Internship at the Cyber Innovation Hub

Cybersecurity in Operational Technologies

Hyb Arloesedd Seiber
Cyber Innovation Hub

FONDATION RENNES 1
Progresser Innover Entreprendre

iut Lannion


Kirkwall
Elgin
Portree
Inverness
HEBRIDES
SCOTLAND
Aberdeen
Dundee
St Andrews
Stirling
Edinburgh
Glasgow
United Kingdom
Newcastle upon Tyne
Sligo
Leeds
Dundalk
Drogheda
Galway
Ireland
Dublin
Liverpool
Manchester
Limerick
Kilkenny
Birmingham
Norwich
Dingle
Tralee
Waterford
Cyber Innovation Hub
Cambridge
Killarney
Cork
Oxford
London
Bristol
Cardiff
Exeter
Bournemouth
Plymouth
English Channel
Rouen


Kirkwall
Elgin
Portree
Inverness
HEBRIDES
SCOTLAND
Aberdeen
Dundee
St Andrews
Stirling
Edinburgh
Glasgow
United Kingdom
Newcastle upon Tyne
Sligo
Leeds
Dundalk
Drogheda
Galway
Ireland
Dublin
Liverpool
Manchester
Limerick
Kilkenny
Birmingham
Norwich
Dingle
Tralee
Waterford
Cyber Innovation Hub
Cambridge
Killarney
Cork
Oxford
London
Bristol
Cardiff
Exeter
Bournemouth
Plymouth
English Channel
Rouen

7 Avril 2025

7 Avril 2025 ⟶ 13 Juin 2025

10 semaines

7 Avril 2025 ⟶ 13 Juin 2025

10 semaines

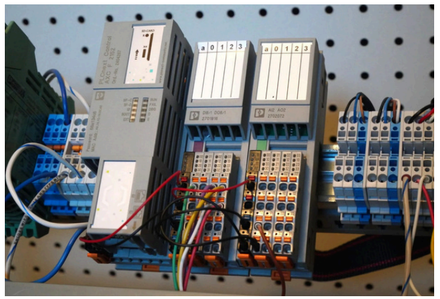
7 Avril 2025 ⟶ 13 Juin 2025

Cybersécurité dans les technologies opérationnelles

10 semaines

7 Avril 2025 ⟶ 13 Juin 2025

Cybersécurité dans les technologies opérationnelles



I - Host Organization & Problematic

II - Existing Situation, Tasks & Difficulties

I - Host Organization & Problematic

III - Tools, Gantt Planning & Personal Organization

I - Host Organization & Problematic
II - Existing Situation, Tasks & Difficulties

IV - The 3 main projects

I - Host Organization & Problematic
II - Existing Situation, Tasks & Difficulties
III - Tools, Gantt Planning & Personal Organization

V - Current VS Initial situation, Technical & Human Assessment

I - Host Organization & Problematic
II - Existing Situation, Tasks & Difficulties
III - Tools, Gantt Planning & Personal Organization
IV - The 3 main projects

I - Host Organization & Problematic

II - Existing Situation, Tasks & Difficulties

III - Tools, Gantt Planning & Personal Organization

IV - The 3 main projects

V - Current VS Initial situation, Technical & Human Assessment

Legal Status: **Non-profit**

Legal Status: Non-profit
Name: **Cyber Innovation Hub**

I - Host Organization & Problematic

Legal Status: Non-profit
Name: Cyber Innovation Hub
Mission: **Transform the South Wales into a leading cybersecurity cluster by 2030**

I - Host Organization & Problematic

Legal Status: Non-profit
Name: Cyber Innovation Hub
Mission: Transform the South Wales into a leading cybersecurity cluster by 2030

I - Host Organization & Problematic

Legal Status: Non-profit
Name: Cyber Innovation Hub
Mission: Transform the South Wales into a leading cybersecurity cluster by 2030

I - Host Organization & Problematic

Legal Status: Non-profit
Name: Cyber Innovation Hub
Mission: Transform the South Wales into a leading cybersecurity cluster by 2030
Size: **12-16 employees**

I - Host Organization & Problematic

Legal Status: Non-profit
Name: Cyber Innovation Hub
Mission: Transform the South Wales into a leading cybersecurity cluster by 2030
Size: 12-16 employees
Products & services: **OT consultancy, trainings and testbeds**

I - Host Organization & Problematic

Legal Status: Non-profit
Name: Cyber Innovation Hub
Mission: Transform the South Wales into a leading cybersecurity cluster by 2030
Size: 12-16 employees
Products & services: OT consultancy, trainings and testbeds
Customers: **Businesses and governmental organizations**

I - Host Organization & Problematic

Legal Status: Non-profit
Name: Cyber Innovation Hub
Mission: Transform the South Wales into a leading cybersecurity cluster by 2030
Size: 12-16 employees
Products & services: OT consultancy, trainings and testbeds
Customers: Businesses and governmental organizations
Divisions:

- **Commercials**
- **Operations**
- **Strategy**
- **Delivery (Mine)**

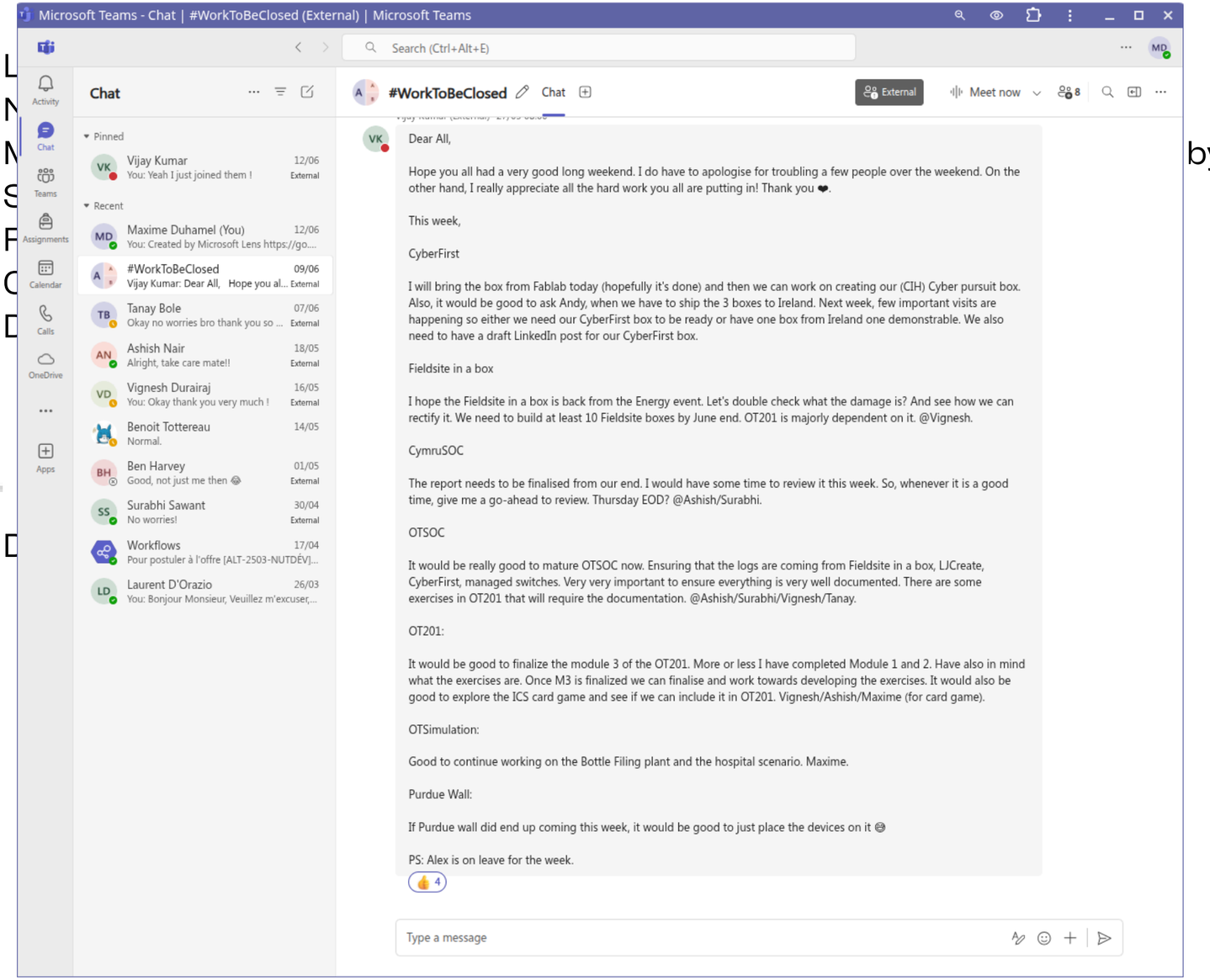
I - Host Organization & Problematic

Legal Status: Non-profit
Name: Cyber Innovation Hub
Mission: Transform the South Wales into a leading cybersecurity cluster by 2030
Size: 12-16 employees
Products & services: OT consultancy, trainings and testbeds
Customers: Businesses and governmental organizations
Divisions:

- Commercials
- Operations
- Strategy
- Delivery (Mine)

Delivery Team: **6 members, led by Vijay**

I - Host Organization & Problematic



by 2030

30

How can the CIH simulate realistic cyberattack environments to efficiently train teams in defense and incident response?

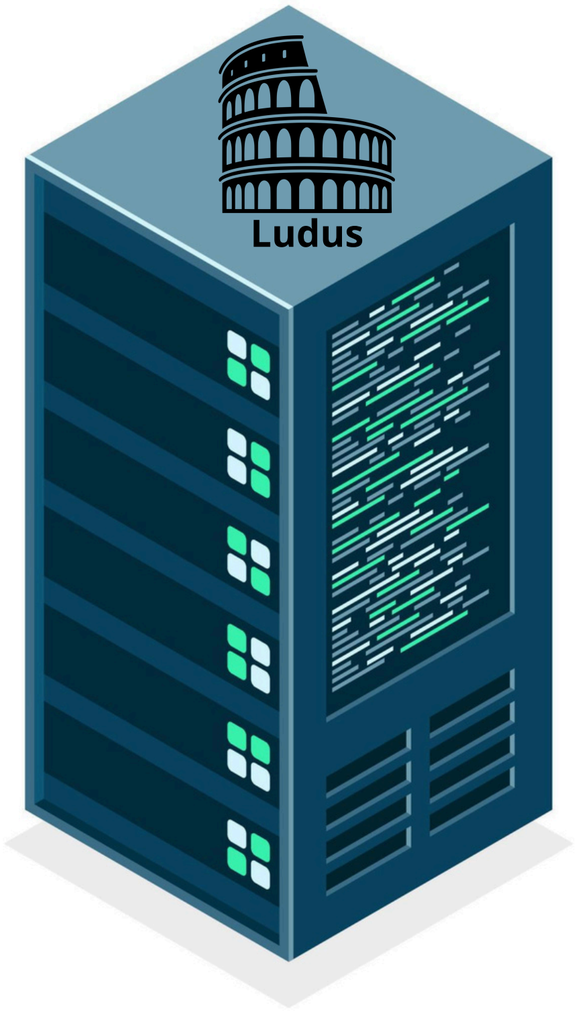
I - Host Organization & Problematic

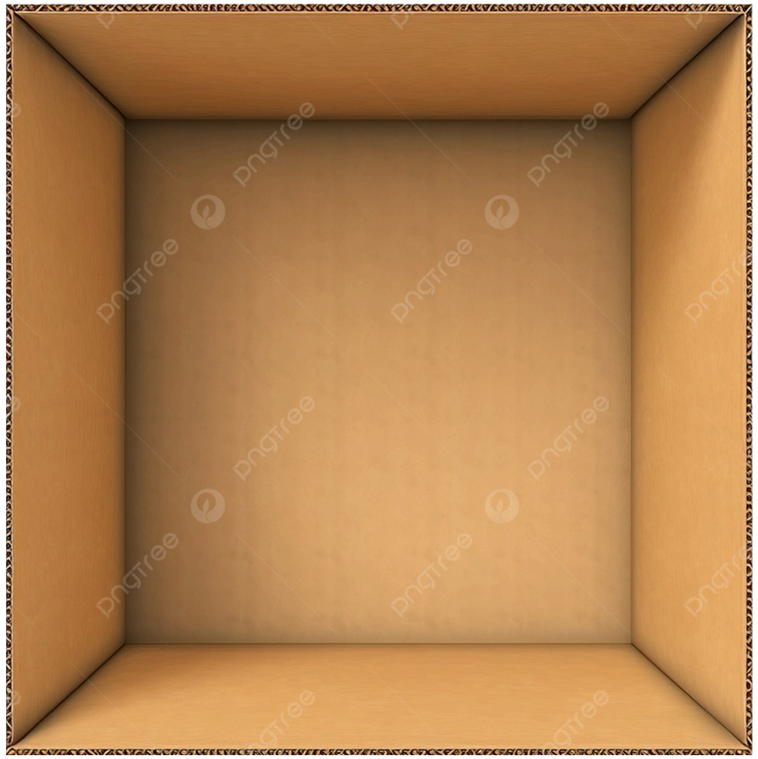
II - Existing Situation, Tasks & Difficulties

III - Tools, Gantt Planning & Personal Organization

IV - The 3 main projects

V - Current VS Initial situation, Technical & Human Assessment


Ludus



Your computer
(physical machine)

Your computer
(physical machine)

Your computer
(physical machine)

Your computer
(physical machine)

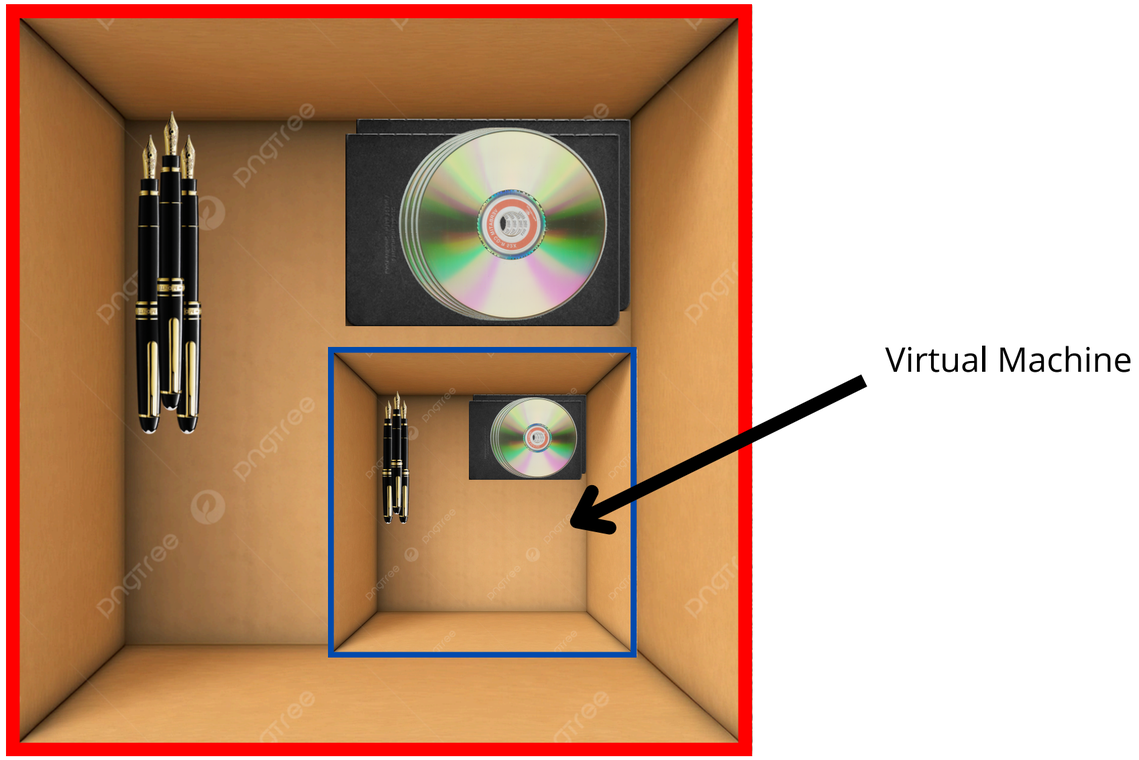
Your computer
(physical machine)

