EUREKA

ITEA3

MIRAI

MACHINE INTELLIGENCE FOR IOT AND EDGE

Machine Intelligence for Smart and Sustainable Planning and Operation of IoT and Edge

D1.2 KPI Framework

Work Package	WP1
Dissemination level	Public
Status	Final
Date	June 2021
Deliverable leader	Eliar
Potential Contributors	All

Contributors

Names	Organisation
Sencer Sultanoğlu	Eliar
Barış Bulut, Burak Ketmen	Enforma
Julien Deckx	3E
Geert Vanstraelen	Macq

Reviewers

Names	Organisation
Joana Sousa	NOS
Pedro Miguel Salgueiro Santos	ISEP

Table of Contents

Abbreviations

AI	Artificial Intelligence
ANPR	Automatic number-plate recognition
AWS	Amazon Web Services
CPE	Consumer Premises Equipment
FoV	Field of View
HD	High Definition
KPIs	Key Performance Indicators
Mbps	Megabits per second
OSI Model	Open Systems Interconnection
SLAs	Service Level Agreements
VGA	Video Graphics Array

Executive Summary

This deliverable is driven by the project's Task 1.2: Service levels and key performance indicators. It is the first version of what is basically a two-version deliverable, with the second version scheduled in 13 months after the first one. The outputs of this task and deliverable contribute to work package 4, in particular Tasks 4.1-3.

Following deliberations with the project consortium, it was concluded that the scope of the deliverable should include only Key Performance Indicators (KPIs) and not Service Level Agreements (SLAs). This is because KPIs are needed to gauge the success of an activity or a project in general, whereas SLAs are more for customer-service provider relations, and that is out of scope of MIRAI.

The methodology based on which whether a particular KPI is met can vary based on the type of the KPI. For a KPI which is based on a physical value such as bandwidth utilisation, duration, rate, performance and so on, the detection is straightforward since it is also based on requesting the value from the system. For softer KPIs such as Market Access and TRL, corresponding definitions must be used to evaluate if a certain criteria is met.

In MIRAI's project, there will be a system or systems distributed on different nodes in a network and potentially across different organizations. In order to evaluate the performance of the distributed system, a set of key performance indicators (KPIs) are needed to evaluate a configuration.

The underlying objectives of Task 1.2 aims to perform the carry out the following actions:

- Elicit and define suitable KPIs, which should be support in the MIRAI solution
- Identify and define relevant context factors such as bandwidth and trustability of nodes in a distributed system.

1. Key Performance Indicators (KPIs)

MIRAI's project has a relatively use case rich consortium despite its relatively small-to-medium size, with 5 use cases from different technical verticals.

This section presents the key performance indicators for each of the 5 use cases within the project, namely:

- Use case 1: Distributed renewable energy systems (UC owner: 3E)
- Use case 2: Secure Internet provisioning (UC owner: NOS)
- Use case 3: Traffic management (UC owner: Macq)
- Use case 4: Water management (UC owner: Shayp)
- Use case 5: Continuous auto configuration of industrial controllers at edge (UC owner: Eliar & Enforma)

A detailed documentation of the above use cases is presented under Section 2 of Deliverable 1.1.

The KPIs were grouped by use cases, where each group of KPIs is listed by the corresponding use case owner. The important thing is to have a KPI attribute which is meaningful to the technology and business, and is measurable (preferably both now and at the end of the project).

1.1. UC1 ("Distributed renewable energy systems")

KPI	Now	Target	Measurement Method
Granularity of data	1min	1s	N/A
Update rate of data	5min	1s	N/A
Response time to control signal	N/A	5s	Communication delay + Plant response time

Network utilisation (5MW plant)	<<1Mbps	≤ 1Mbps	The network load measured by Network Monitor tools is an indicator of the network utilization.
Availability	99.8%	99.9%	The ratio of the system uptime to total time
Configuration person-hours (5MW plant)	3h	15min	Plant configuration and integration time in SynaptiQ

1.2. UC2 ("Secure Internet provisioning")

KPI	Now	Target	Measurement Method
Traffic Monitoring period	-	Always-on.	Extract timestamp when a packet is captured at CPE and when it arrives at the cloud: Monitor_period=Tcloud – Tcapture Check at regular times that packets are arriving at the cloud.
Smart and customized protection	-	Three profiles should be created: Normal Client, IoT Client and Gamer Client.	Train the system with a given profile. Then completely change the profile that is being used. Check the effects of the solution
Layers of the OSI model to be analysed	-	System should detect attacks in OSI layer 3,4 and 7 (100% detection rate)	Use different types of threats that affect different layers of the OSI model. For example, an ICMP flood can be used to measure the network layer performance, a TCP fragmented attack can be used to measure the transport layer performance, and an HTTP flood attack to measure the application layer performance.
Type of DDoS attacks to be mitigated	Firewall rules to mitigate some attacks (ICMP flood)	Protection against flood, amplifier and fragmented attacks.	Perform different attacks and evaluate how the system behaves. Check if the defence mechanism is able to detect the attack, if the home network of the client was successfully protected and if the system was able to quarantine the infected devices.
Report	-	For every alert, a report shall be generated and contain the type of attack and the time when it happened.	For every alert a report must beavailable.
Alerts	-	The alert should take less then 1s to be generated and sent to the victim.	Perform an attack and check if, after the detection of the attack, an alert is generated. Take timestamps from

