019-12-20 21:27:36,701 :: ERROR :: Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
2019-12-20 21:27:37,708 :: ERROR :: Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
2019-12-20 21:27:38,718 :: ERROR :: Packet from : ('192.168.1.1', 46824) , Sign:OK|Time:!!NOK!!
```

5.5 AIS receiver acknowledgement

```
vagrant@catcher:~/group02/Catcher$ curl 172.20.104.167/report.json
{
    "last_message": {
        "172.20.104.158": 2523924,
        "172.20.104.159": 2523403,
        "172.20.104.161": 2524289,
        "172.20.104.162": 2524289,
        "172.20.104.166": 2524289
    },
    "time": 1576874957
```

6. Security target (Common Criteria)

6.1. Introduction

6.1.1 ST Reference

- Title: Data Diode for GASP Security
- ST Version: 1.0
- ST Date : 21/12/2019
- Authors : Aranibar Mondragon Vladimir, Tchiagou Tékédo Loïc, Croche Loïc, Cochez Benjamin and Hanquin Benjamin

6.1.2 TOE Reference

TOE Name : Data Diode
Version 1.0

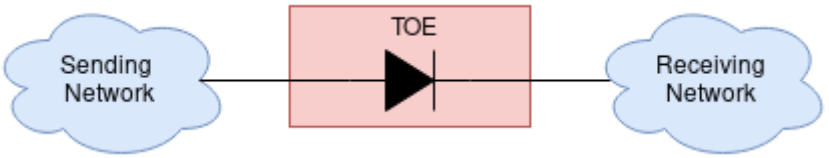
6.1.3 TOE Overview

6.1.3.1 TOE Type

The Target of Evaluation (TOE) is a network gateway that ensures physical layer only one-way data transmission through the TOE .

So the goal is to connect two different networks. Informations and data are able to go through the TOE from the Sending Network to the Receiving one, but not in the opposite way. While obviously ensuring the data integrity.

In our case, we will name the Sending Network as the High Network and the Receiving is the Low Network.



This TOE can address two security problem :

- Prevent information leak from Low Network to High Network.
- Prevent the corruption of any data in the High network from the Low Network.

The final goal of this TOE is to send data from an AIS Sender to an AIS Receiver while ensuring the data integrity.

6.1.4 TOE Description

6.1.4.1 Physical Scope

The TOE is composed of two servers, separated by an optical fiber (one way (not duplex)) with a light emitter on the High Network (optical transmitter) and a light receiver on the Low Network.

In the scope of this project, the two servers are simulated by two VMs (virtual machine). The connexion between them is not under our supervision.

6.1.4.2 Software Scope

Each server is using Ubuntu 16.04.6 LTS as Operating System.

6.2.4.3 Logical Scope

When the Sending server send data over the optic fiber (light go through the fiber), the receptor of the Receiver server get the data. And this is the only way for this server to receive data, all other input interfaces must be blocked.

6.2 Conformance Claims

The TOE and ST are compliant with the Common Criteria (CC) version 3.1 revision 5 (April 2017). This TOE and Security Target is CC part 2 and 3 conformant, with a claimed Evaluation Assurance Level of EAL4.

6.3 Security Problem Definition

6.3.1 Threats

T.OPPOSITE_WAY
Something (user,process,...) from the Low Network breaches the TOE by sending data to the High Network.

T.INTEGRITY
The data has been modified between the High Network and the Low Network.

T.REPUDIATION
The data are not send from the High Network but from another source.

6.3.2 Organizational Security Policies (OSP)

P.TR_USER

The users of the TOE are trusted and trained. They are well-trained and the organization shall trust that he is not malicious.

6.3.3 Assumptions

A.CONTROLLED_PHYSICAL_ACCESS
The TOE shall be installed in a secure place which is access controlled to authorize only authorized users.

A.NETWORK
The TOE is the only way to send data between the High Network and the Low Network, there shall not be other network connection between them.

6.4 Security Objectives

6.4.1 Security Objectives for the TOE

O.ONLY_ONE_WAY
The TOE shall allow the data to flow only from the High Network to the Low Network but not in the opposite way.

O.INTEGRITY
The TOE shall ensure that the data integrity is keeped.

O.CHECK_SIGNATURE
The Low Network shall check the signature of the received data, and verify if it correspond to the High Network signature.

6.4.2 Security Objectives for the Operational Environment

OE.TR_USER
The users of the TOE are trusted and trained. They are well-trained and the organization shall trust that he is not malicious.

OE.PHYSICAL_CONTROL
The TOE shall be installed in a secure place which is access controlled to authorize only authorized users.

OE.NETWORK
The TOE is the only way to send data between the High Network and the Low Network, there shall not be other network connection between them.