Your computer
(physical machine)

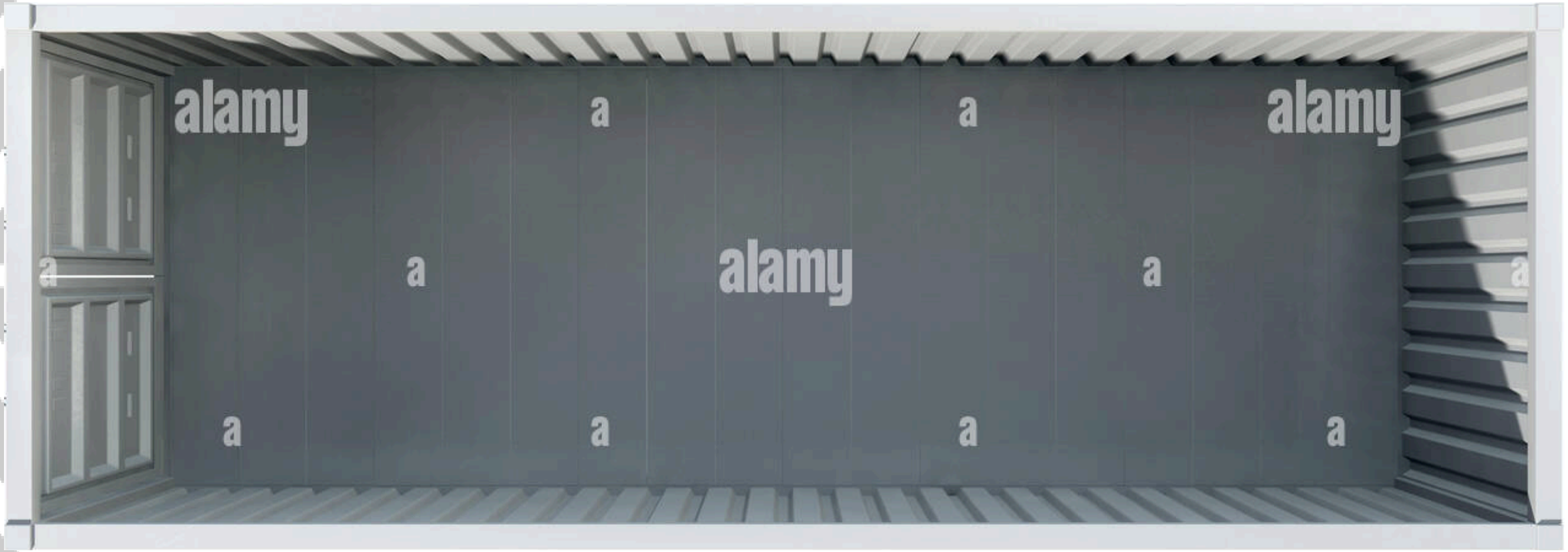
Your computer
(physical machine)

Your computer
(physical machine)

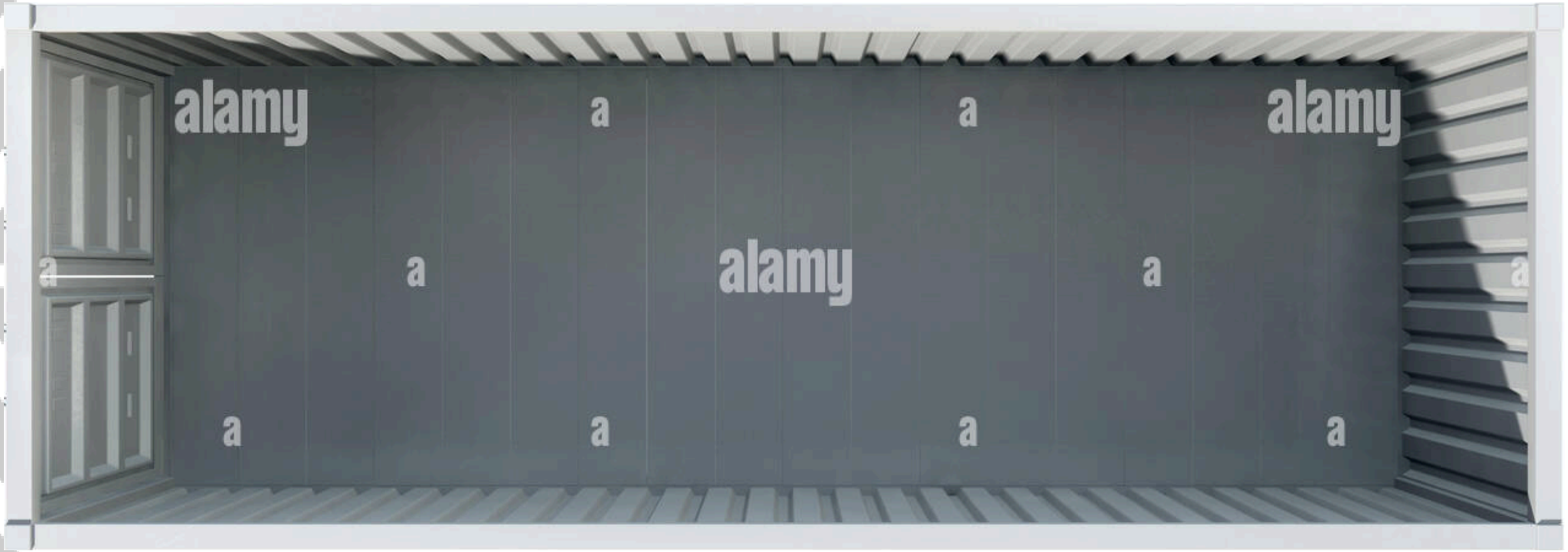
Your computer
(physical machine)



