THREAT-ASSET MATRIX
FOR A HYPOTHETICAL NUCLEAR POWER PLANT NETWORK DIAGRAM

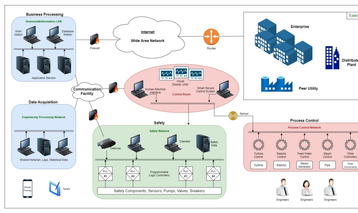
In this study, a fictitious Nuclear Power Plant Network Diagram is drawn and a threat-asset matrix is created with the valued assets of this network and the threat types. Then, the security risk value for each cell in the matrix is estimated based on the probabilities and consequences.

Below is the table of five elements considered while determining the assets of the network:

Hardware	Described as any physical component of a computer system that contains a circuit board, ICs, or other electronics
Software	A collection of instructions that enable the user to interact with a computer, its hardware, or perform tasks.
Data	Any set of characters that is gathered and translated for some purpose, usually analysis
Facilities	Something designed, built or installed, to serve a specific function affording a convenience or service
People	Individuals take part in the planning and operating the system

---

A Hypothetical Nuclear Power Plant Network Diagram



Threat-Asset Matrix

Estimated Probability and Consequence ratings are on a scale of 1-5
1: Very Low | 2: Low | 3: Medium | 4: High | 5: Very High

Color Scheme based on the risk value

20-25	15-19	10-14	6-9	1-5

Estimated Risk Value = Estimated Probability x Estimated Consequence

	Confidentiality	Integrity	Availability	Theft/Fraud
Computers	5 (1x5)	5 (1x5)	5 (1x5)	5 (1x5)
Tablets	6 (2x3)	6 (2x3)	6 (2x3)	9 (3x3)
Phones	3 (3x1)	2 (2x1)	2 (2x1)	4 (4x1)
Smart Secure Control System	20 (4x5)	20 (4x5)	10 (2x5)	10 (2x5)
Simulation System	4 (2x2)	5 (2x5)	8 (2x4)	5 (1x5)
Encrypted Communication System	15 (3x5)	10 (2x5)	10 (2x5)	5 (1x5)
Reactor Monitoring And Control Software	10 (2x5)	10 (2x5)	15 (3x5)	5 (1x5)
Visual Display Units	4 (1x4)	5 (1x5)	8 (2x4)	5 (1x5)
Strict Logs	12 (3x4)	8 (2x4)	8 (2x4)	9 (3x3)
Statistical Data	12 (3x4)	8 (2x4)	8 (2x4)	9 (3x3)
Inventory Data	4 (2x2)	8 (2x4)	8 (2x4)	4 (2x2)
Sensors	8 (2x4)	10 (2x5)	12 (3x4)	12 (3x4)
Catalyst	5 (1x5)	5 (1x5)	8 (2x4)	5 (1x5)
Programmable Logic Controller	10 (2x5)	5 (1x5)	15 (3x5)	5 (1x5)
Access Code	10 (2x5)	10 (2x5)	10 (2x5)	20 (4x5)
Turbine	10 (2x5)	5 (1x5)	15 (3x5)	5 (1x5)
Reactor	10 (2x5)	5 (1x5)	15 (3x5)	5 (1x5)
Steam Generator	10 (2x5)	5 (1x5)	15 (3x5)	5 (1x5)
Pipe	10 (2x5)	5 (1x5)	15 (3x5)	5 (1x5)
Scientists	15 (3x5)	5 (1x5)	10 (2x5)	5 (1x5)

*** Click the Asset to go to its risk estimation details**

Details of Each Cell of the Threat-Asset Matrix

Computers

Confidentiality: Unlikely to be accessed from unauthorized users as they are protected with strict rules but if someone access them, the consequence would be very high because it can be dangerous for the system
Integrity: Unlikely to be changed by unauthorized users as they are protected with strict rules. passwords but if someone changes it, the consequence would be very high as they may behave wrong which would be dangerous for the system
Availability: Low probability of being unavailable (computers can be locked for a certain time) but the consequence would be very high because there may be an emergency that needs to be controlled
Theft/Fraud: Unlikely to be a subject of Theft/Fraud as they are protected with strict rules, but the consequence would be very high because they may contain sensitive data

Tablets

Confidentiality: Low probability of being accessed from unauthorized users. They are protected with strong passwords but they can be easily moved from one place to another. If someone accesses them, the consequence would be medium because they may contain sensitive data
Integrity: Unlikely to be changed by unauthorized users as they are protected with strict passwords but if someone changes them, the consequence would be high as they may behave wrong which would be dangerous for the system
Availability: Low probability of being unavailable but the consequence would be high because there may be an emergency that needs to be controlled
Theft/Fraud: Medium probability of being a subject of Theft/Fraud as they can be easily moved from one place to another, and the consequence would also be medium high because they may contain sensitive data (not much like computers)

