Applying STPA to improve the satellite security using Dense Neural Network e PNL

LA STAMP WORKSHOP 2024

Wagner dos Santos Clementino de Jesus (Univap/Unifesp)
Carlos Henrique Netto Lahoz (Univap/ITA)
Luiz Eduardo Galvão Martins (Unifesp)

INTRODUCTION

Space systems, such as Satellites, Rockets, Telescopes and Space Probes, increasingly demand safe/security against a variety of threats (Tsamis, 2021).

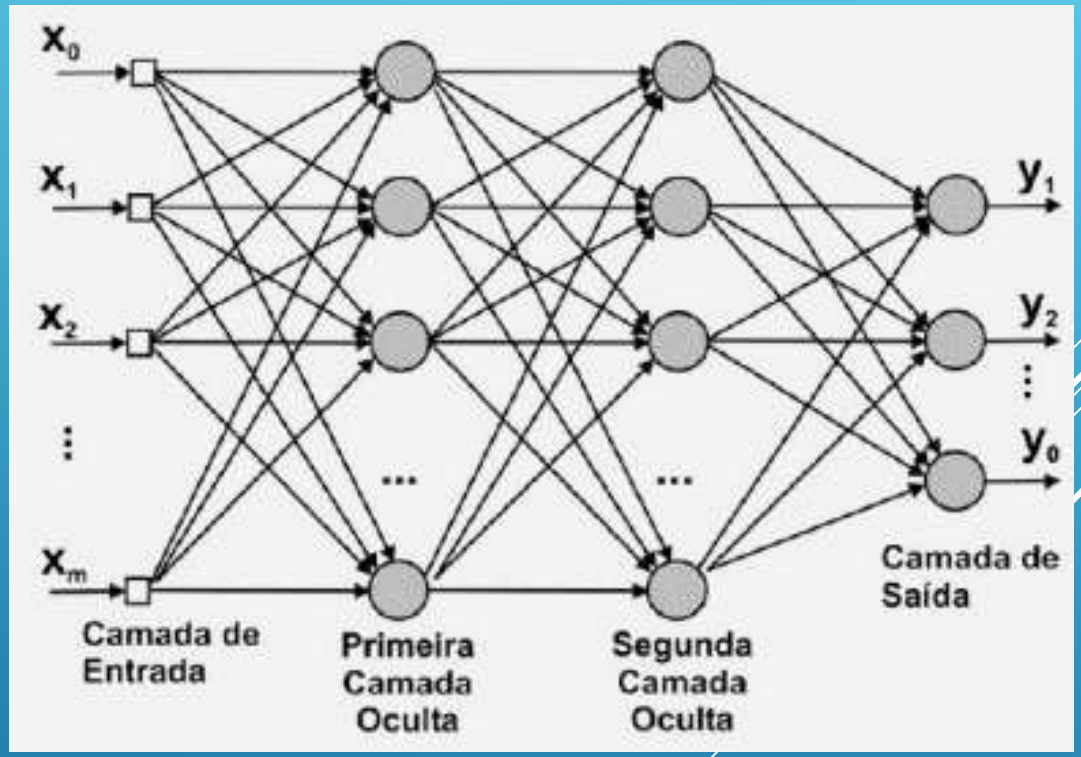
One way to support STPA in complex scenarios is to use AI algorithms like Dense Neural Networks

Forward Pass Dense Networks: Input data is passed through the network layer by layer. Each neuron calculates a weighted sum of its inputs and applies an activation function. This process continues until the output layer, where results are generated.

STRUCTURE OF A DENSE NEURAL NETWORK

Dense neural networks, also known as feedforward neural networks or fully connected neural networks, are a type of artificial neural network architecture where every neuron in a layer is connected to every neuron in the subsequent layer.

These complete connections between neurons allow information to flow from the input layer to the output layer directly, without cycles or loops.