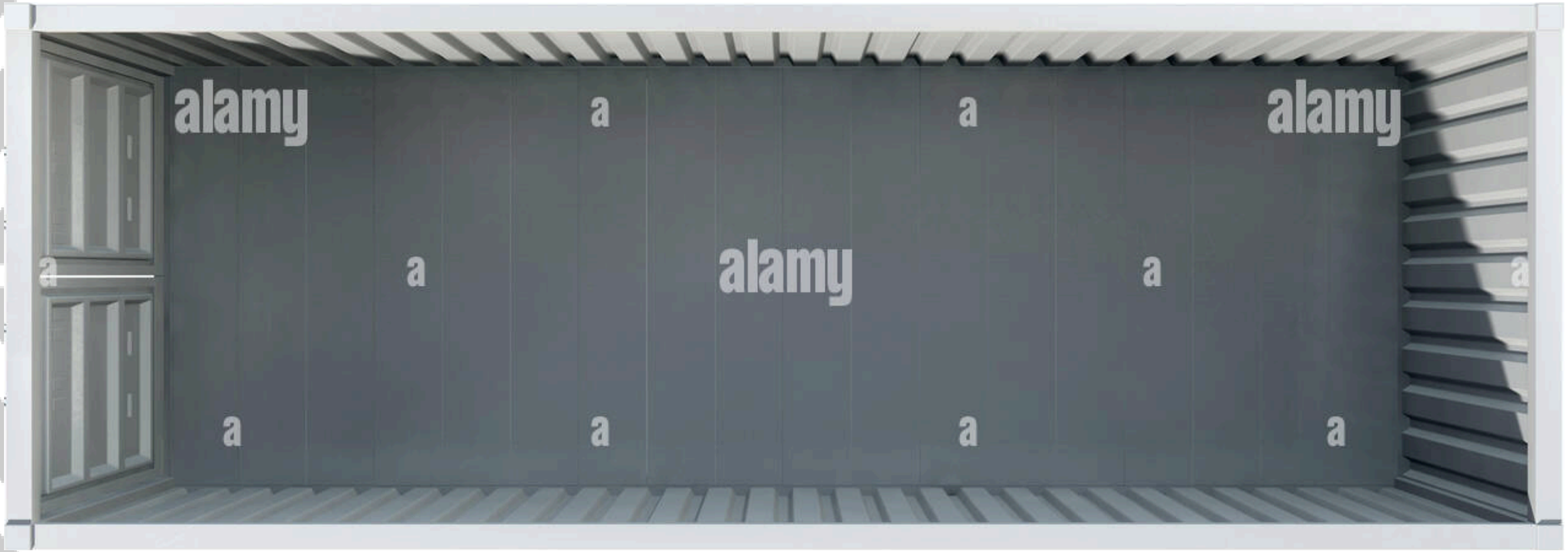
Virtual Machine


alamy
alamy
alamy

User 1 User 2 User 3

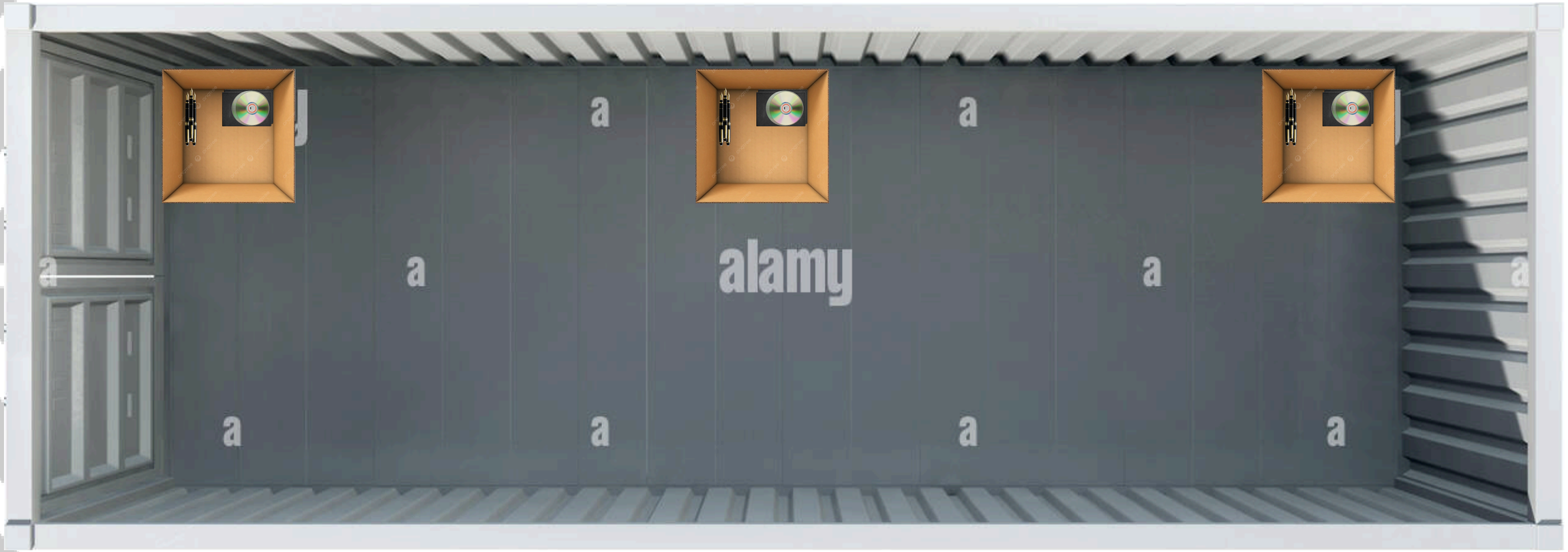


User 1 User 2 User 3



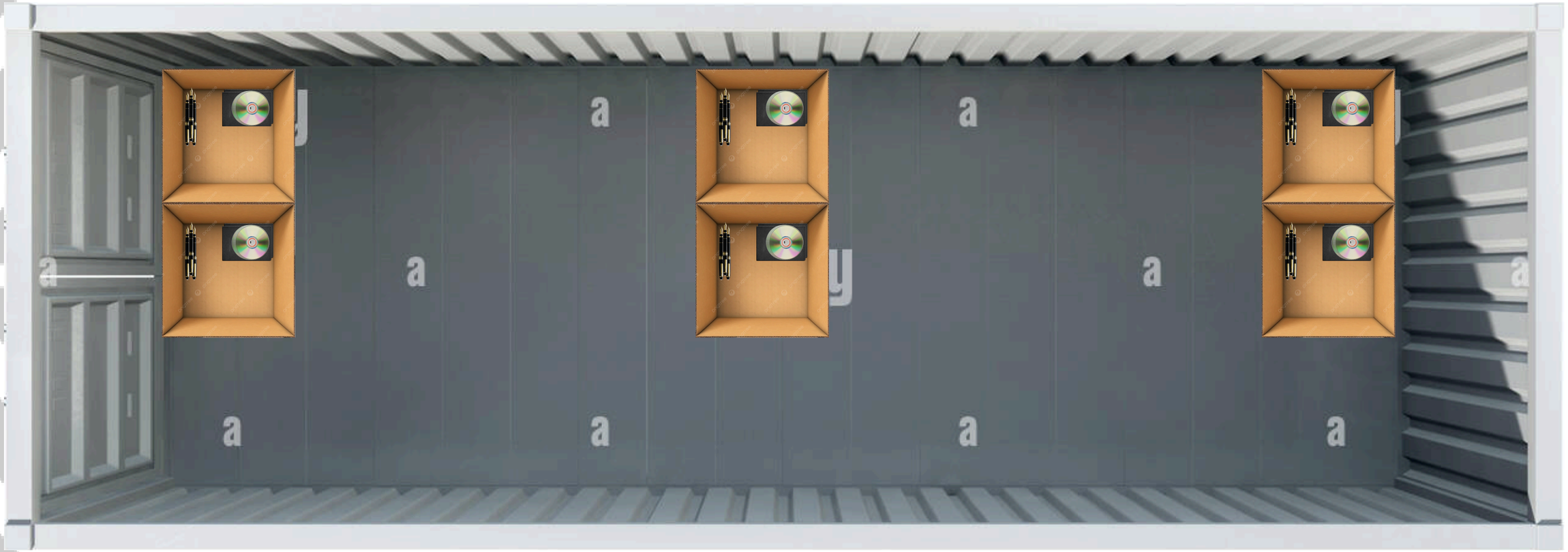
Virtual Machine 1

User 1 User 2 User 3



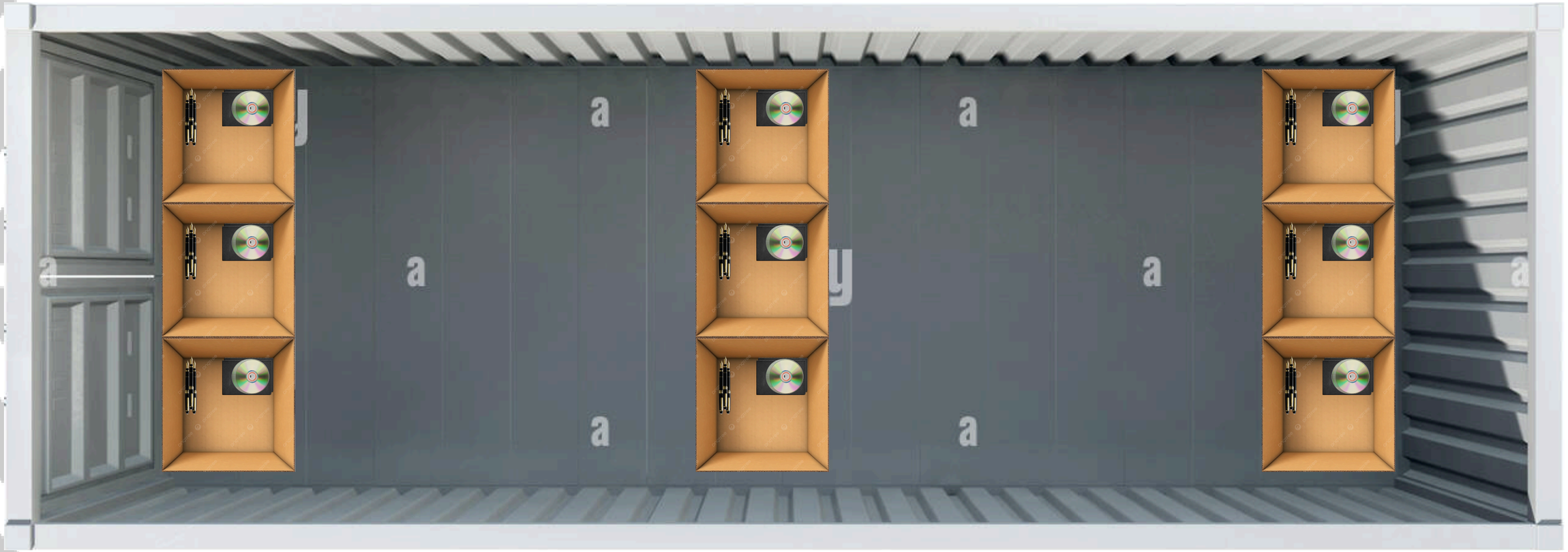
Virtual Machine 1

User 1 User 2 User 3



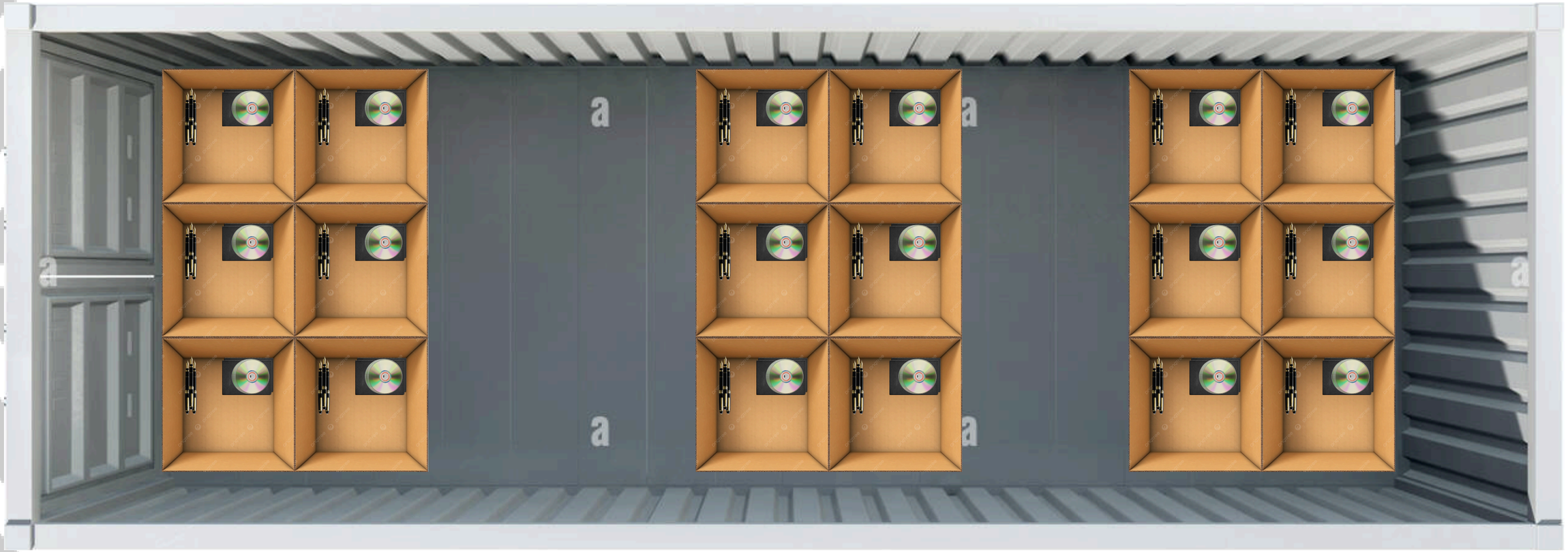
Virtual Machine 1

User 1 User 2 User 3

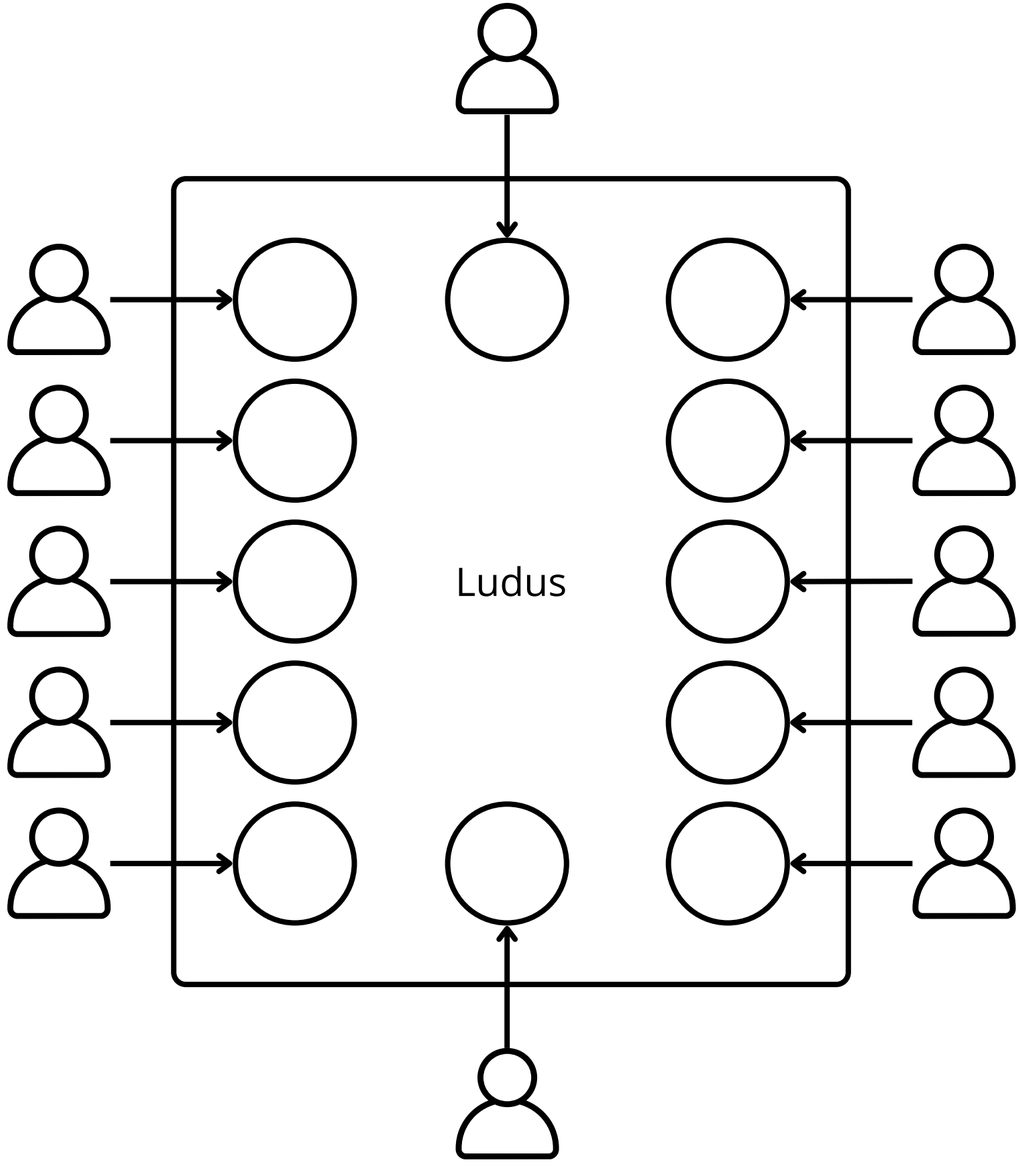


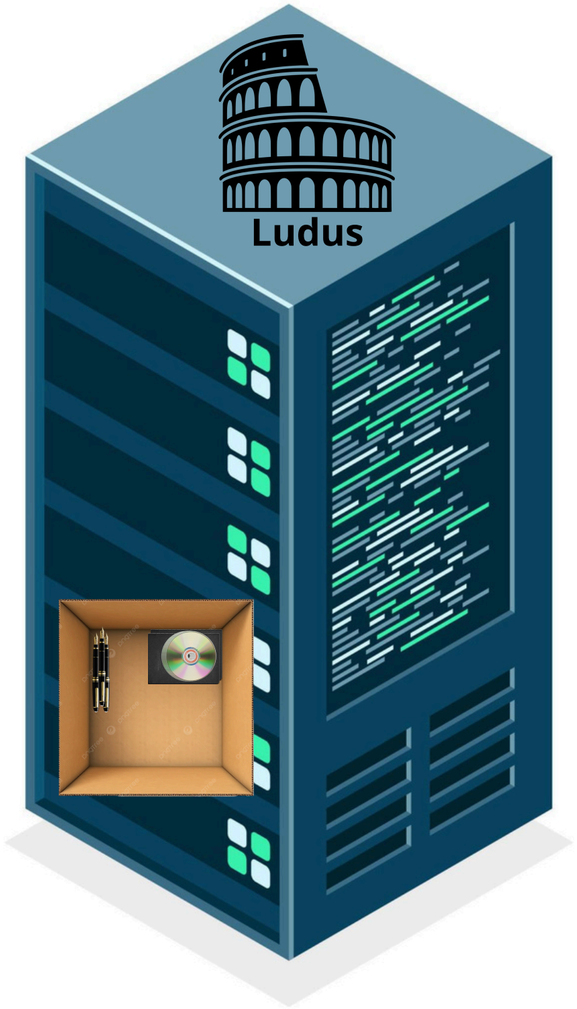
Virtual Machine 1

User 1 User 2 User 3



Virtual Machine 1


Ludus



1 - Installing and configuring the simulations

2 - Deploying and managing the ranges

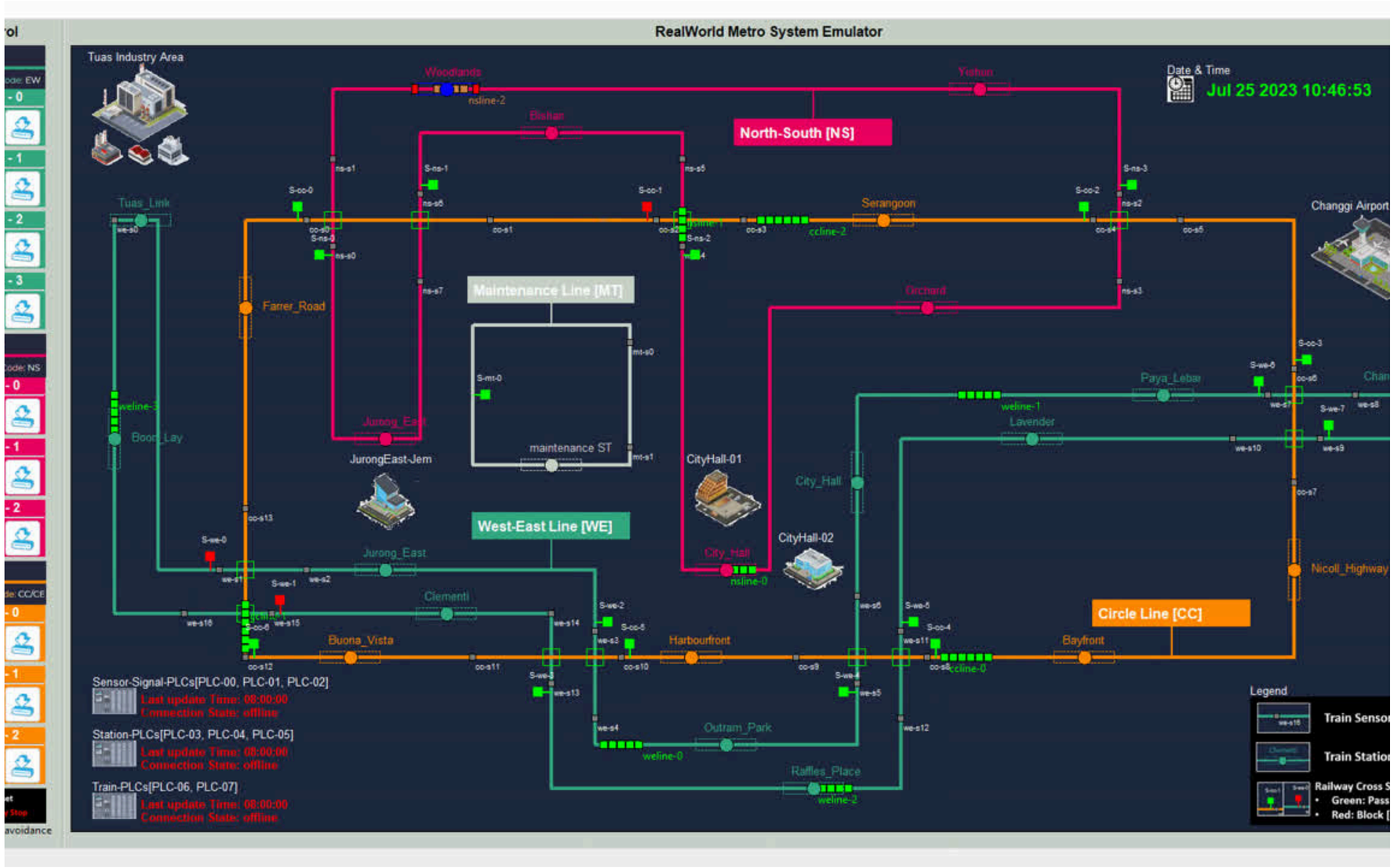
3 - Documenting the processes

II - Existing Situation, Tasks & Difficulties

1 - Installing and configuring the simulations

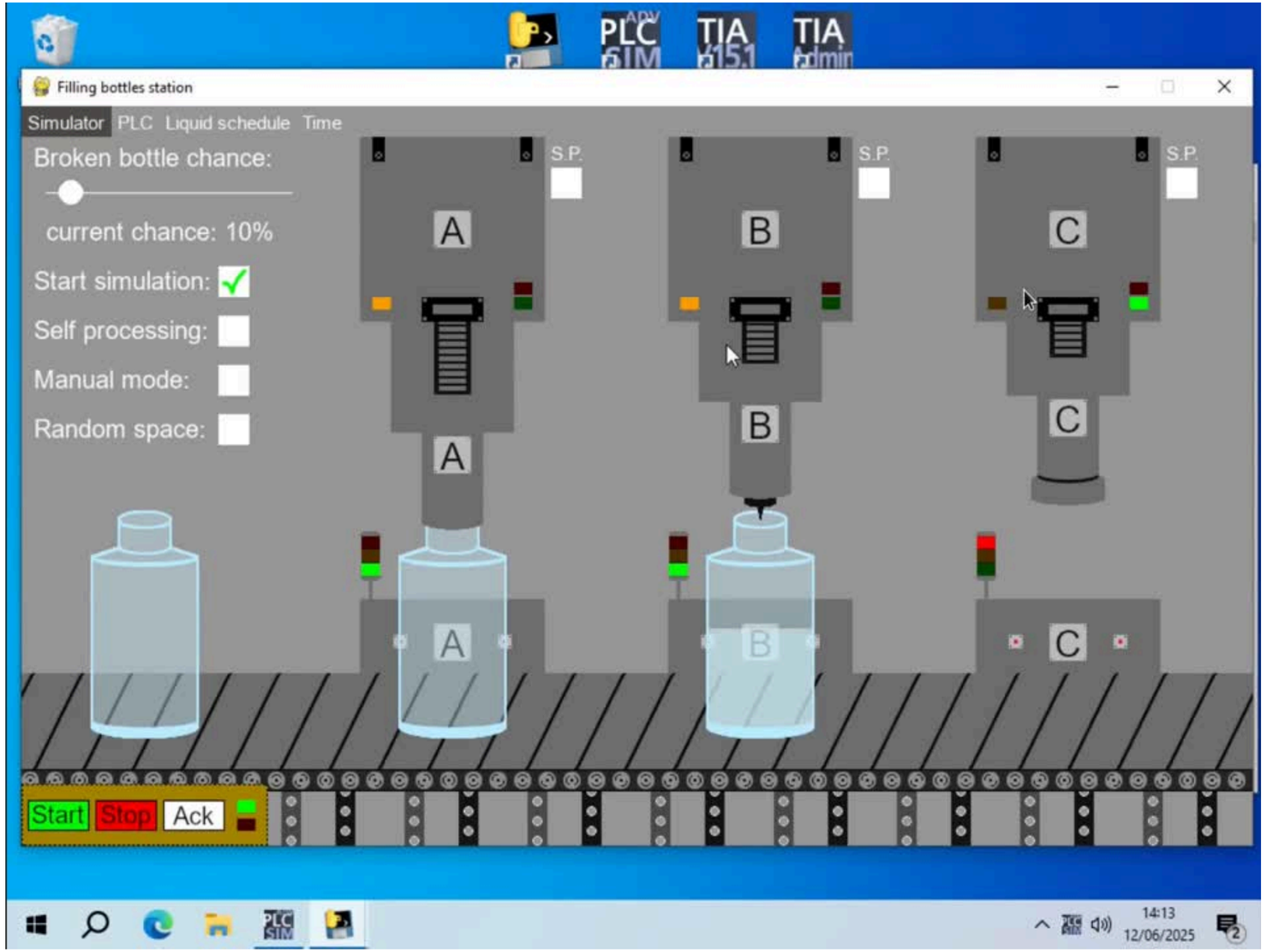
II - Existing Situation, Tasks & Difficulties