			when the alert is generated and when it arrives at the user.
Detection Speed	-	< 5 seconds	A test bench should be used to generate an attack. When the attack starts a timestamp is taken. Then when the edge node detects the attack, another timestamp is taken. It is then possible to measure the time that the system took to detect an ongoing attack.
Multi Platforms	-	Priority: Google Cloud and AWS Nice to have: Azure.	Repeat all the process that took place in Google Cloud to the other clouds.
Service Recovery Time	-	The CPU usage during an attack cannot reach 100% systematically. Memory usage cannot make the router unusable.	When the edge node is under attack a serious of metrics such as, the internet speed connection, the gigabit connection and the responsiveness of the CPE interface should be measured. A measurement of the CPU and memory usage could be useful to indicate how the CPE handles an attack.
Operationally unavailable (optional, requires analyses).	-	The system should continue to monitor and detect attacks when the network is not available.	Perform a test without an internet connection (no cloud access). Then start an attack and check if the CPE is able to detect the infected device and quarantine the device in question.
Loss of performance	-	The performance of the CPE cannot be affected. The internet speed shall be the same with or without the MIRAI mechanism.	When the monitoring system is implemented on the CPE a series of tests should be performed such as responsiveness of the CPE, checking for interference with other modules, internet speed test, gigabit availability and resources used.
Router restarting	NOS already monitors the number of reboots.	The project shall not increase the number of reboots. The detection mechanism should be resilient to avoid reboots.	During the tests performed for the MIRAI project, if a reboot of the CPE happens it should be thoroughly investigated. If the investigation finds out that the cause is related with the MIRAI defence mechanism the problem leading to the reboot should be solved.
Detection of infected CPE	-	A variation in 10% of the CPU usage and memory should trigger an alert of a possible ongoing attack. If a CPE is being used to	Use the CPE in a way that does not correspond to the profile created (for example, using a tool to stress the CPU and memory). Verify if the system

		search the web shall trigger the system	is able to detect the anomalous behaviour.
Accuracy of the Machine Learning Algorithm.	-	False positive and true negative rates should be low (less or equal to <5%).	Use different malicious datasets/attacks and measure the efficiency of the machine learning algorithm.

1.3. UC3 ("Traffic management")

KPI	Now	Target	Measurement Method
Reaction time	Depending on the load	100 ms	Difference between image timestamp and message timestamp
Effective framerate	10 fps	30 fps	The framerate is a sensor parameter. To measure if it is effective the dropped frame count should be close to zero.
Actual FoV	416 x41 6	Covering half of 5MP image	The ROI is a configuration of the camera. It must be verified that all frames are handled and the object detections work on all parts of the configured ROI.
Graceful degradation	No	Yes	Observe the working of the system in following scenario's: • one of the camera's powered off • removed network cable • camera operational but sensor covered • camera moved outside the region The cameras are not redundant. Installing two cameras that see the same scene would be more expensive than what customers would pay for the additional up time.
Communication maintaining privacy	No [100%]	Yes 100%	Assessment of the protocol(s) used between MFBB that reside on different edge devices or backend servers. Assessment that exchanged data is necessary for the functional needs of the application. For each protocol the values are binary. There can be more than one interface exposing data. Minimizing the number of attack surfaces is an overall security goal for the edge devices that not only concerns privacy.
Number of supported kinds of sensor data	1	6	To be counted but also evaluate how data is stored after fusion
Bandwidth needed for communication relative to generated raw data.	Not available	0.1	Volume communicated data divided by Volume raw data
Time synchronisation accuracy	10 ms	1 ms	NTP Measurements

Accuracy of timestamps on data	10 ms	5 ms	Compare with time info injected at the source (for instance a precision clock visible in the image)
Use of a common framework like MIRAI.	No	Yes	Assessment
Pool of distributed collaborating cameras	No	Yes	Assessment
Number of different countries the distributed AI enabled product is marketed to.	For distributed systems: 0	5 countries	Assessment of market penetration at the end of the project and 3 years after the end of the project
TRL	3-4	6-7	Assessment

Notes on “Graceful degradation”: In case of a failure on one of the distributed cameras the system as a whole will continue to operate. Failure does not only mean a hardware or software failure but also occlusion of the camera’s sight or blinded by direct sun light.