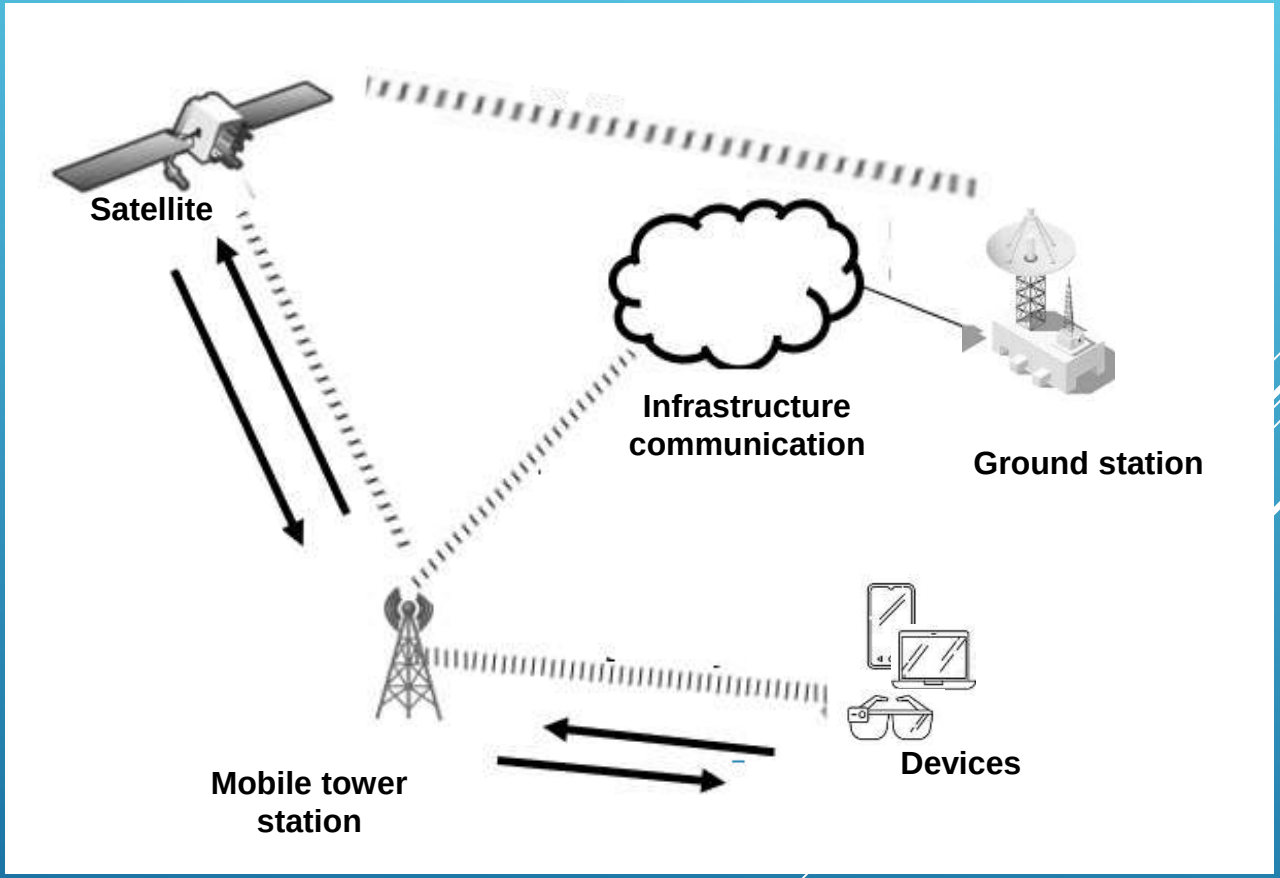


SATELLITE COMMUNICATION SYSTEM

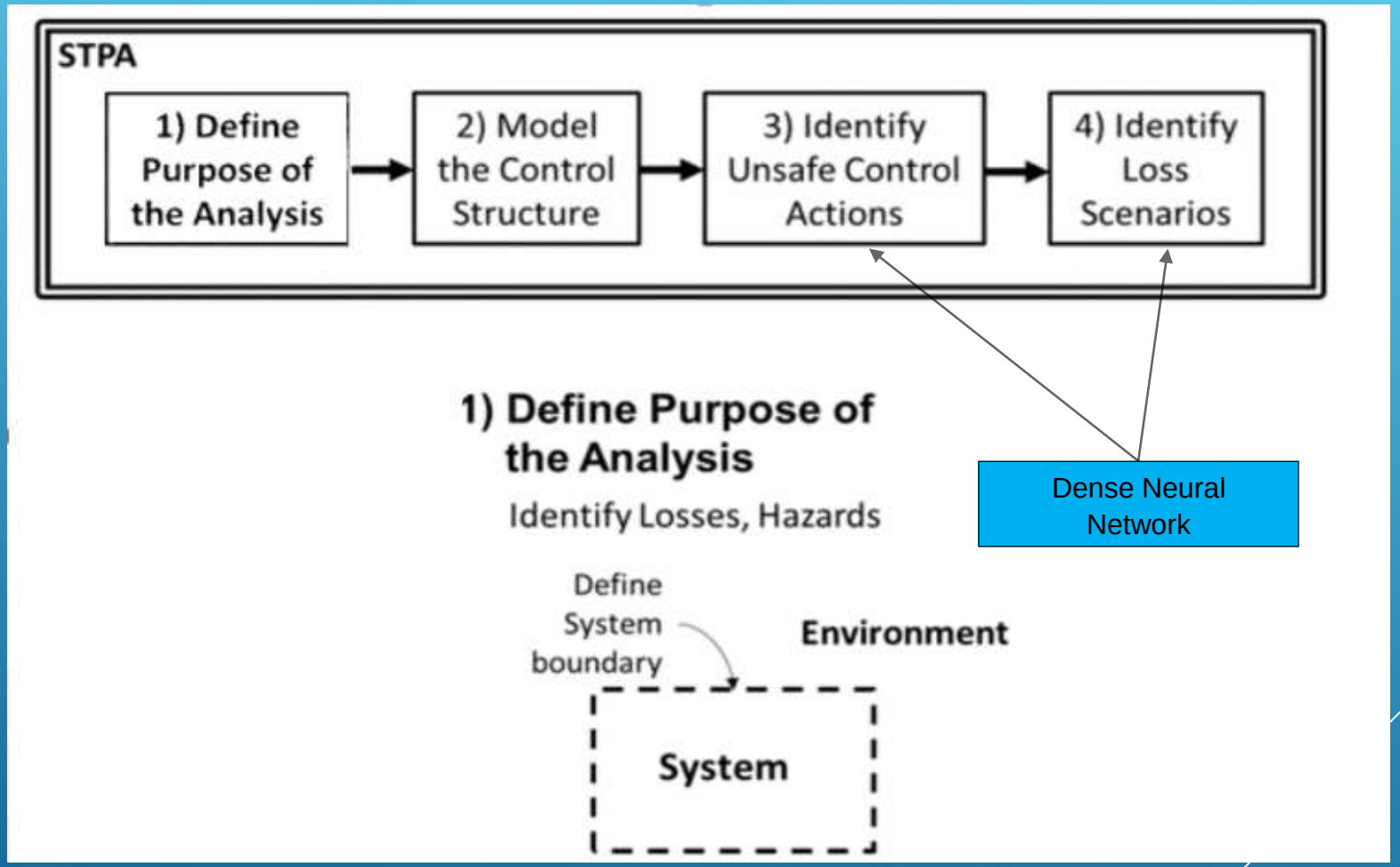
The satellite plays a central role, processing and relaying signals to personal devices, with position and attitude control.

The infrastructure includes antennas and amplifiers, while the ground station coordinates communications and monitors the satellite.

Mobile towers station expand coverage, and personal devices connect to the system for communication.