1 - Installing and configuring the simulations



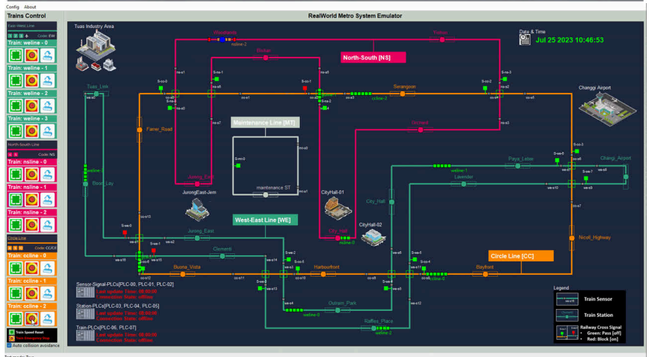
II - Existing Situation, Tasks & Difficulties

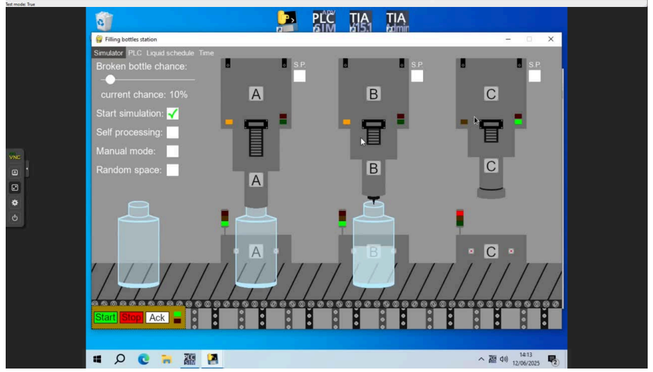
1 - Installing and configuring the simulations



II - Existing Situation, Tasks & Difficulties

1 - Installing and configuring the simulations

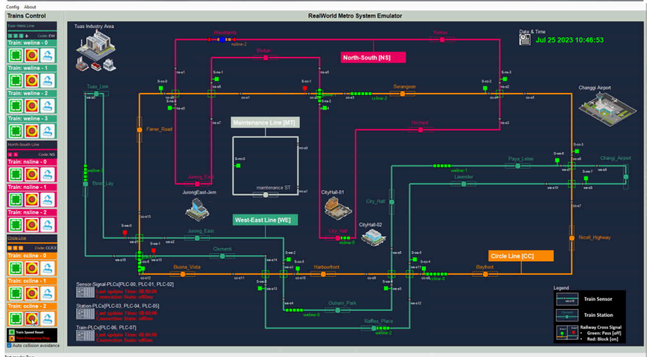


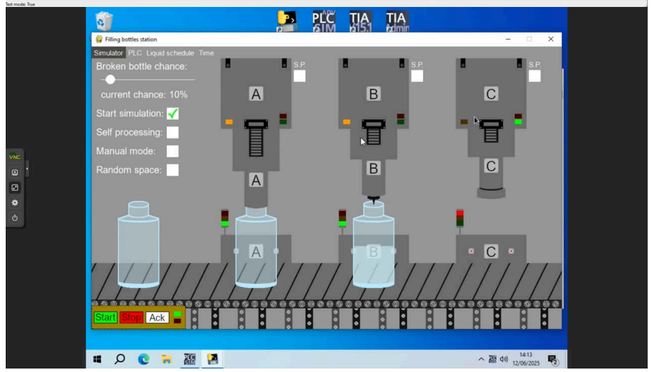


Replicate **real-world industrial systems** in a **controlled environment**

II - Existing Situation, Tasks & Difficulties

1 - Installing and configuring the simulations



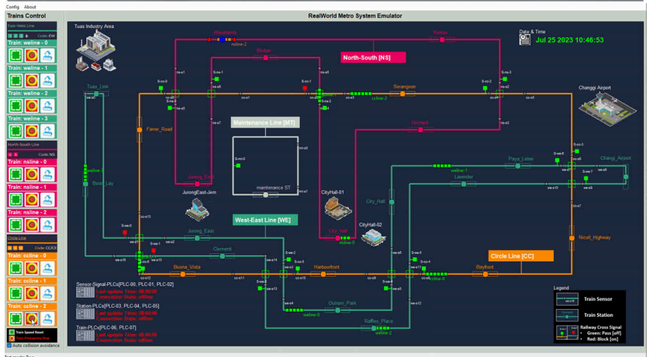


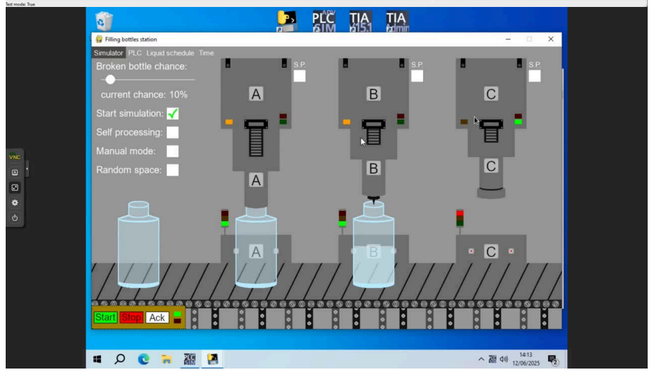
Replicate **real-world industrial systems** in a **controlled environment**

Steep **learning curve**

II - Existing Situation, Tasks & Difficulties

1 - Installing and configuring the simulations





Replicate **real-world industrial systems** in a **controlled environment**

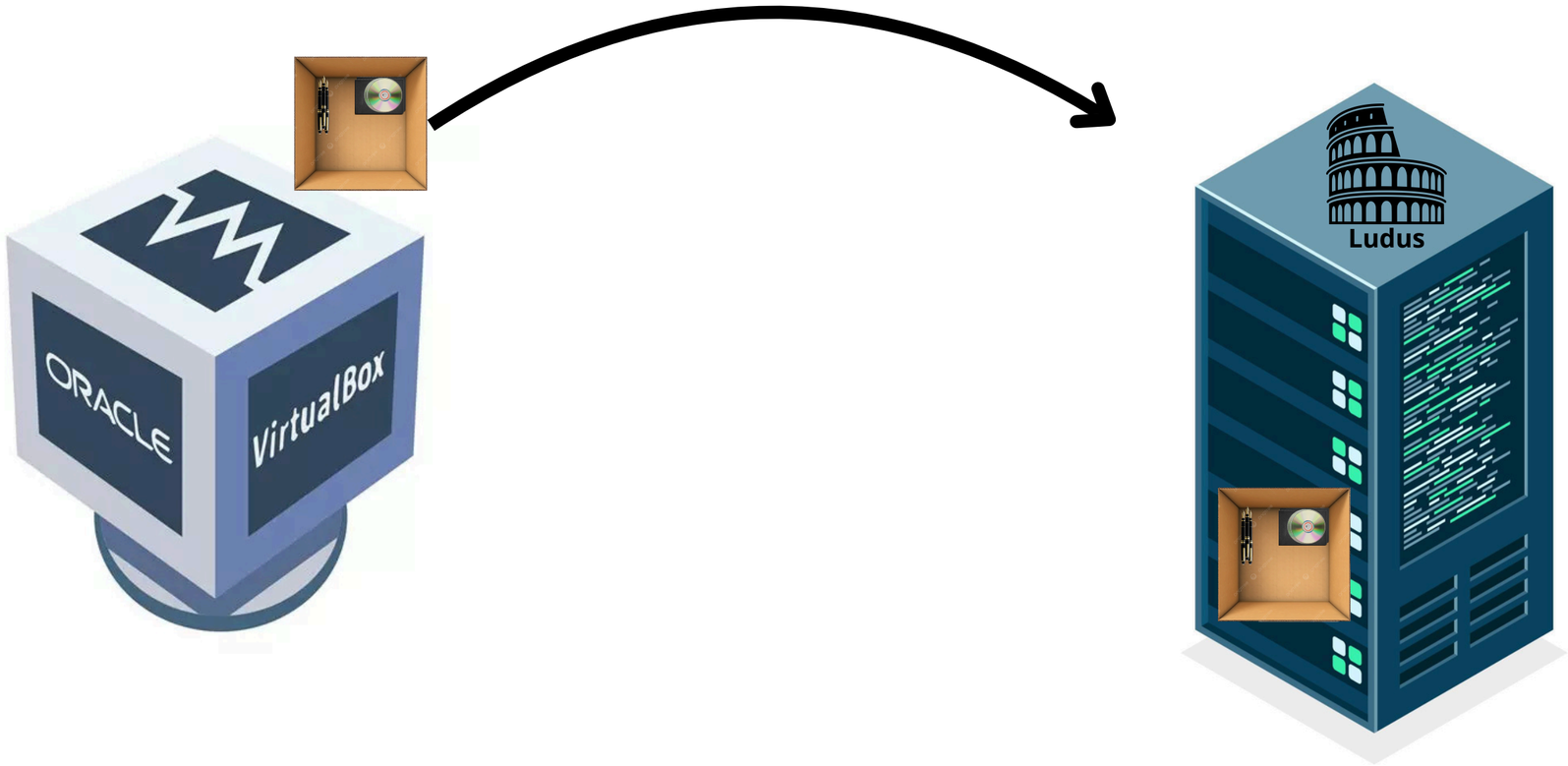
Steep **learning curve**

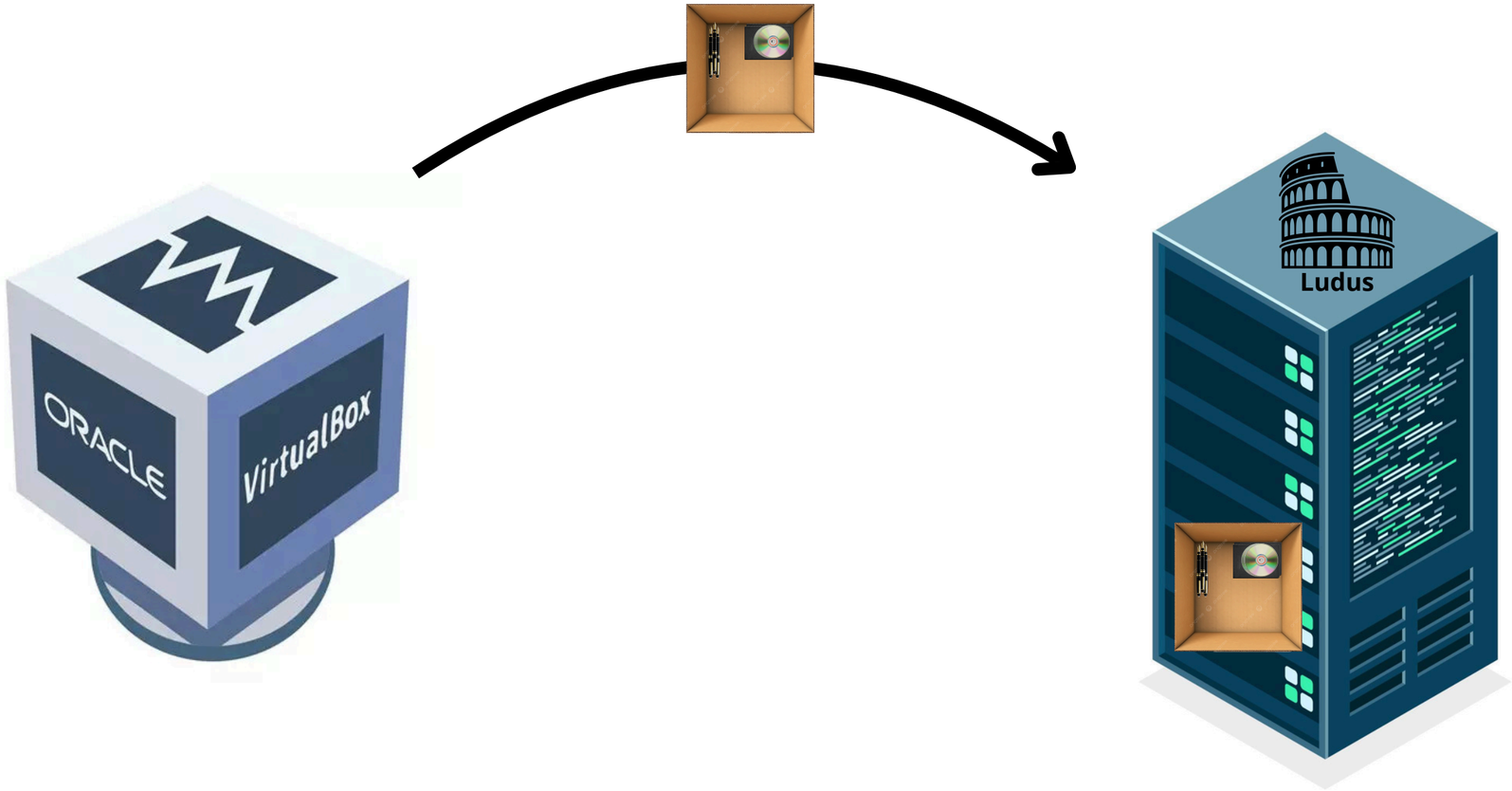
Searching for **solutions online**, **asking colleagues** and **experimenting** until I found what worked