Notes on “Communication maintaining privacy”: All communications involving sensitive data between components of the MIRAI framework are secured. Depending on the application privacy sensitive information will or will not leave the camera. On one side of the spectrum, we have license plate (ANPR) information with a visible picture of the car and his driver using a cell phone and not wearing his safety belt. There are however also a lot of applications where we don’t need this and where cameras are only accepted if they don’t send nor store privacy sensitive information. This becomes more complicated when in the case of a cooperating distributed edge camera system they need to share intermediate calculation results. We need a new data sharing protocol where both from the data and the communication protocol point of view privacy and security are guaranteed.

Notes on “Number of supported kinds of sensor data”: The MFBB must support data from various type of heterogeneous sensors such as:

- Colour
- B&W
- Thermal
- Time of Flight
- Radar
- Sound

Notes on “Bandwidth needed for communication relative to generated raw data”. Considering static images, the range is from 6 Mbyte (2 Mpixels images) to 24Mbyte (8 Mpixels image). Considering video streaming a VGA camera consumes 7.1Mbit/sec and a FullHD camera consumes 48Mb/s. The current generation of cameras already does all calculations on the edge and only sends the final results to the backend system in the cloud. This is a multiple times one camera to the cloud architecture. We want to extend this to a multiple time multiple (distributed) camera to the cloud model. The distributed cameras will share intermediate results, which are optimized to reduce the communication bandwidth and balance the calculation power. The communication resources used must be more than 10 times less than the raw data.

Notes on "Time synchronisation accuracy": Correct time synchronization between the systems is important to allow data fusion of intermediate results from the different components."

Notes on "Use of a common framework like MIRAI": In the current state of the art integrating third party components heavily weights on the used computational resources because each component has a tendency to be as standalone as possible. A framework where those components can share intermediate results would be beneficial to the system as a whole. Macq has co-creative relationships with the 'third' party component manufactures. If they adapt to the MFBB more components could cohabit offering more functionality to the end-user and more market offerings for Macq and his third-party suppliers.

1.4. UC4 ("Water management")

KPI	Now	Target	Measurement Method
Device lifetime	10 years	16 years	Not provided
Anomaly detection time for households	1-3 hours	< 1 hour	Not provided
Anomaly detection time for corporate buildings	3-24 hours	< 3 hours	Not provided
Pattern recognition at the edge	-	Anomalies	Not provided
Field test validation of anomaly detection (TRL 7)	-	1	Not provided
Device firmware remote update to support new patterns	-	1	Not provided

1.5. UC5 ("Continuous auto configuration of industrial controllers at edge")

KPI	Now	Target	Measurement Method
Percentage overshoot in closed-loop temperature control (*process*)	3%	2%	At least 50 instances of temperature control phase data will be analysed from collected process values
Percentage of processes with oscillatory and/or unstable behaviour (*process*)	1%	0%	At least 50 instances of temperature control phase data will be analysed from collected process values
Percentage of processes getting to setpoint in time (*process*)	99%	100%	At least 50 instances of temperature control phase data will be analysed from collected process values
Number of {Attribute, edge device} that will be handled by distributed AI algorithms (*distributed AI; horizontal scaling*)	{0, 0}	{100, 30}	Counting T7701ex edge devices and attributes
Number of TRL-7 validated systems using distributed AI (*system*)	0	1	Validation at a dyehouse.

Average CPU utilisation of T7701ex (*edge device*) (*distributed AI; horizontal scaling*)	25%	≤ %35	Collecting CPU usage trends at least once a day.
Network utilisation (*distributed AI; horizontal scaling*)	~3.6Kbps	≤ 100Kbps	Using network monitoring tools.
Steam source being allocated according to an algorithm instead of first come first served (*process*) (*distributed AI; horizontal scaling*)	-	Present	n/a

2. Conclusions

In a distributed Artificial Intelligence (AI) environment, in order to evaluate where in the network to distribute the computation, a set of key performance indicators (KPIs) are needed to evaluate a configuration. This report successfully presents the various KPIs that are relevant and meaningful for each of the 5 use cases in project MIRAI.

This deliverable was driven by the project's Task 1.2: Service levels and key performance indicators, being the first version of what will basically become a two-version deliverable, with the sequel scheduled 13 months after the first one. The outputs of this task and deliverable is aimed to contribute to work package 4, in particular Tasks 4.1-3. Following deliberations with the project consortium, it was concluded that the scope of the deliverable should include only the KPIs and not the SLAs, since KPIs are needed to gauge the success of an activity or a project in general, whereas SLAs are more for customer-service provider relations, and that is out of scope of MIRAI.