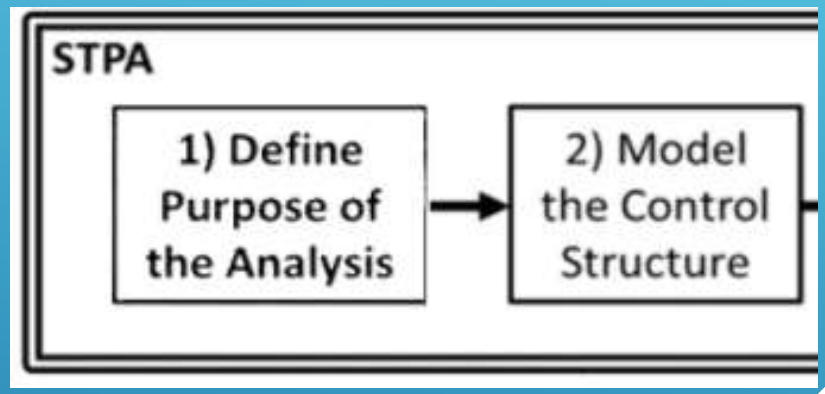


DEFINE PURPOSE OF THE ANALYSIS



PROCESSES THAT PRECEDE THE AI MODEL

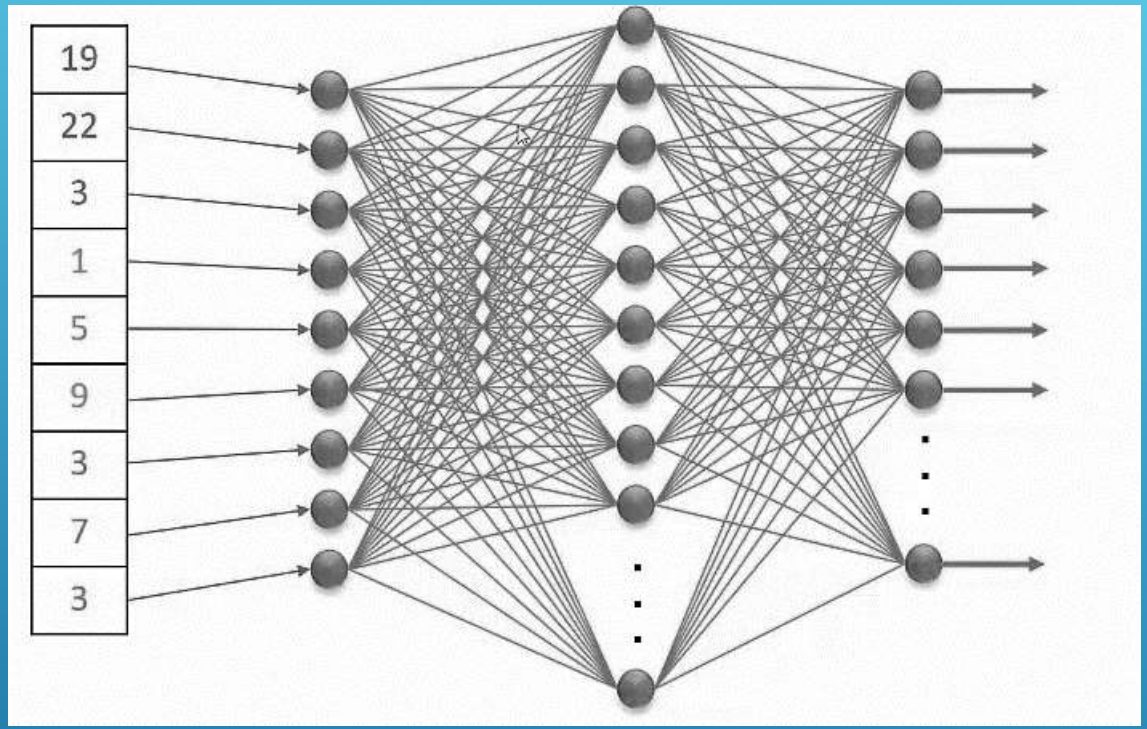
For the effective continuation of the research project that integrates Artificial Intelligence (AI) techniques to reinforce the safe/security of STPA systems, especially in aerospace missions, it is essential that certain fundamental steps of the STPA model have already been carried out.



Identify system-level losses and hazards In this phase, some of the main elements that could present hazards in a Satellite System were identified.

Using Dense Neural Network to Identify Unsafe/Insecury Control Actions UCAs

GENERAL STRUCTURE OF THE MODEL



$$a = ReLU(W_i x_i + b_i)$$

$$\hat{y} = \sigma(W_i a + b)$$

where:

- x - is the input vector.
- W - is the weight matrix of the first layer.
- b - is the bias vector of the first layer.
- ReLU = max(0,z) is the ReLU activation function.
- a - is the output of the first layer.

$$\sigma(z) = \frac{1}{1 + e^{-z}}$$

EXAMPLE: TRAINING AND ADJUSTING WEIGHTS

During neural network training, the values of the weight matrix W and the bias vector b are adjusted to minimize the loss function, allowing the network to learn to map inputs to outputs efficiently. This is done through optimization techniques such as gradient descent.