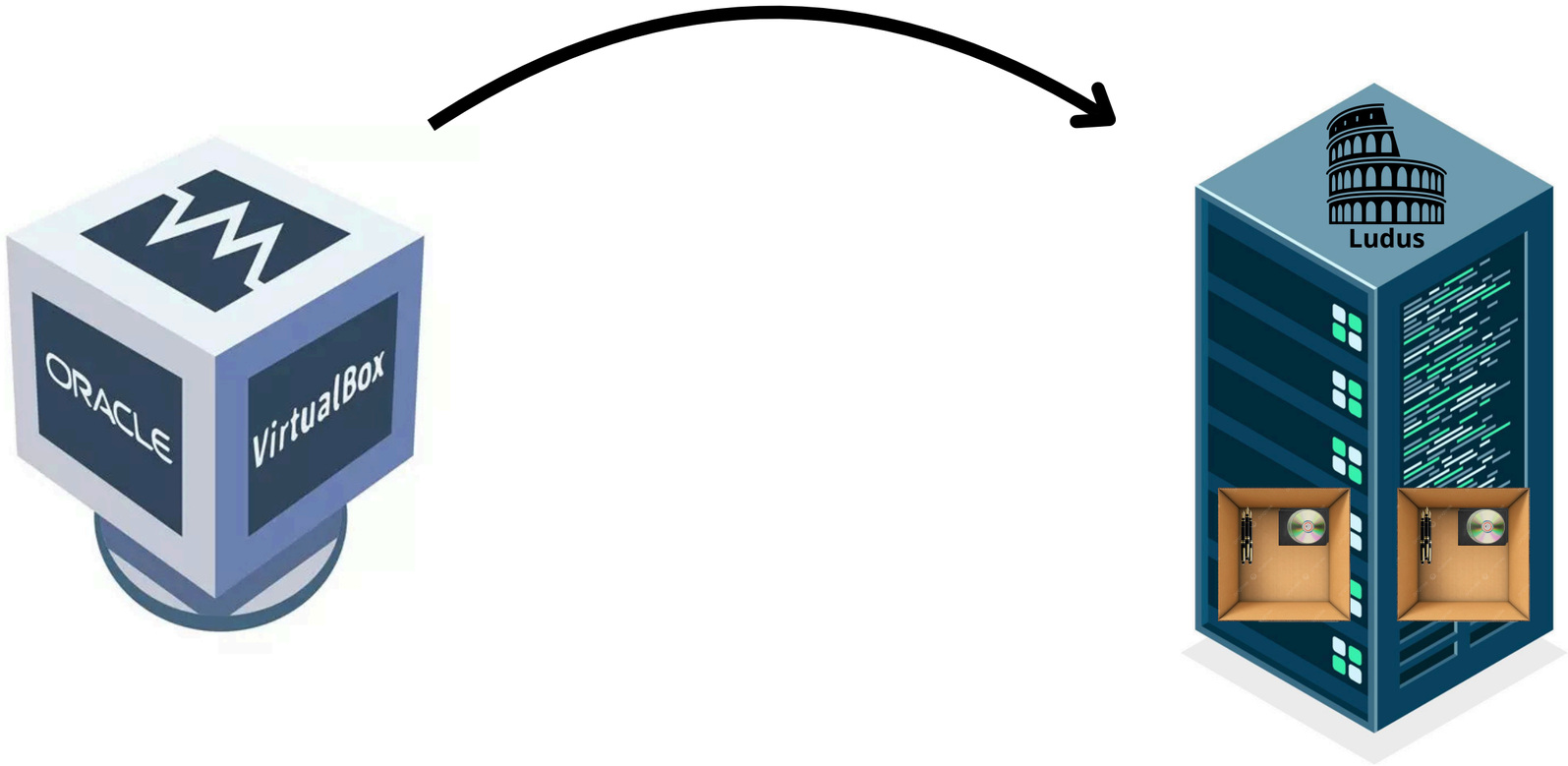
1 - Installing and configuring the simulations

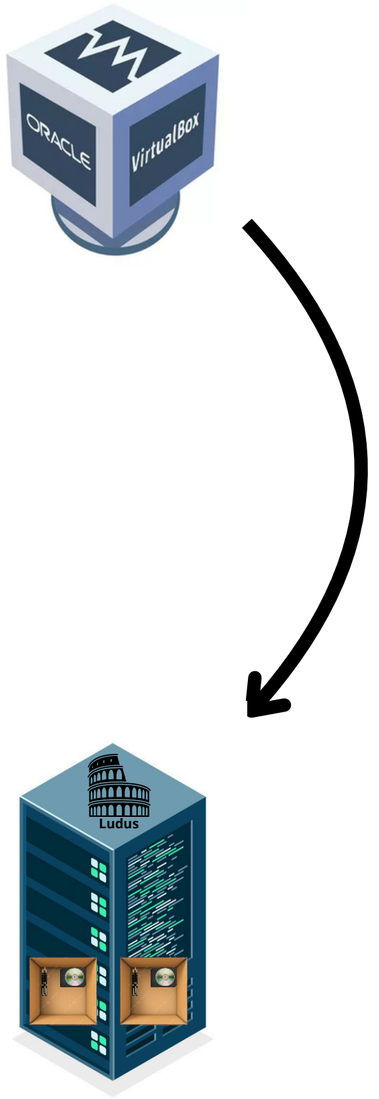
2 - Deploying and managing the ranges

3 - Documenting the processes

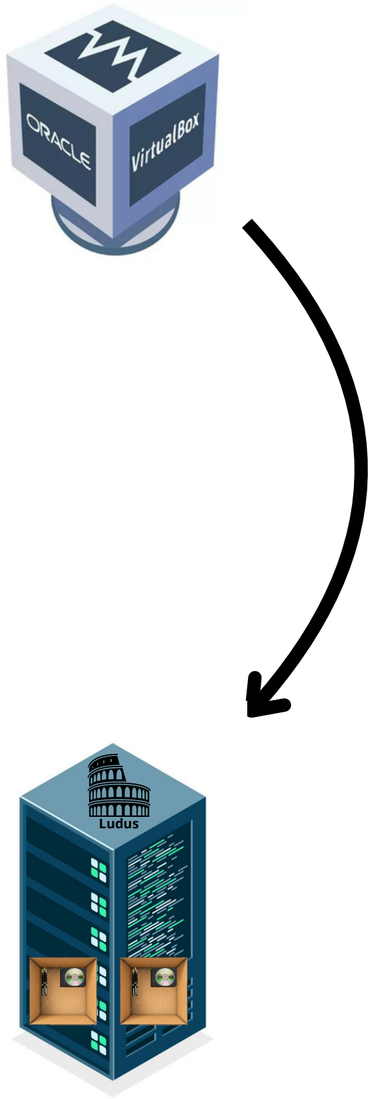

ORACLE
VirtualBox
Ludus


ORACLE
VirtualBox
Ludus


ORACLE
VirtualBox
Ludus

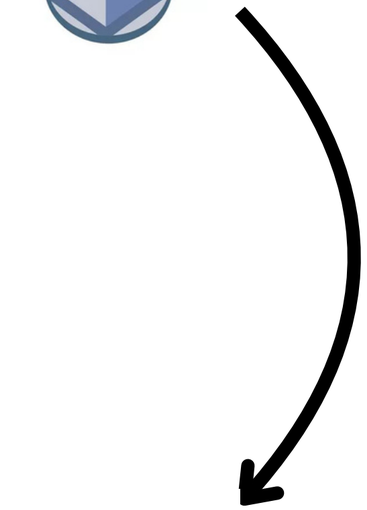


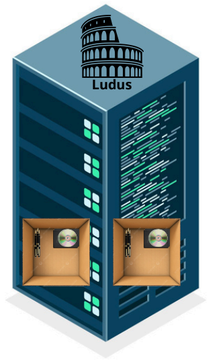
Ensure the range could be **easily duplicated** for different users



Ensure the range could be **easily duplicated** for different users

Time-consuming, especially when dealing with large files or complex network topologies





Ensure the range could be **easily duplicated** for different users

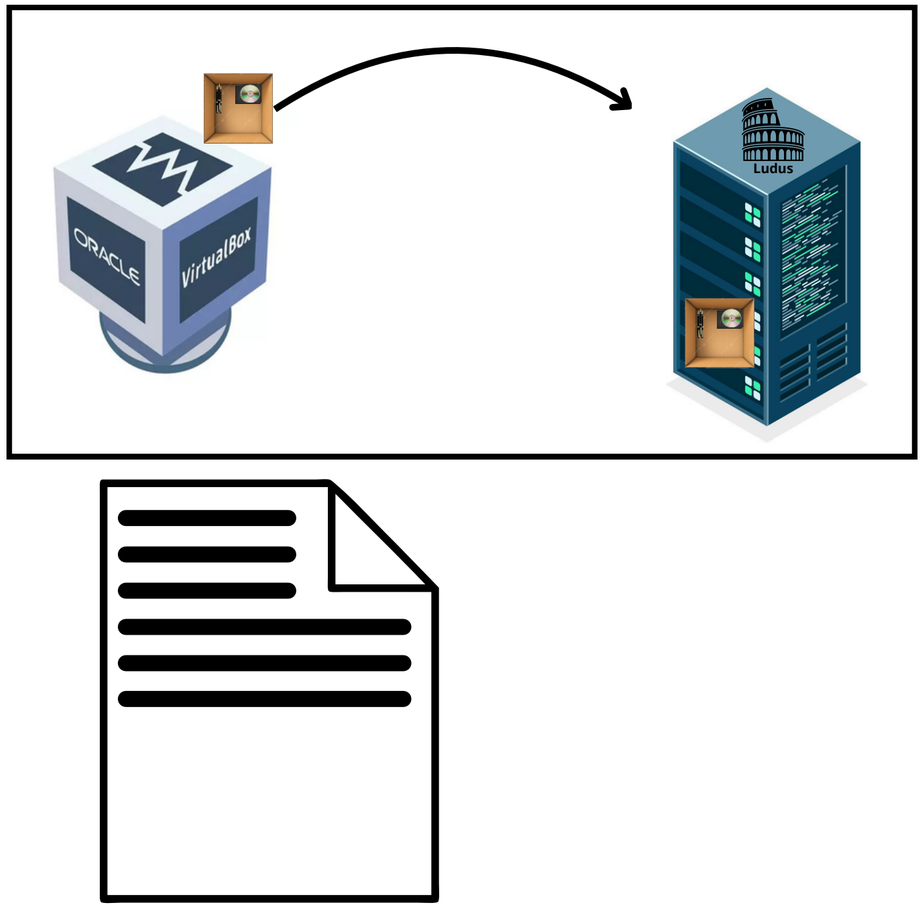
Time-consuming, especially when dealing with large files or complex network topologies

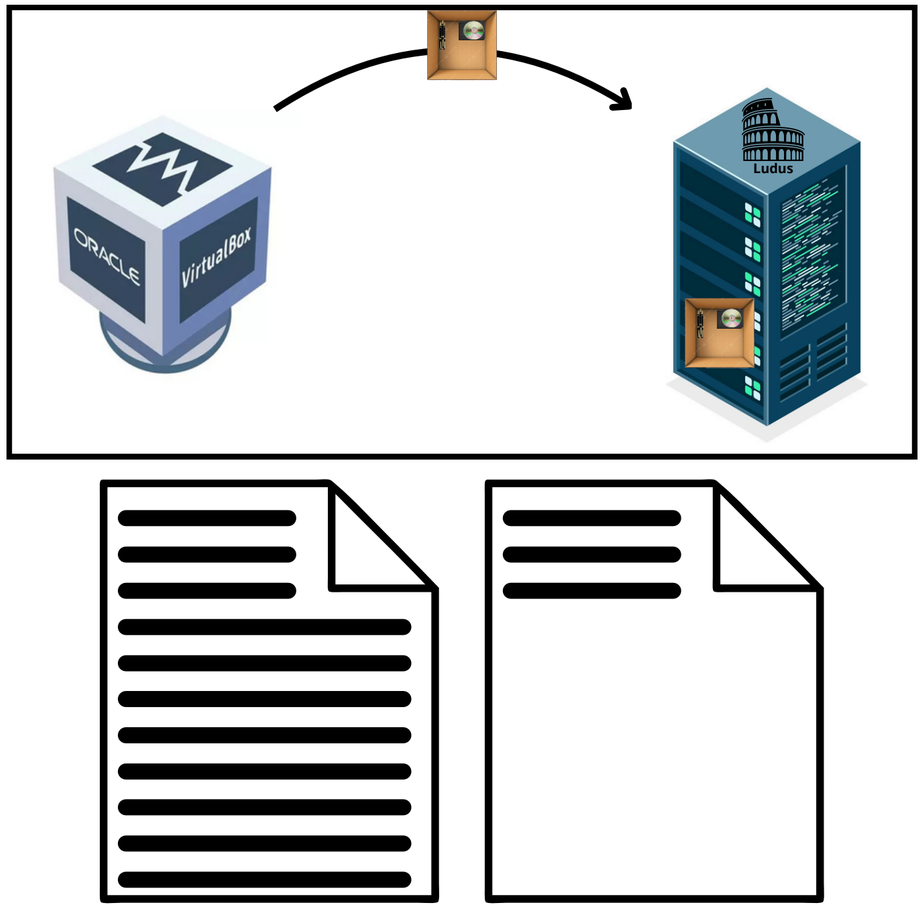
Even **small configurations** could cause **big problems**, leading to hours of debugging

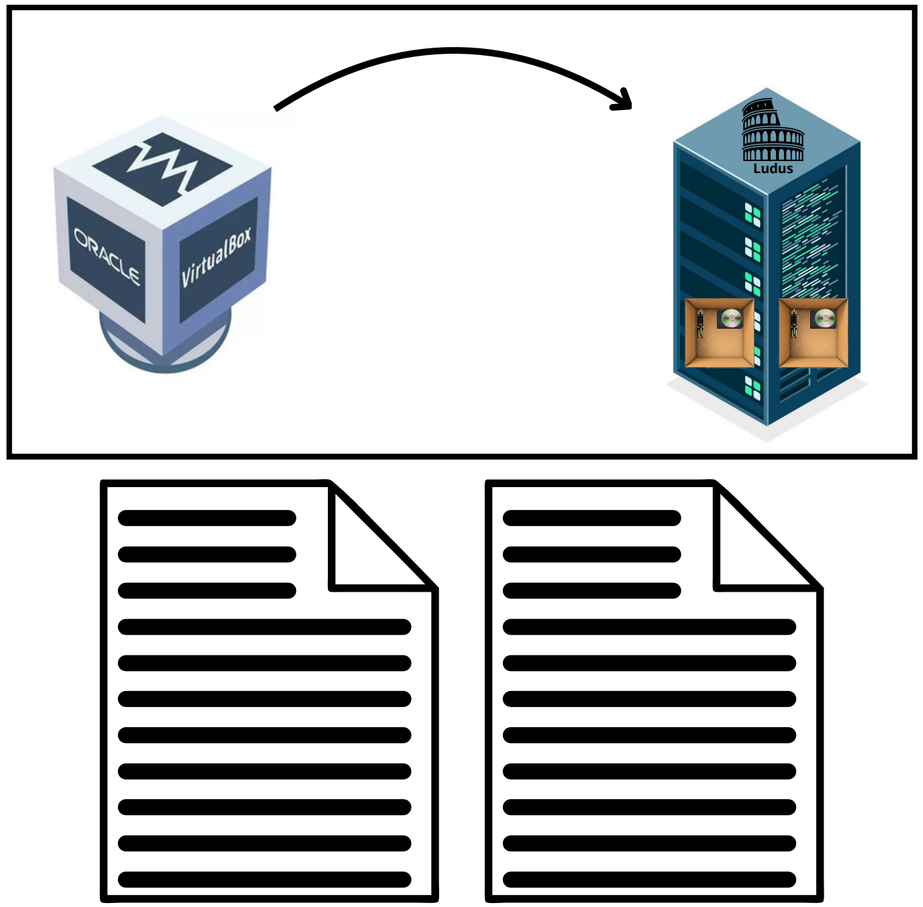
1 - Installing and configuring the simulations