6.4.3 Security Objectives Rationale

Threats and assumptions ---------- Security Objectives	T.OPPOSITE_WAY	T.INTEGRITY	T.REPUDIATION	P.TR_USER	A.CONTROLLED_PHYSICAL_ACCESS	A.NETWORK
O.ONLY_ONE_WAY	X					
O.INTEGRITY		X				
O.CHECK_SIGNATURE			X			
OE.TR_USER				X		
OE.PHYSICAL_CONTROL					X	
OE.NETWORK	X					X

T.OPPOSITE_WAY

O.ONLY_ONE_WAY

O.ONLY_ONE_WAY ensures that data is only allowed to flow from High Network to Low Network but not in the opposite direction.

OE.NETWORK ensure that the only possible connection between the High Network and the Low Network is by the TOE. And ensuring this, it ensure that it is the only way. Combined with O.ONLY_ONE_WAY it ensure that the only possible way is in this way, and in the good direction from the High to Low Network as needed.

T.REPUDIATION

The information shall be reliable, thus the information is signed in the High Network, and to verify that the information come from this Network, a check on the signature is done.

O.CHECK_SIGNATURE directly upholds T.REPUDIATION

T.INTEGRITY

The information shall be reliable, thus the information shall not be modified between the High Network and the Low one. The integrity is checked at the signature.

O.INTEGRITY directly upholds T.INTEGRITY

P.TR_USER
The users shall not maliciously (or not) compromise the security functionality of the TOE, while using a bad procedure (i.e install the optic fiber in the wrong way). The user shall comply to the operating procedures stipulated in the user guidance.

OE.TR_USER directly upholds A.USER.

A.CONTROLLED_PHYSICAL_ACCESS
Assumption is made that the TOE is located in a secure environment where there is physical access control.

OE.PHYSICAL_CONTROL directly upholds
A.CONTROLLED_PHYSICAL_ACCESS.

A.NETWORK
Assumption is made that there is no other connection between the High Network and the Low Network possible than the TOE.

OE.NETWORK directly upholds A.NETWORK

6.5 Extended Components Definition
No additional extended components are needed and therefore none are defined.

6.6 Security Requirements

6.6.1 Security Functional Requirements

6.6.1.1 User Data Protection (FDP)

6.6.1.1.1 Information Flow Control Policy (FDP_IFC)
There is a complete information flow control. So FDP_IFC.2 shall be used.

FDP_IFC.2.1 : The TSF shall enforce the only one way data flow on every information from the High Network to the Low Network and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.6.1.1.2 Information Flow Control (FDP_IFF)

FDP_IFF.1.1 The TSF shall enforce the only one way data flow based on the following types of subject and information security attributes: High Network and Low Network

FDP_IFF.1.4 The TSF shall explicitly authorise an information
flow based on the following rules:

- If the High Network want to send data to the Low Network.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow
based on the following rules:

- If the Low Network want to send data to the High Network.
- If the Low Network get information from another interface than the one connected from the High Network.
- If the High Network send information to another interface than the one connected to the Low Network.

6.6.1.2 Cryptographic support (FCS)

6.6.1.2.1 Cryptographic operation (FCS_COP)

FCS_COP.1.1
The TSF shall perform an *asymmetric encryption* in accordance with a specified cryptographic algorithm SHA and cryptographic key sizes of 256 bits.

6.6.1.3 Communication (FCO)

6.6.1.3.1 Non-repudiation of origin (FCO_NRO)

FCO_NRO.1.2 The TSF shall be able to relate that the originator of the information is the High Network.

6.6.2 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 4.
These requirements are listed in the following table[3] :

[3] Found on https://www.commoncriteriaportal.org/cc/ in CCPART3V3.1R5.pdf

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

6.6.3 Security Requirements Rationale

Security Objectives ---------- SFR	O.ONLY_ONE_WAY	O.INTEGRITY	O.CHECK_SIGNATURE
FDP_IFC.2	X		
FDP_IFF.1	X		
FCS_COP1.1		X	
FCO_NRO1.2			X

6.7 TOE Summary Specifications

The TOE addresses multiple security functional requirements : FDP_IFC.2, FDP_IFF.1, FCS_COP1.1, FCO_NRO1.2. They work together to satisfy the security objective for TOE. The following provides a description of the general mechanisms that the TOE uses to satisfy each SFR defined.

FDP_IFC.2 & FDP_IFF.1
The TOE is connected by a *one way* optic fiber. It means that on the High Network there is an optical transmitter (which is not on the Low Network). And on the Low Network, there is an optical receiver (which is not on the High Network). It means that even if, the Low Network could logically send data to the High Network it would not be physically possible.

And there shall not be any other connection between the High and Low Network other than through the TOE.

FCS_COP1.1
The message received from the High Network combined with the current time will be hashed using SHA-256. We send the message across the TOE.

The Low network will receive both of signed hash and message. The signed hash will be verified and compared to the received message hash using the public key certificate. If the hash is successfully identified as coming from the High network and if the both hashes match.

FCO_NRO1.2
The High Network sign the information to ensure the non-repudiation. When the Low Network receive some data, it must check if the signature is valid.