Phones

Confidentiality: Medium probability of being accessed from unauthorized users. They are protected with strong passwords but they can be easily moved from one place to another. If someone accesses them, the consequence would be very low because they do not contain any sensitive data or have any control mechanism
Integrity: Low probability of being changed by unauthorized users as they are protected with strict passwords. If someone changes them, the consequence would be very low as they do not contain any sensitive data or have any control mechanism
Availability: Very low probability of being unavailable and the consequence would be very low as they do not contain any sensitive data or have any control mechanism
Theft/Fraud: High probability of being a subject of Theft/Fraud as they can be easily moved from one place to another, but the consequence would be very low as they do not contain any sensitive data or have any control mechanism

Smart Secure Control System

Confidentiality: High probability of being accessed from unauthorized users as it is threatened by the external threats even if it is protected with strict rules. If someone accesses it, the consequence would be very high because they are the main part of the system
Integrity: High probability of being changed by unauthorized users as it is threatened by the external threats. If someone changes it, the consequence would be very high as it may behave wrong which would be dangerous for the system
Availability: Low probability of being unavailable as it must always be ready to get controlled, but the consequence would be very high when it is not available as there may be an emergency that needs to be controlled at that moment
Theft/Fraud: Low probability of being a subject of Theft/Fraud, but the consequence would be very high because they are the main part of the system

Simulation System

Confidentiality: Low probability of being accessed from unauthorized users as they are protected with strict rules. If someone access it, the consequence would be low because it is just for simulation and does not have any control mechanism for the real system
Integrity: Low probability of being changed by unauthorized users as they are protected with strict rules but if someones change it, the consequence would be very high as it may show wrong simulating results which would be dangerous for the system
Availability: Low probability of being unavailable, but the consequence would be high because the simulation can be delayed due to unavailability
Theft/Fraud: Unlikely to be a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be high because it contains the sensitive system data such as detailed copy of the real system

Encrypted Communication System

Confidentiality: Medium probability of being accessed from unauthorized users as it is threatened by the external threats even if it is protected with strict rules. If someone accesses it, the consequence would be very high because it may reveal the hidden information to the untrusted sources
Integrity: Low probability of being changed by unauthorized users as they are protected with strict rules but if someone changes it, the consequence would be very high as it may block the communication between people and the important parts of the system
Availability: Low probability of being unavailable, but the consequence would be very high because the connection can be interrupted between people and the important parts of the system
Theft/Fraud: Unlikely to be a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be very high because it contains the sensitive information of the system

Reactor Monitoring And Control Software

Confidentiality: Low probability of being accessed by unauthorized users as they are protected with strict rules but if someone accesses it, the consequence would be very high as they may operate it in a wrong way
Integrity: Low probability of being changed by unauthorized users as they are protected with strict rules but if someone changes it, the consequence would be very high as the system can behave in an unexpected way
Availability: Medium probability of being unavailable because of some uninterruptible processes and the consequence would be very high because there may be an emergency that needs to be controlled
Theft/Fraud: Unlikely to be a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be very high because it contains the sensitive controls of the reactor

Visual Display Units

Confidentiality: Unlikely to be accessed from unauthorized users as it is protected with strict rules but if someone access them, the consequence would be high because it may reveal all the information about the system
Integrity: Unlike probability of being changed by unauthorized users as it is protected with strict rules but if someone changes it, the consequence would be very high as it would show the wrong information and can lead unexpected results
Availability: Low probability of being unavailable, but the consequence would be high because the some processes can be delayed due to unavailability
Theft/Fraud: Unlikely to be a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be very high because it contains the sensitive information of the system

Strict Logs

Confidentiality: Medium probability of being accessed from unauthorized users as it is threatened by the external threats even if it is protected with strict rules. If someone accesses them, the consequence would be high because it may reveal some sensitive information about the system
Integrity: Low probability of being changed by unauthorized users as it is protected with strict rules but if someone changes it, the consequence would be high as it would show the wrong information
Availability: Low probability of being unavailable, but the consequence would be high because the next steps which would be taken based on the logs can be delayed due to unavailability
Theft/Fraud: Unlikely to be a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be very high because it contains the sensitive information of the system

Statistical Data

Confidentiality: Medium probability of being accessed from unauthorized users as it is threatened by the external threats even if it is protected with strict rules. If someone accesses them, the consequence would be high because it may reveal some sensitive information about the system
Integrity: Low probability of being changed by unauthorized users as it is protected with strict rules but if someone changes it, the consequence would be high as it would show the wrong information
Availability: Low probability of being unavailable, but the consequence would be high because the next steps which would be taken based on the logs can be delayed due to unavailability
Theft/Fraud: Unlikely to be a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be very high because it contains the sensitive information of the system

Inventory Data

Confidentiality: Low probability of being accessed from unauthorized users and the consequence would also be low because it does not have an essential information about the network and sensitive information
Integrity: Low probability of being changed by unauthorized users but if someone changes it, the wrong data may cause a mislead
Availability: Low probability of being unavailable, but the consequence would be high because it is important to know the inventory data when needed
Theft/Fraud: Low probability of being a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be very high because it contains the data about the inventory