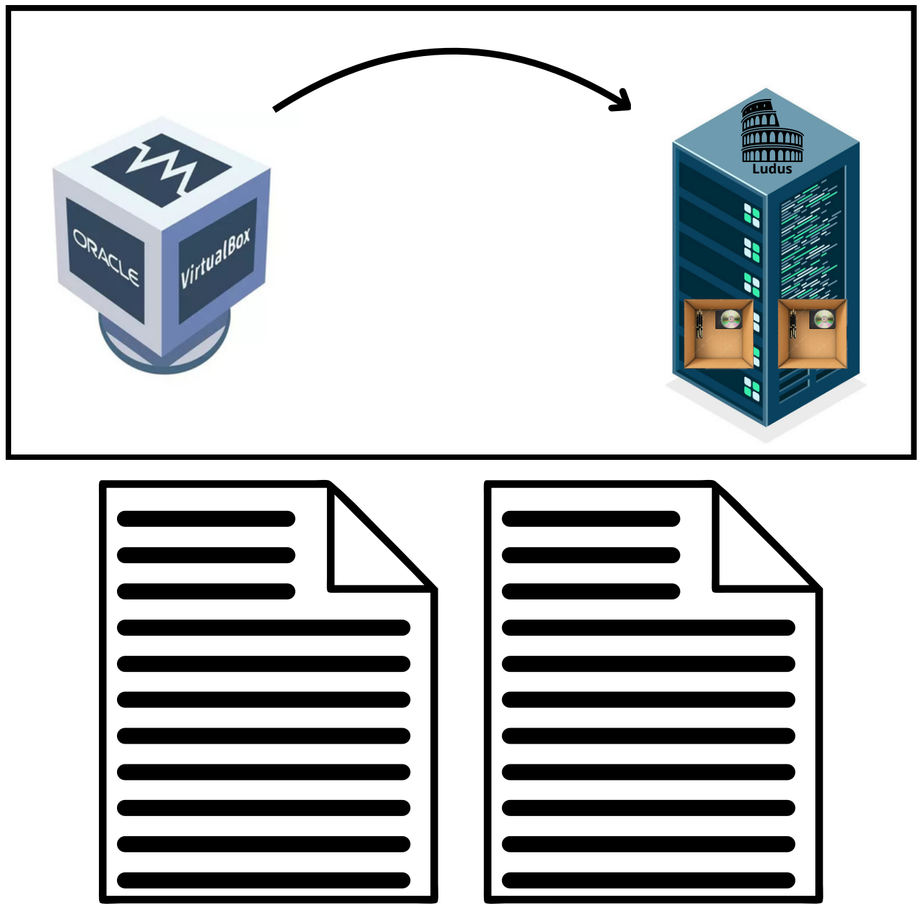
2 - Deploying and managing the ranges

3 - Documenting the processes

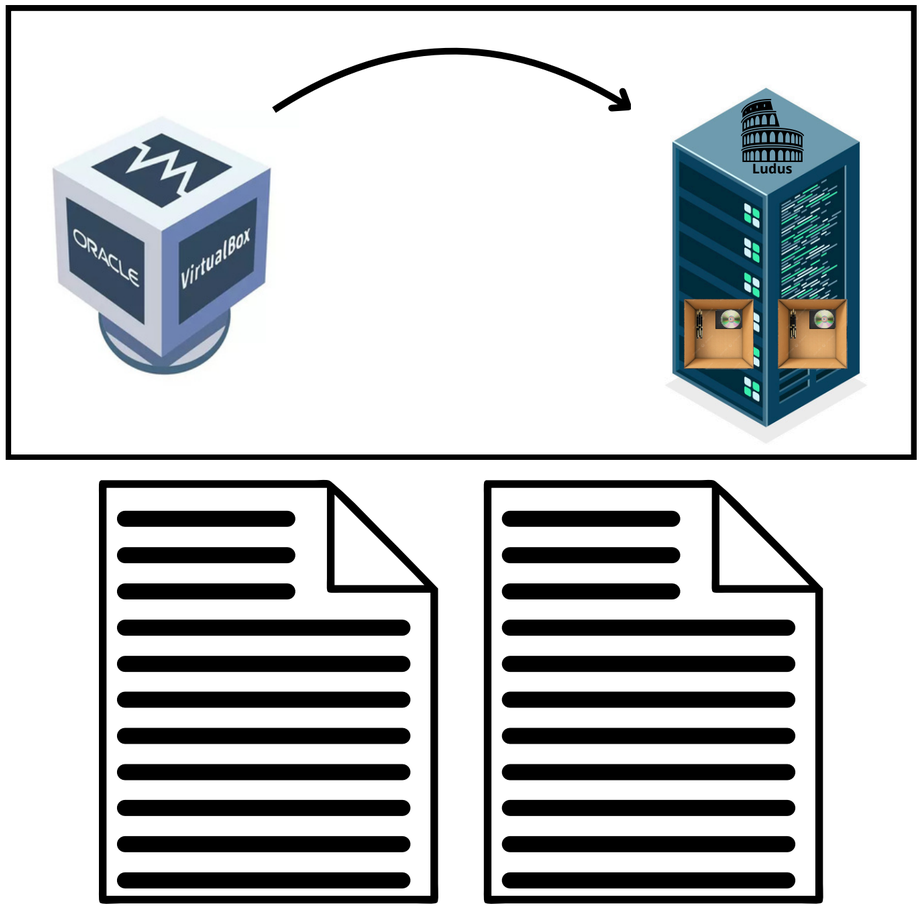

ORACLE
VirtualBox
Ludus


ORACLE
VirtualBox
Ludus


ORACLE
VirtualBox
Ludus

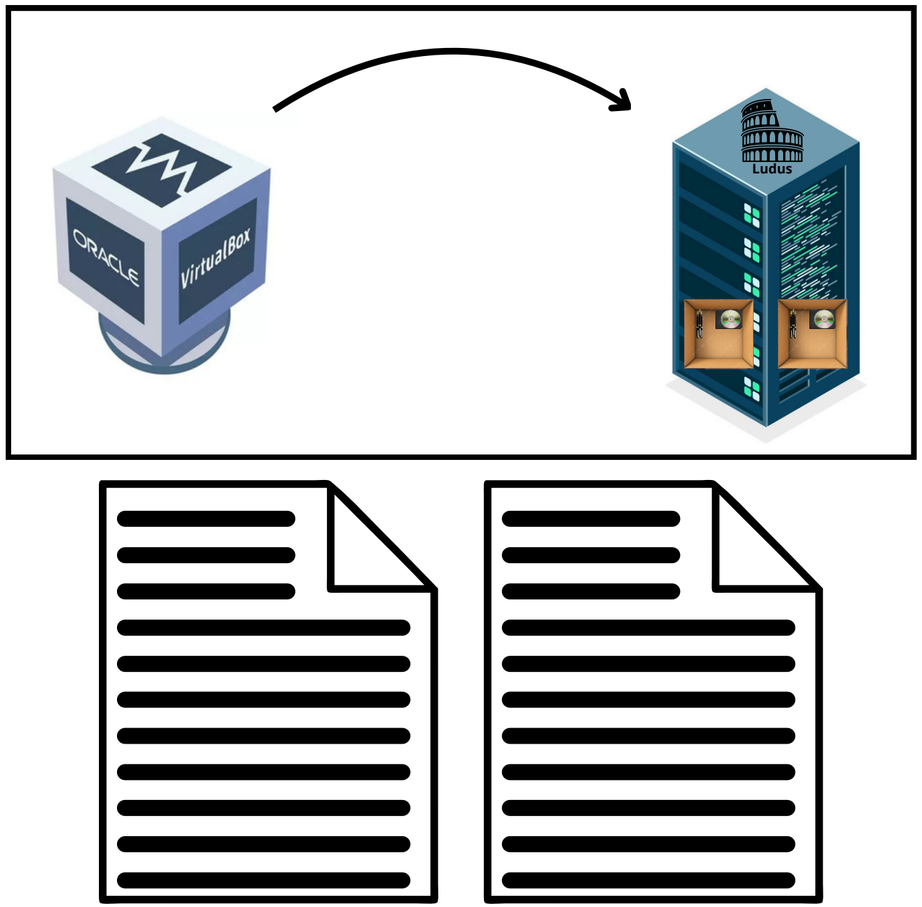


Anyone on the team could **easily replicate** what I had done



Anyone on the team could **easily replicate** what I had done

The amount of **time and focus** it required



Anyone on the team could **easily replicate** what I had done

The amount of **time and focus** it required

Hard to stay motivated, particularly when I had **to repeat processes**

1 - Installing and configuring the simulations

2 - Deploying and managing the ranges

3 - Documenting the processes

1 - Installing and configuring the simulations

2 - Deploying and managing the ranges

3 - Documenting the processes

Bonus - Others


Backdoors
&Breaches

II - Existing Situation, Tasks & Difficulties

Bonus - Others

I - Host Organization & Problematic

II - Existing Situation, Tasks & Difficulties

III - Tools, Gantt Planning & Personal Organization

IV - The 3 main projects

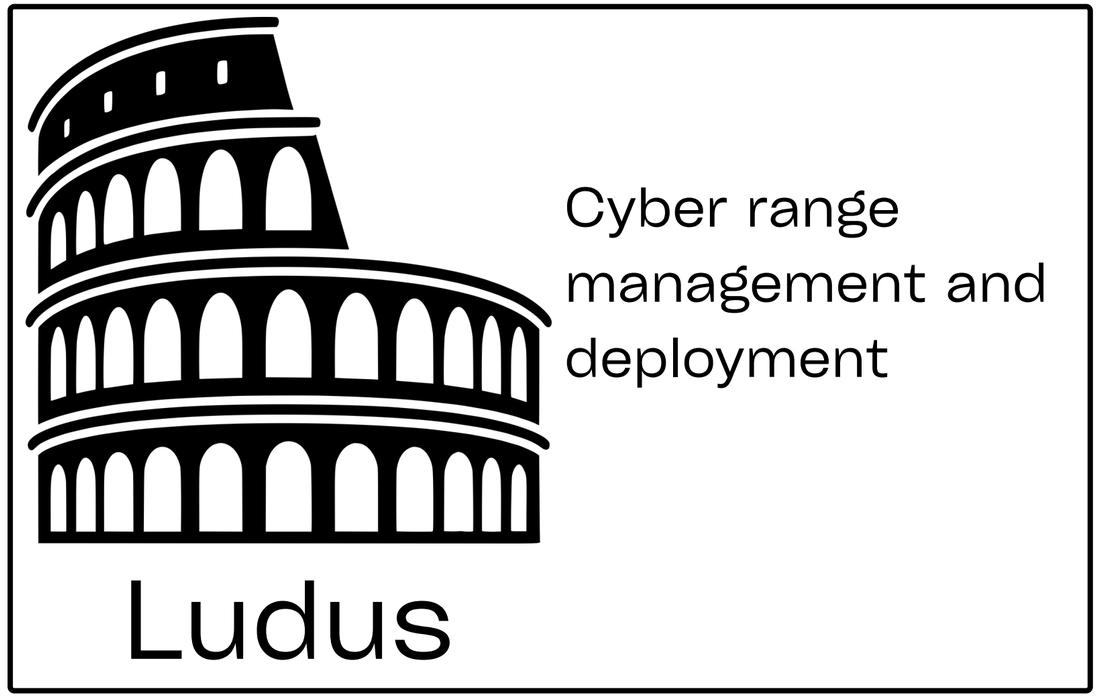
V - Current VS Initial situation, Technical & Human Assessment

III - Tools, Gantt Planning & Personal Organization

1 - Tools and programming languages

2 - Gantt diagram

3 - Personal Organisation

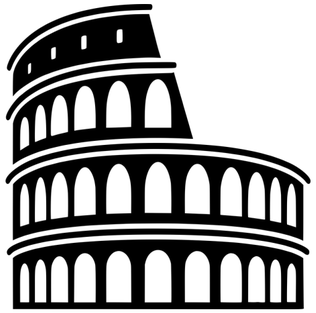

Cyber range
management and
deployment
Ludus

Ludus

Cyber range
man
depl

Local virtual machine management and simulation

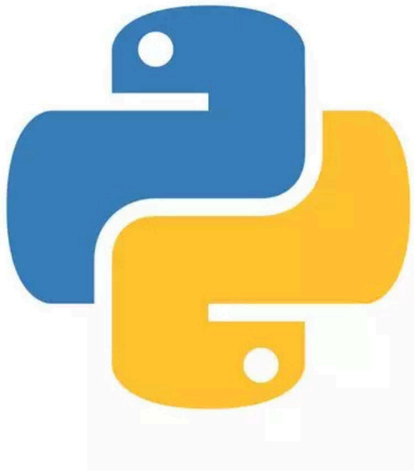
VirtualBox



Ludus

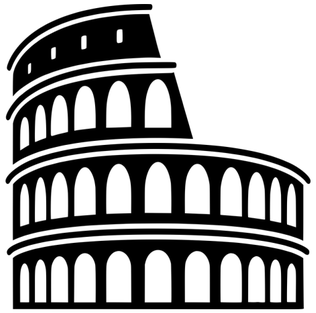
Cyber range
man
depl

Local virtual



Very easy and complete programming language used in most projects

Python



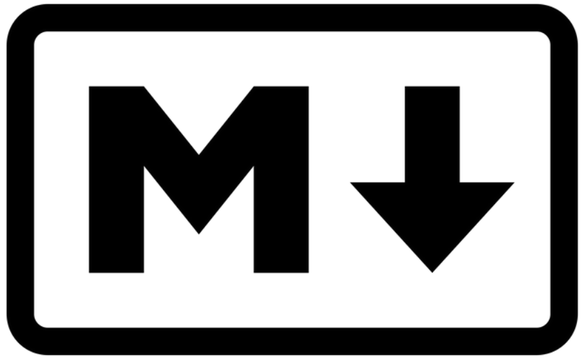
Ludus

Cyber range
man
depl

Local virtual

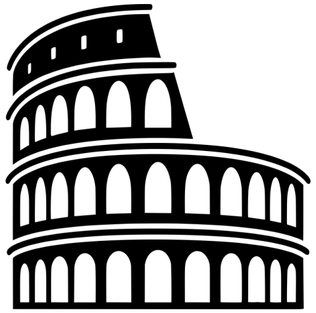
Very easy and complete programming language used in most projects