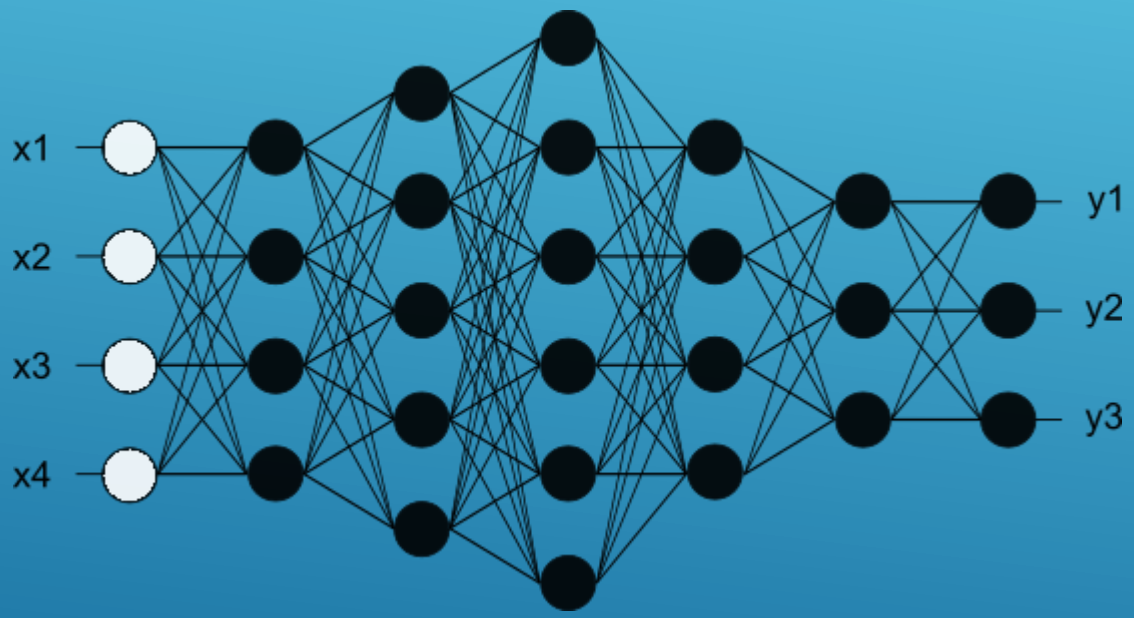
Weight matrix W :

```
[[ 0.0488135   0.21518937  0.10276338  0.04488318 -0.0763452 ]
 [-0.07266913  0.15189299  0.19763478 -0.02485648  0.17827692]
 [ 0.15761308 -0.08571854  0.11500048 -0.10908206  0.05144827]
 [ 0.19336093 -0.08656676  0.0665775   0.08429333 -0.12265167]
 [-0.04978854  0.02241914 -0.00492202 -0.1542998   0.09490053]
 [ 0.01842732  0.19561145  0.01472571 -0.05992527 -0.1525375 ]
 [ 0.13244667  0.13172169 -0.15407422 -0.0697119  -0.05924732]
 [ 0.03843959 -0.15753151 -0.09554833  0.15869363 -0.01376402]
 [-0.15759347  0.1090574  -0.10806355 -0.14616066  0.00369429]
 [ 0.07397278 -0.11837684  0.10834902  0.03525673  0.01948538]]
```

Bias vector b:

```
[0. 0. 0. 0. 0. 0. 0. 0. 0. 0.]
```

In a network where all neurons in a layer are connected to all neurons in the previous layer, we then have a fully connected layer, also called dense.



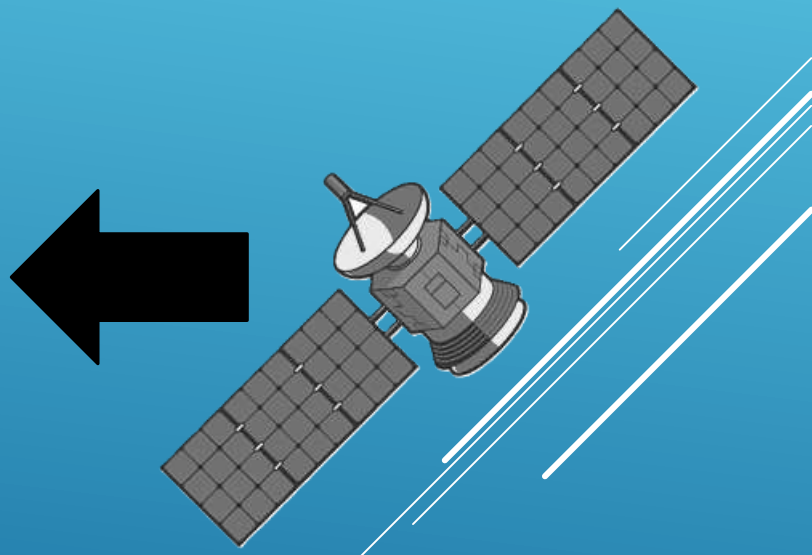
Model Structure:

The model is composed of a sequence of dense layers interspersed with Dropout layers to reduce the risk of overfitting. ReLU activation is used in the hidden layers to introduce nonlinearity, and the sigmoid function in the last layer to generate the probability of the positive class.Compilation: The model is compiled with the Adam optimizer and the binary_crossentropy loss function, common in binary classification problems. Accuracy is chosen as the performance metric.

UCA COMPONENTS BEHAVIOUR

Attributes for each record in the dataset:

1. Temperature: Temperature of the satellite (in degrees Celsius)
2. Vibration: Level of vibration detected (in Gs)
3. Current: Electrical current used (in amps)
4. Voltage: Electrical voltage (in volts)
5. Orientation: Deviation from expected orientation (in degrees)
6. Operation_time: Continuous operating time (in hours)



Examples of Unsafe Control Actions that the AI model should Find

UCAS ABOUT TEMPERATURE

Inadequate cooling control UCA: Poor management of the cooling system, allowing the temperature to exceed safe limits.

Types of Unsafety:

Component Failure:
Increased temperatures can cause the failure of critical satellite components, such as processors, batteries and scientific instruments.

Reduced Lifespan: Excessive temperatures can accelerate the aging of materials and components, reducing the satellite's lifespan.

Loss of Functionality: Certain satellite functionalities may be compromised due to overheating, affecting the ability to perform critical missions.

Risk of Explosion: In extreme cases, overheating can lead to the risk of explosion of batteries or other volatile materials on board.

UCAS ABOUT VIBRATION

- Vibration Sensor Disabling: Vibration sensors are disabled or fail to detect excessive vibrations that could cause structural damage.
- Ineffective Damping Control: Inadequate implementation of damping controls, allowing dangerous vibrations to persist.
- Failure to Respond to Vibration Signals: Ignoring signals of excessive vibration, failing to trigger corrective measures such as reducing load or speed.

UCAS ABOUT VOLTAGE

- Poor Voltage Regulation: unregulated voltage, resulting in voltage spikes that can damage electronic components.
- Overvoltage Protection Trips: Disabling or bypassing overvoltage protection systems, exposing the system to electrical loss.
- Delayed Voltage Adjustments: Delayed responses to voltage deviations, not solve the problems in time to prevent loss.