Sensors

Confidentiality: Low probability of being accessed from unauthorized users but the consequence would be high because they warn the staff the when something is going wrong with the system
Integrity: Low probability of being changed by unauthorized users but if someone changes it, the consequence would be very high as the wrong data may cause a mislead and to give wrong decisions about the system
Availability: Medium probability of being unavailable because they can be affected easily with the environment, and the consequence would be high because they are used to track the system
Theft/Fraud: Medium probability of being a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be high because they are used to track the system

Catalyst

Confidentiality: Low probability of being accessed from unauthorized users but the consequence would be very high as it is the one of the most dangerous part of the system
Integrity: Very low probability of being changed by unauthorized users but if someone changes it, the consequence would be very high as it may cause unexpected results
Availability: Low probability of being unavailable because of some uninterruptible processes and the consequence would be high because there may be an emergency that needs to be controlled immediately
Theft/Fraud: Very low probability of being a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be very high because it is some of the main parts of the system

Access Code

Confidentiality: Low probability of being accessed from unauthorized users but the consequence would be very high as it is the code of accessing the system
Integrity: Low probability of being changed by unauthorized users as it is protected with strict rules, but if someone changes it, the consequence would be very high on certain times when the stuff need to do some urgent work with the access code
Availability: Low probability of being unavailable, but the consequence would be very high when it is not available as there may be an emergency that needs to be controlled with the access code
Theft/Fraud: High probability of being a subject of Theft/Fraud even if it is protected with strict rules, and the consequence would be very high because it can affect all the system by a third-party

Programmable Logic Controller

Confidentiality: Low probability of being accessed from unauthorized users but the consequence would be very high as it is the controller of the system
Integrity: Very low probability of being changed by unauthorized users as it is protected with strict rules, but if someone changes it, the consequence would be very high as the system can behave unexpectedly
Availability: Medium probability of being unavailable because of some uninterruptible processes, and the consequence would be very high when it is not available as there may be an emergency that needs to be controlled at that moment
Theft/Fraud: Very low probability of being a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be very high because it can affect all the system

Turbine

Confidentiality: Low probability of being accessed from unauthorized users but the consequence would be very high as it is the one of the main parts of the system
Integrity: Very low probability of being changed by unauthorized users as it is protected with strict rules, but if someone changes it, the consequence would be very high as the turbine can behave unexpectedly
Availability: Medium probability of being unavailable because of some uninterruptible processes, and the consequence would be very high when it is not available as there may be an emergency that needs to be controlled at that moment
Theft/Fraud: Very low probability of being a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be very high because it is one of the main parts of the system

Reactor

Confidentiality: Low probability of being accessed from unauthorized users but the consequence would be very high as it is the one of the main parts of the system
Integrity: Very low probability of being changed by unauthorized users as it is protected with strict rules, but if someone changes it, the consequence would be very high as the reactor can behave unexpectedly which can be very dangerous
Availability: Medium probability of being unavailable because of some uninterruptible processes, and the consequence would be very high when it is not available as there may be an emergency that needs to be controlled at that moment
Theft/Fraud: Very low probability of being a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be very high because it is one of the main parts of the system

Steam Generator

Confidentiality: Low probability of being accessed from unauthorized users but the consequence would be very high as it is the one of the main parts of the system
Integrity: Very low probability of being changed by unauthorized users as it is protected with strict rules, but if someone changes it, the consequence would be very high as the generator can behave unexpectedly and can be dangerous
Availability: Medium probability of being unavailable because of some uninterruptible processes, and the consequence would be very high when it is not available as there may be an emergency that needs to be controlled at that moment
Theft/Fraud: Very low probability of being a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be very high because it is one of the main parts of the system

Pipe

Confidentiality: Low probability of being accessed from unauthorized users but the consequence would be very high as it is the one of the main parts of the system
Integrity: Very low probability of being changed by unauthorized users as it is protected with strict rules, but if someone changes it, the consequence would be very high as the pipe can behave unexpectedly and cause dangerous results
Availability: Medium probability of being unavailable because of some uninterruptible processes, and the consequence would be very high when it is not available as there may be an emergency that needs to be controlled at that moment
Theft/Fraud: Very low probability of being a subject of Theft/Fraud as it is protected with strict rules, but the consequence would be very high because it is one of the main parts of the system

Engineers

Confidentiality: Medium probability of being forced by unauthorized people to ask information about the system. The consequence would be high if third-parties are able to get some sensitive information
Integrity: Very low probability of being forced by unauthorized people to change some information with the system but the consequence would be high if they do something wrong
Availability: Low probability of being unavailable, but the consequence would be very high when they are not available at an emergency situation
Theft/Fraud: Very low probability of being a subject of Theft/Fraud, but the consequence can be very high when losing them

---

Total Estimated Risk for the Assets

Asset	Total Estimated Risk
Smart Secure Control System	60
Access Code	50
Sensors	42
Encrypted Communication System	40
Reactor Monitoring And Control Software	40
Strict Logs	37
Statistical Data	37
Programmable Logic Controller	35
Turbine	35
Reactor	35
Steam Generator	35
Pipe	35
Engineers	35
Tablets	27
Inventory Data	24
Catalyst	23
Simulation System	22
Visual Display Units	22
Computers	20
Phones	11