n



Format documentation before converting into Sphinx

Markdown



Ludus

Cyber range
man
depl

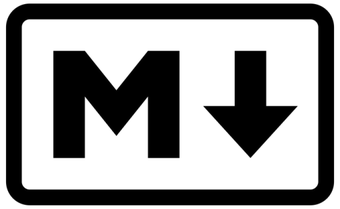
Local virtual

Very easy and complete programming language used in most projects

n

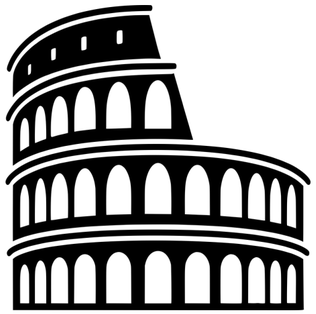
Internal Communication

Teams



Markdown

F
d
b
c
Sphinx



Ludus

Cyber range
man
depl

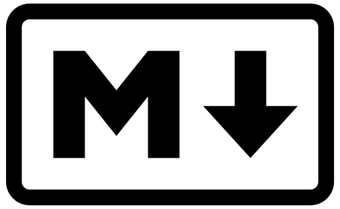
Local virtual

Very easy and complete programming language used in most projects

n

To save, keep track of and share my modifications to projects

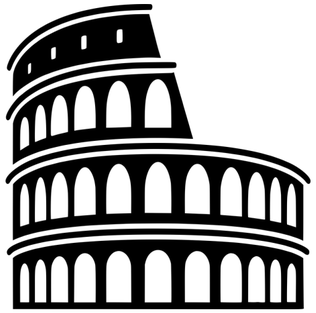
Github



Markdown

F
d
b
c
Sphinx

Teams

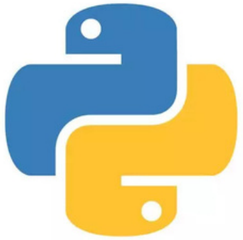


Ludus

Cyber range management and deployment

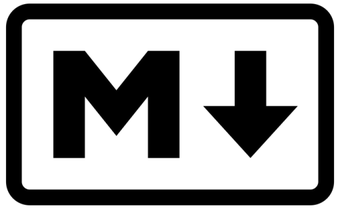
VirtualBox

Local virtual machine management and simulation



Python

Very easy and complete programming language used in most projects



Markdown

Format documentation before converting into Sphinx

Teams

Internal Communication

Github

To save, keep track of and share my modifications to projects

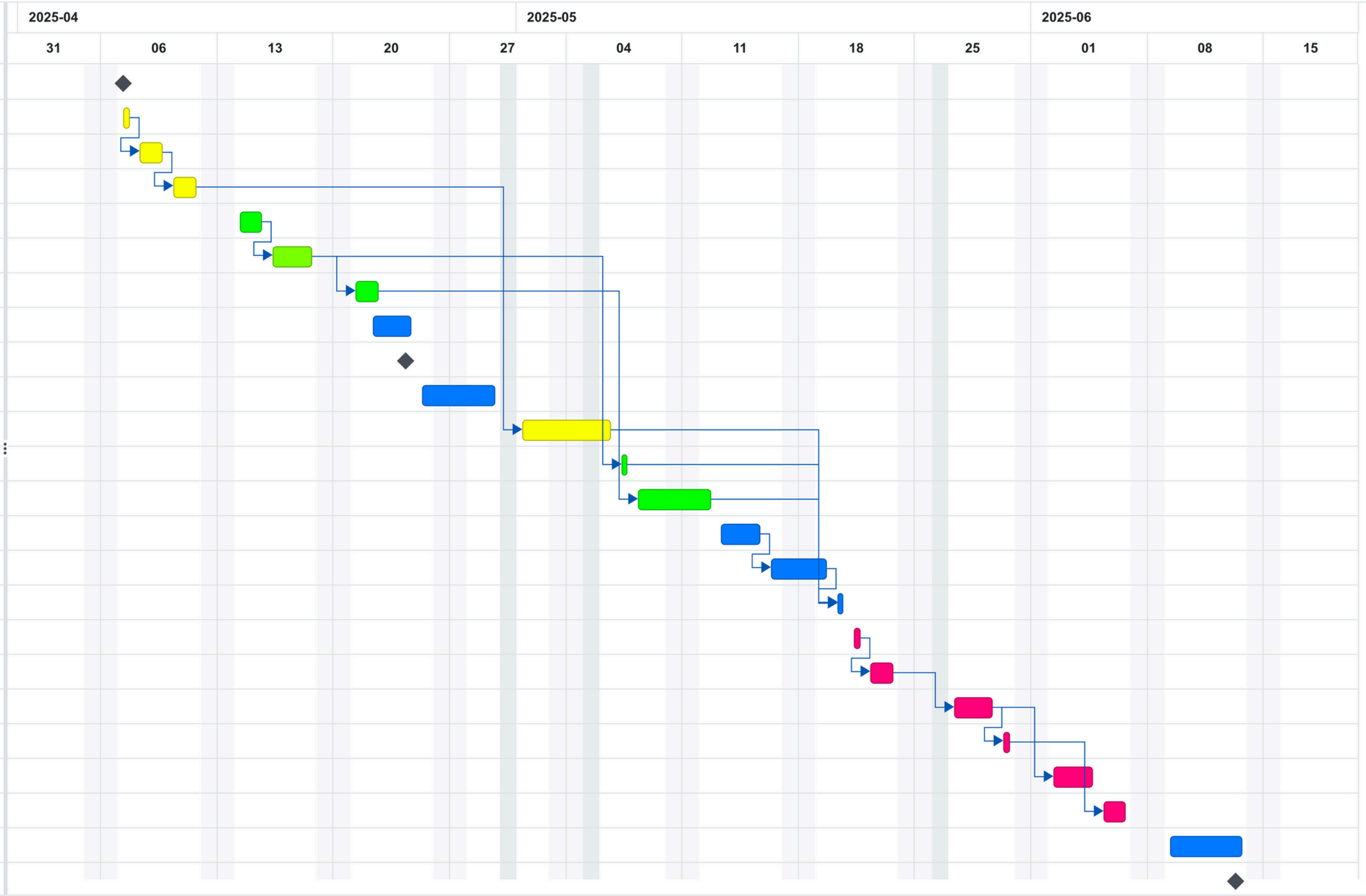
III - Tools, Gantt Planning & Personal Organization

1 - Tools and programming languages

2 - Gantt diagram

3 - Personal Organisation

ID	Task Name
22	First Day
1	Exploring the GRFICS project
2	Understand how Ludus works
3	Configure the GRFICS project in the Ludus
5	Understand the Metro Railway project
6	Implement an attack in the Metro Railway
8	Install the Metro railway in the Ludus
20	Create videos to present the GRFICS and Met…
23	Visit from DSIT
19	Set up a multi-instances VLC Controller
4	Document how I installed the GRFICS project …
7	Document how to attack the Metro Railway
9	Document how I installed the Metro Railway p…
10	Reinstall a new Ludus in an empty server
11	Document the installation of the Ludus
12	Merge all the documentations in one file
13	Understand the Bottle Filling project
14	Install the Bottle Filling project to make it work
15	Configure the PLC in the Bottle Filling project t…
17	Install the Bottle Filling project in the Ludus
16	Document the configuration of the PLC in the …
18	Document the installation of the Bottle Filling p…
21	Prepare this presentation
24	Last day



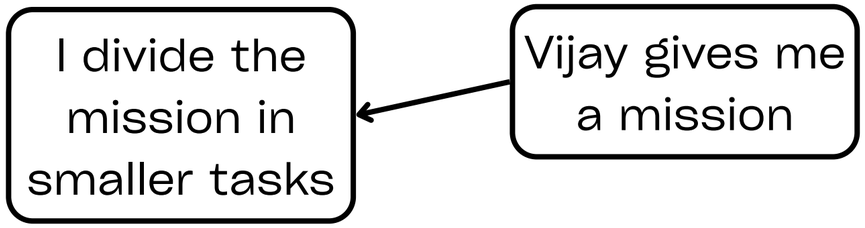
III - Tools, Gantt Planning & Personal Organization