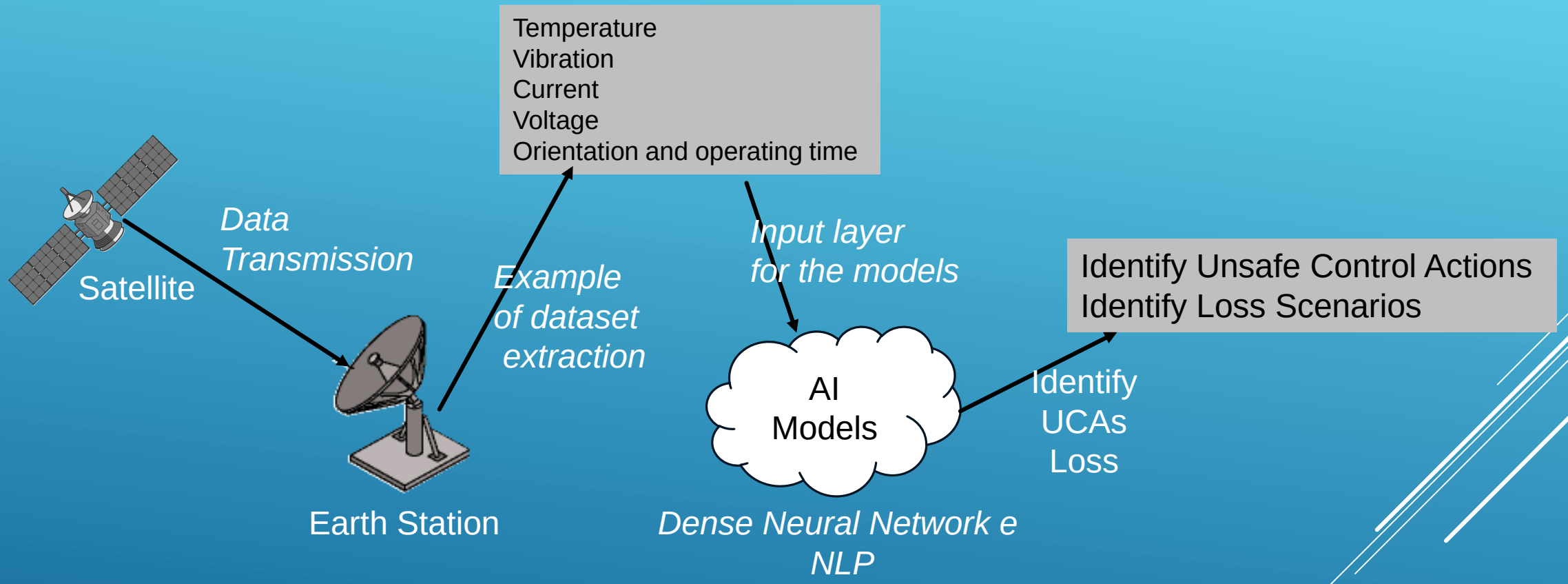
UCAS ABOUT ORIENTATION

- Sensor Misalignment: Improper installation or misfunction of sensors, providing inaccurate data to the control system.
- Inadequate Orientation Control: Inadequate implementation of orientation control mechanisms, leading to uncorrected deviations.
- Incorrect Deviations: delay in correcting orientation deviations, compromising the stability and safe operation of the system.

UCAS ABOUT OPERATING TIME

- Prolonged Operation Without Maintenance: Allowing the system to operate beyond the recommended maintenance intervals, increases the risk of failures due to wear.
- Disregarding Operating Time Limits: Ignoring safe operating time limits, forcing components to operate beyond their expected service life.
- No Operating Time Monitor: no monitoring and recording operating time, failing to identify when components require inspection or replacement.

SYSTEM OPERATION



Resultados Experimentais

Part of the data used for training

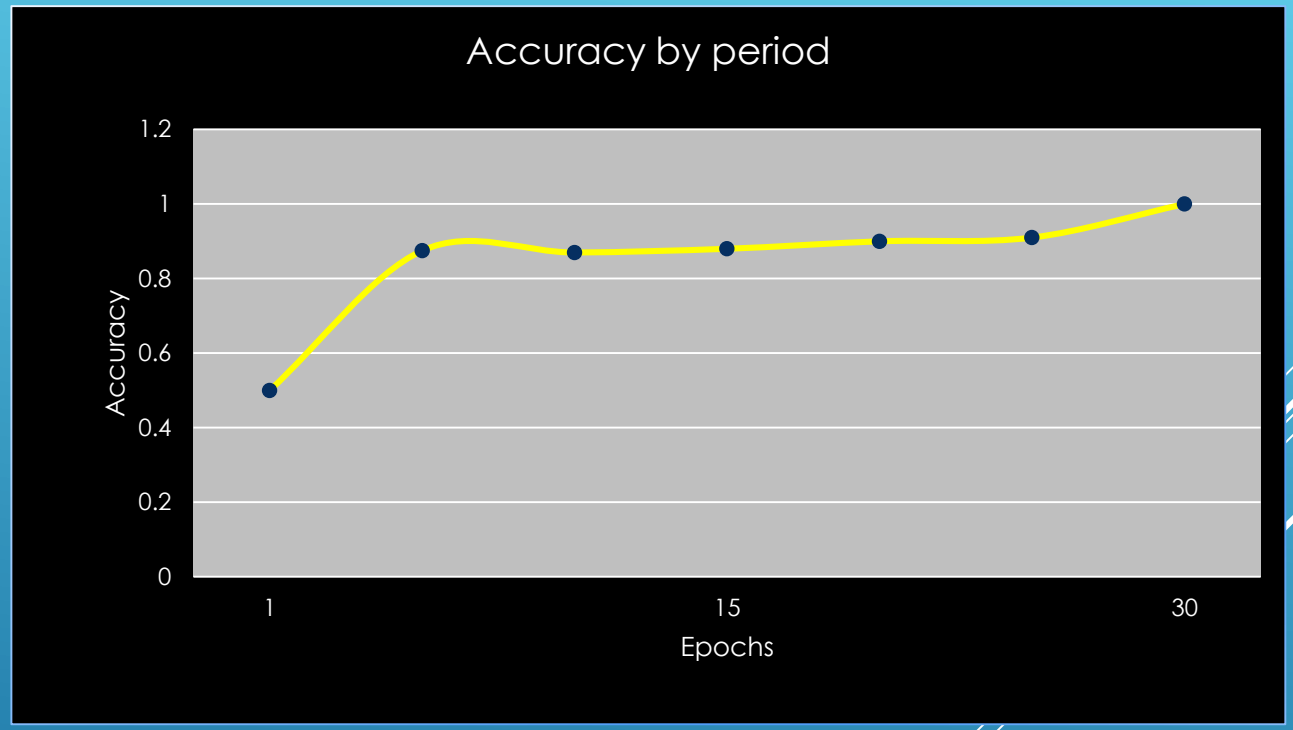
temperature	vibration	current	voltage	orientation	operating_time	Label
55	0,02	2,0	3,3	1	100	0
65	0,05	2,5	3,5	3	150	1
45	0,01	1,8	3,1	1	80	0

Safe Operation (0): Cases where the attribute values are within acceptable limits for satellite operation.

Dangerous Situation (1): Cases where one or more attributes are outside acceptable limits, indicating a possible hazard. For example, extremely high temperatures, high vibration levels, abnormal currents and voltages, large orientation deviations, or excessively long operating times.

Experimental results of model training

The model performed exceptionally well throughout the 30 training epochs, achieving a perfect 100% accuracy on both training and validation data. The loss continued to decrease consistently across epochs, indicating a continuous improvement in the accuracy of the model's predictions. The model performed exceptionally well across all 30 training epochs , achieving a perfect 100% accuracy on both training and validation data. The loss continued to decrease consistently across epochs, indicating a continuous improvement in the accuracy of the model's predictions.



CONCLUSION

The use of dense neural networks and NLP (Natural Language Processing) techniques to identify unsafe control actions and loss scenarios in the STPA represents a significant advance in safety analysis.

These technologies enable more robust and automated analysis, improving the detection of potential failures and mitigating risks.

CONCLUSION

With dense neural networks, it is possible to process large volumes of data to identify insecurity patterns.

while NLP techniques facilitate the interpretation and analysis of complex documents and safety reports.

Together, these approaches promote more effective and comprehensive security analysis.

REFERENCES

Curtis, H.D. Orbital mechanics for engineering students, 2013.

Duarte K.; Falbo R. A., Uma Ontologia de Qualidade de Software, Anais do VII Workshop de Qualidade de Software, XIV Simpósio Brasileiro de Engenharia de Software, João Pessoa; 2000.

Fei T. Liu; Kai M. Ting; Zhi-Hua Zhou, Isolation Forest Disponível em: <https://cs.nju.edu.cn/zhouzh/zhouzh.files/publication/icdm08b.pdf> Acesso em 5 Mar. 2024.

JimmiemcEver, Jamesvasatka, Russsyphert, Timothy D. West, Benmiled Z. Cybersecurity as a Complex Adaptive Systems Problem Article 2019 DOI 10.2514/5.9781624105654.0201.0214 Disponível em: < https://arc.aiaa.org/doi/10.2514/5.9781624105654.0201.0214> Acesso em: 09 out. 2022.

Lemos R.: Requirements Engineering for Embedded Systems, tutorial, Centro Técnico Aeroespacial. São José dos Campos, 1998.

Nancy G. Leveson; John P. Thomas, STPA HANDBOOK <http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf> Acesso em 11 jan. 2024.

Rodrigues, Luis Eduardo Miranda José Fundamentos da Engenharia Aeronáutica CENGAGE LEARNING,2013.

S. Robertson, J. Robertson. Mastering the Requirements Process, Harlow, England: Addison-Wesley, 1999.

Visner S. Samuel; Kordella Scott. Cyber Best Practices for Small Satellites Article 2020. DOI 10.2514/6.2020-4013 Disponível em: < https://arc.aiaa.org/doi/10.2514/6.2020-4013> Acesso em 11 out. 2022.

Visner, Samuel S. Development of Cybersecurity Norms for Space Systems Article 2018. DOI 10.2514/6.2021-4050 Disponível em: <https://arc.aiaa.org/doi/pdf/10.2514/6.2021-4050> Acesso em: 08 out. 2022.