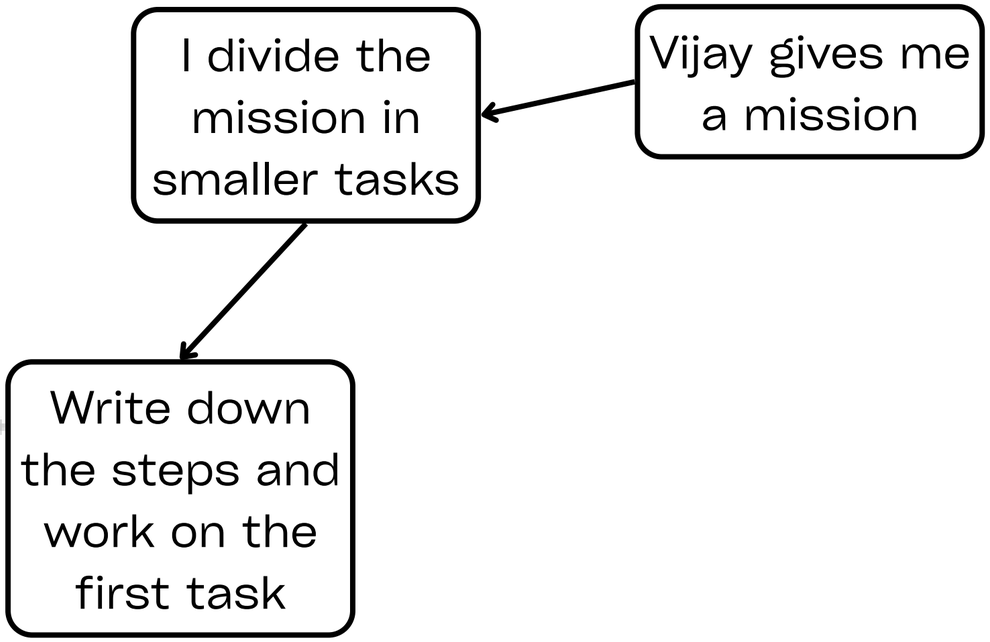
1 - Tools and programming languages

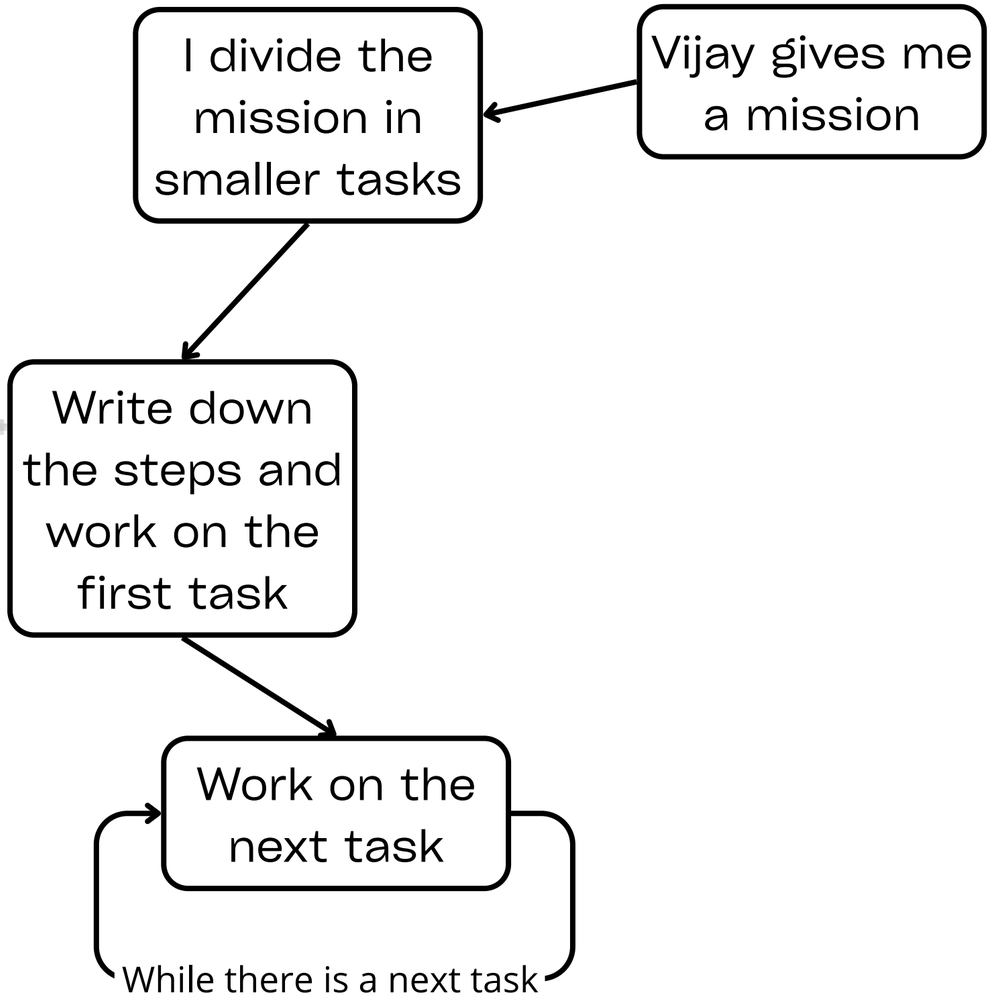
2 - Gantt diagram

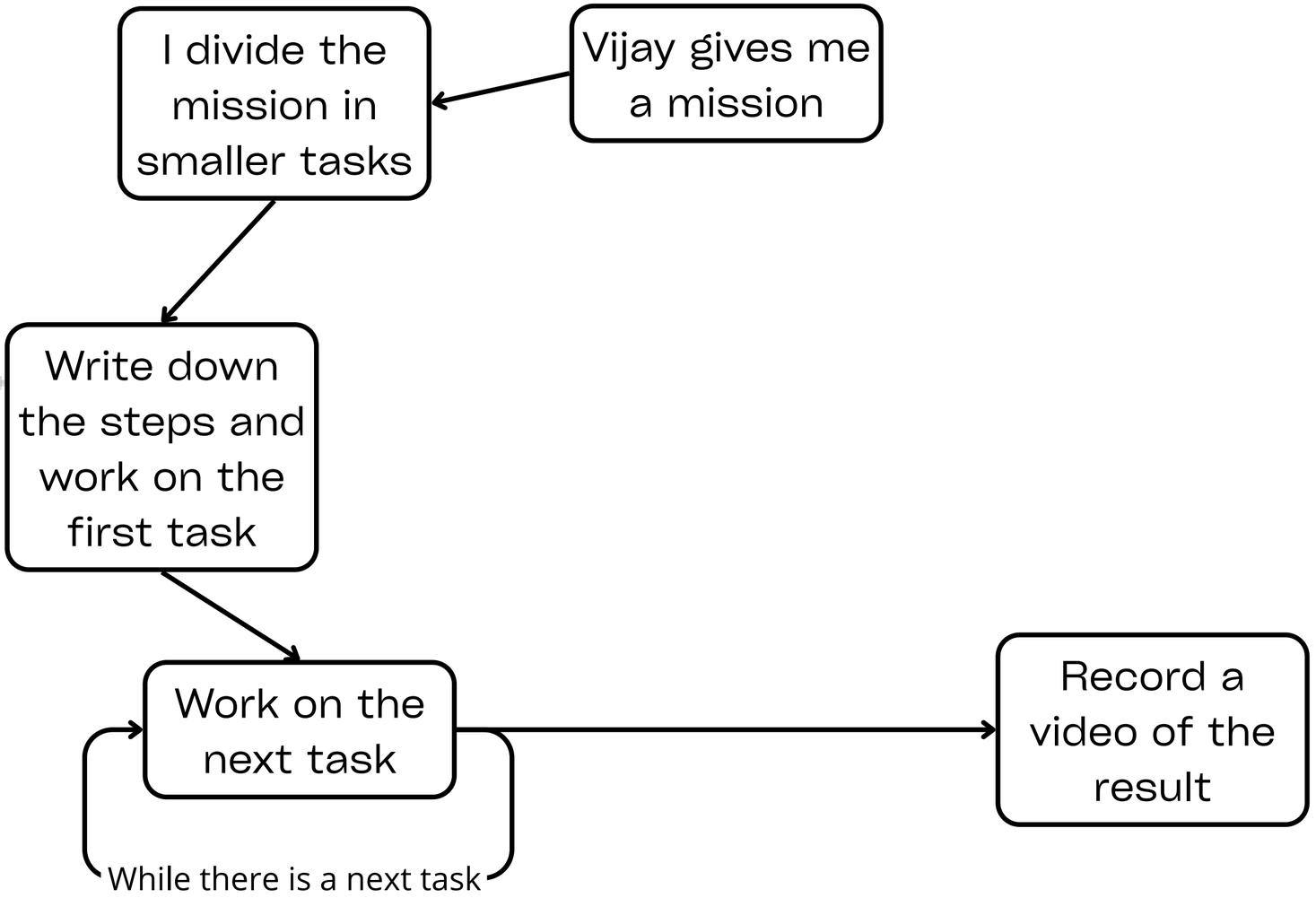
3 - Personal Organisation

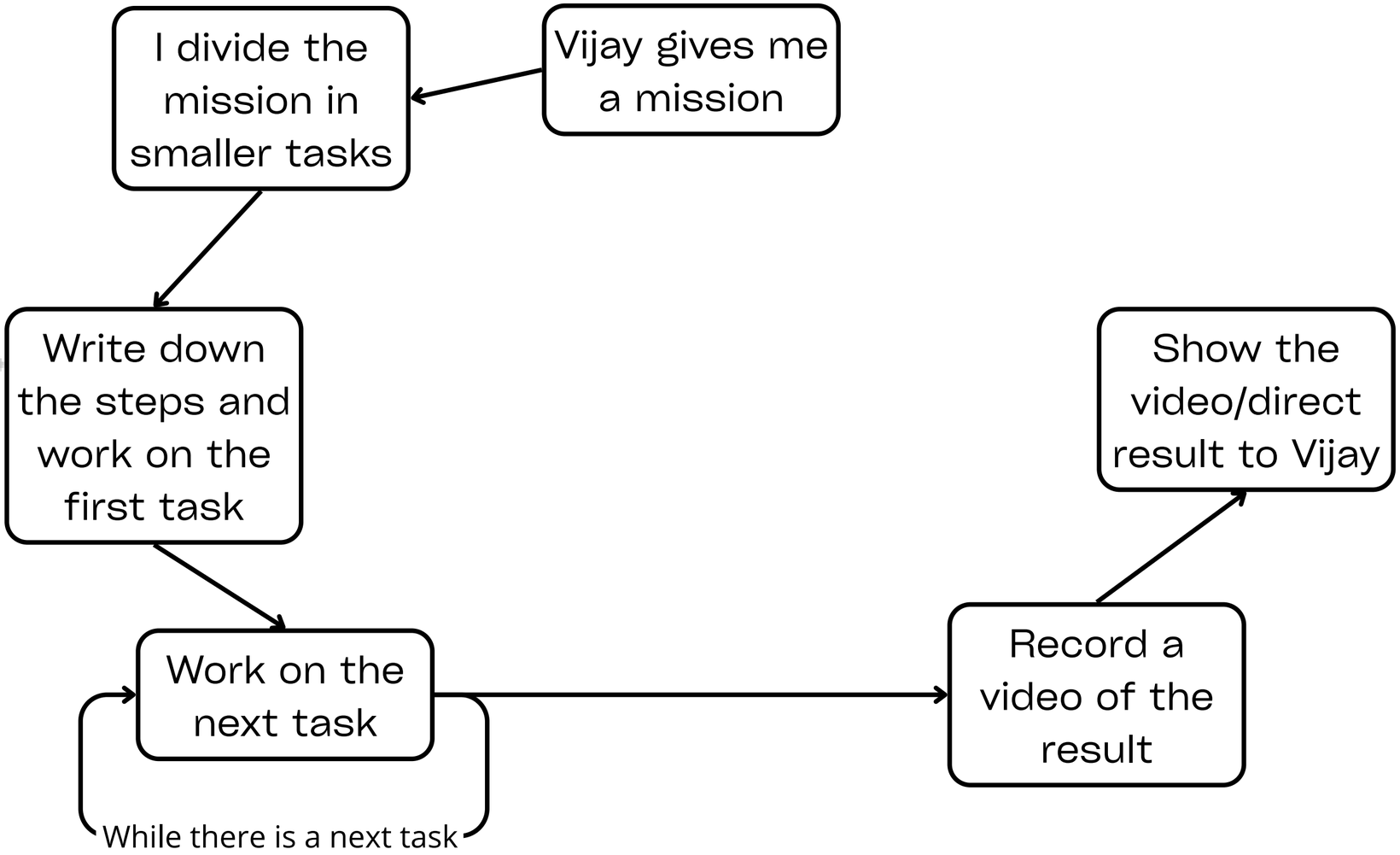
Vijay gives me
a mission

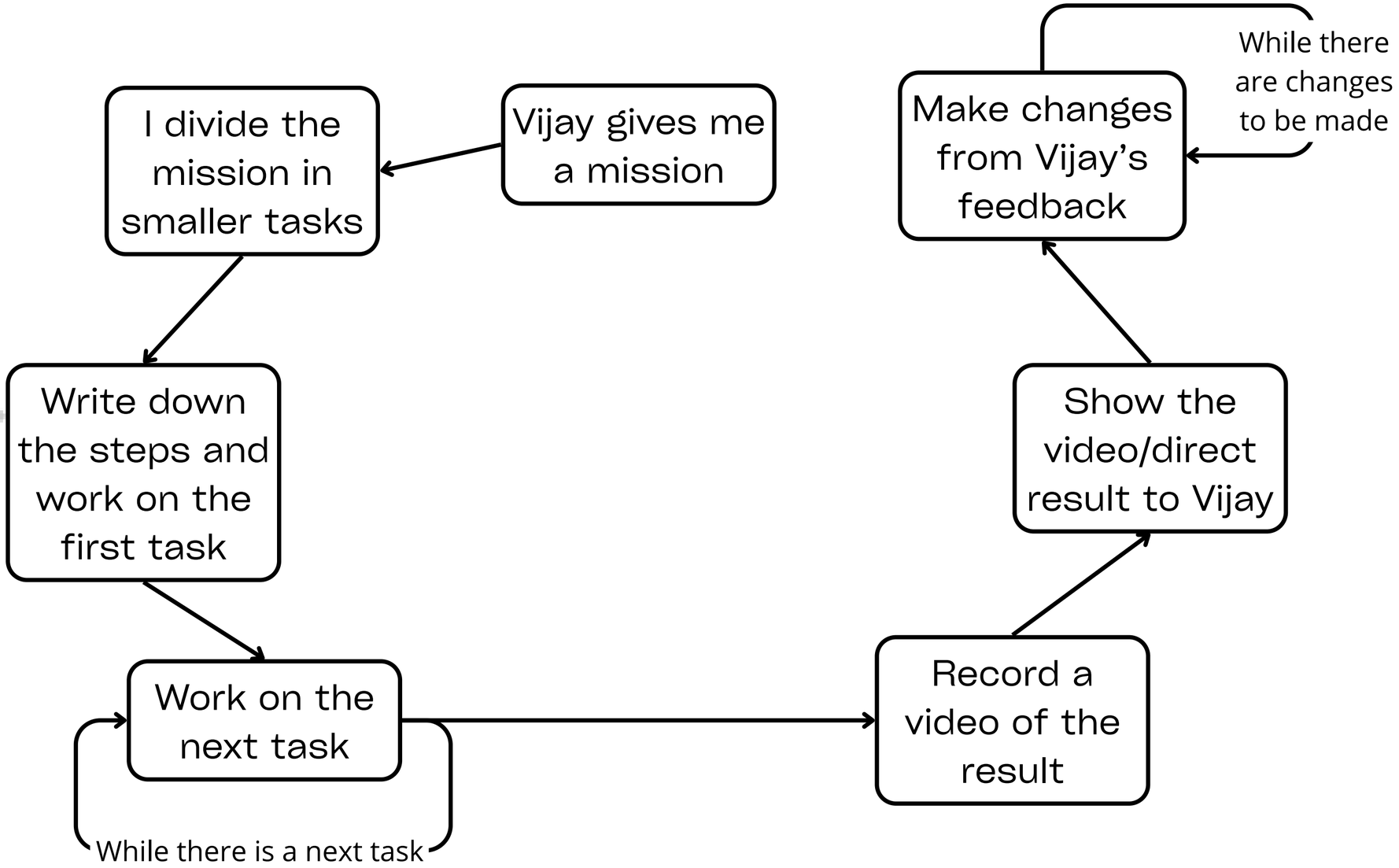

I divide the mission in smaller tasks
Vijay gives me a mission

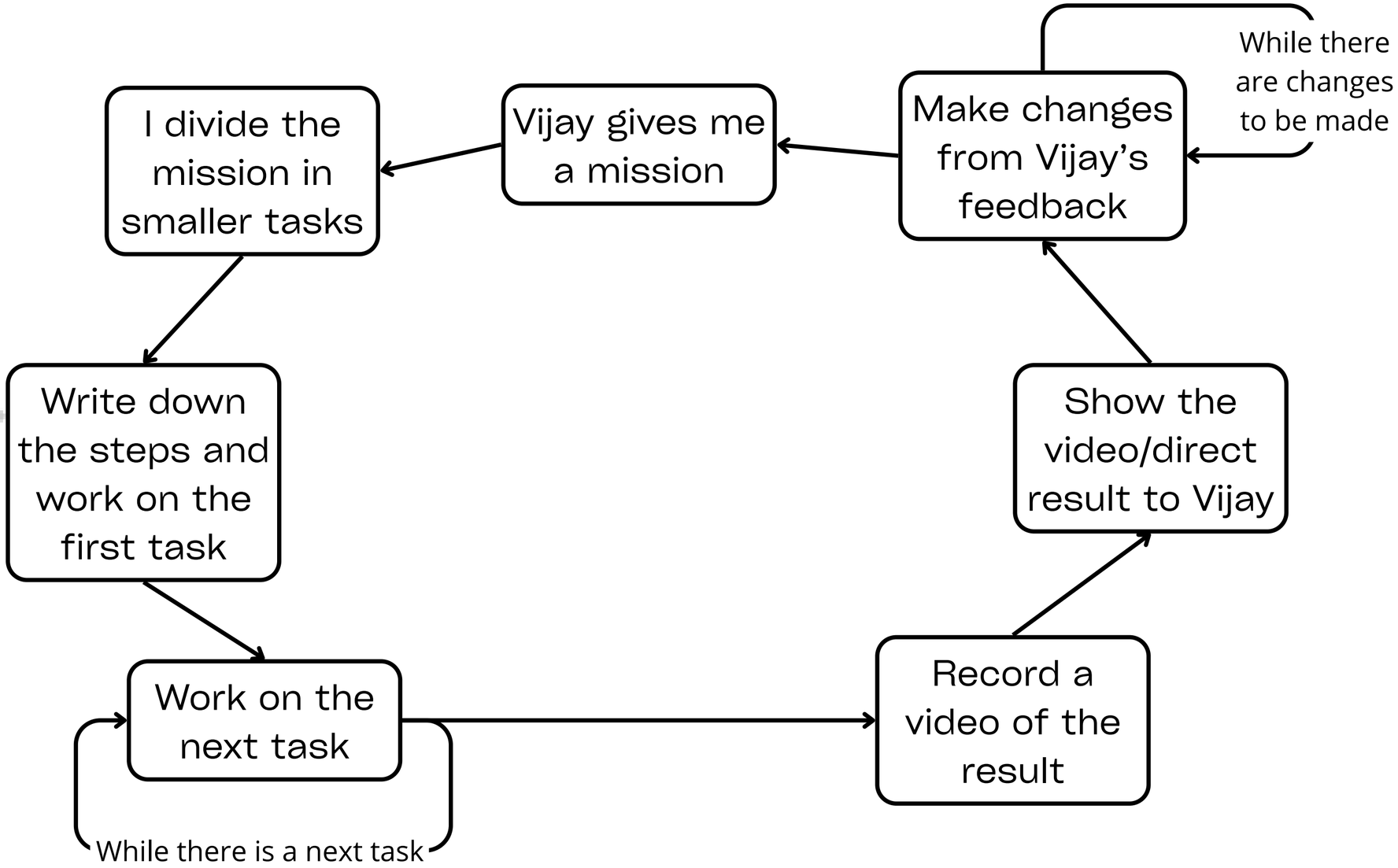

I divide the mission in smaller tasks
Vijay gives me a mission
Write down the steps and work on the first task


I divide the mission in smaller tasks
Vijay gives me a mission
Write down the steps and work on the first task
Work on the next task
While there is a next task


I divide the mission in smaller tasks
Vijay gives me a mission
Write down the steps and work on the first task
Work on the next task
While there is a next task
Record a video of the result


I divide the mission in smaller tasks
Vijay gives me a mission
Write down the steps and work on the first task
Work on the next task
While there is a next task
Record a video of the result
Show the video/direct result to Vijay


Vijay gives me a mission
I divide the mission in smaller tasks
Write down the steps and work on the first task
Work on the next task
While there is a next task
Record a video of the result
Show the video/direct result to Vijay
Make changes from Vijay's feedback
While there are changes to be made


While there are changes to be made
Make changes from Vijay's feedback
Vijay gives me a mission
I divide the mission in smaller tasks
Write down the steps and work on the first task
Work on the next task
While there is a next task
Record a video of the result
Show the video/direct result to Vijay

I - Host Organization & Problematic

II - Existing Situation, Tasks & Difficulties

III - Tools, Gantt Planning & Personal Organization

IV - The 3 main projects

V - Current VS Initial situation, Technical & Human Assessment

IV - The 3 main projects

1 - GRFICS

2 - Cardiff Metro Emulator

3 - Bottle Filling Plant

IV - The 3 main projects

1 - GRFICS

IV - The 3 main projects

1 - GRFICS

Graphical Realism Framework for Industrial Control Simulation

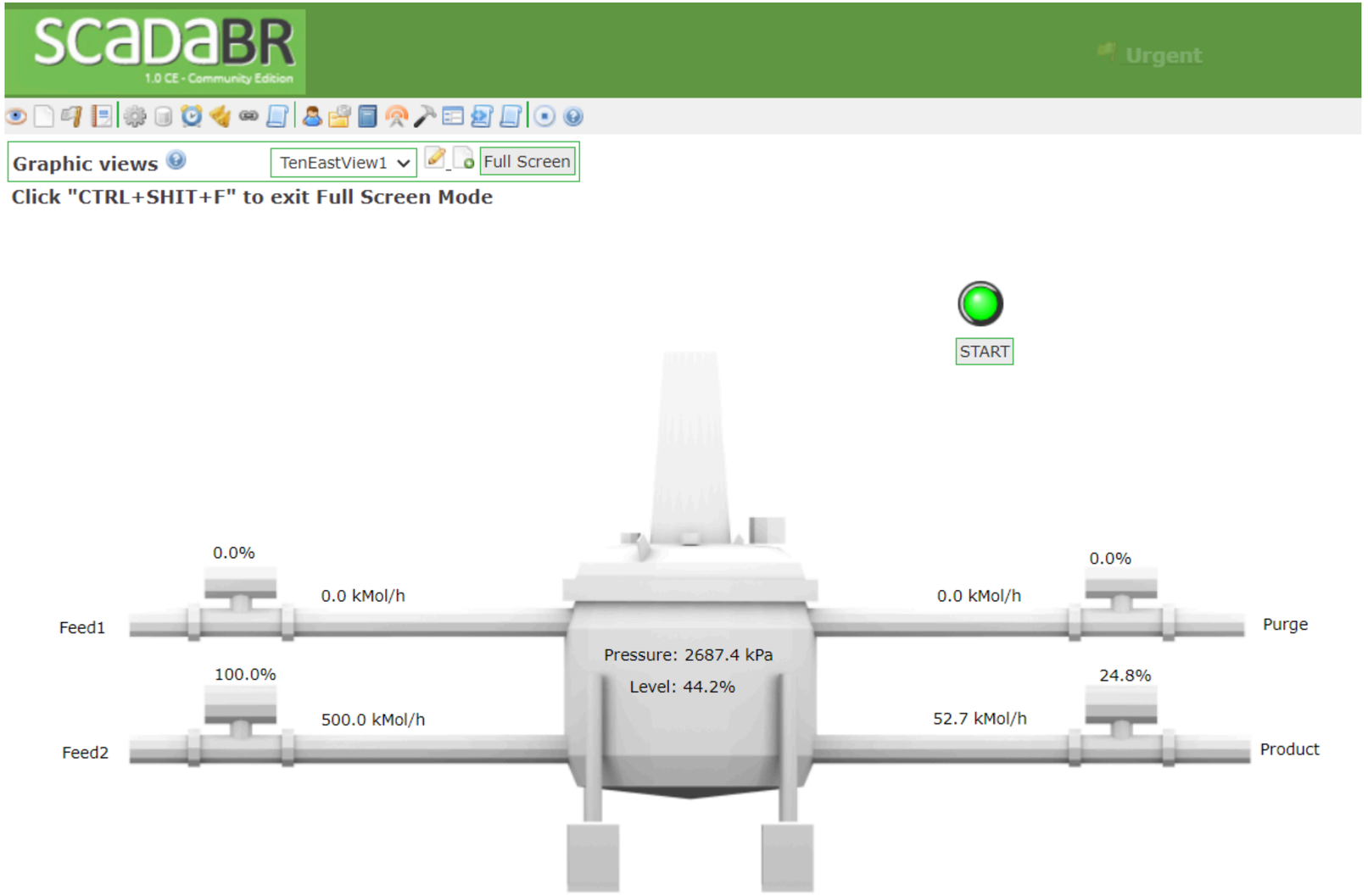
IV - The 3 main projects

1 - GRFICS (Chemical Plant)

IV - The 3 main projects

1 - GRFICS (Chemical Plant)

IV - The 3 main projects
1 - GRFICS (Chemical Plant)

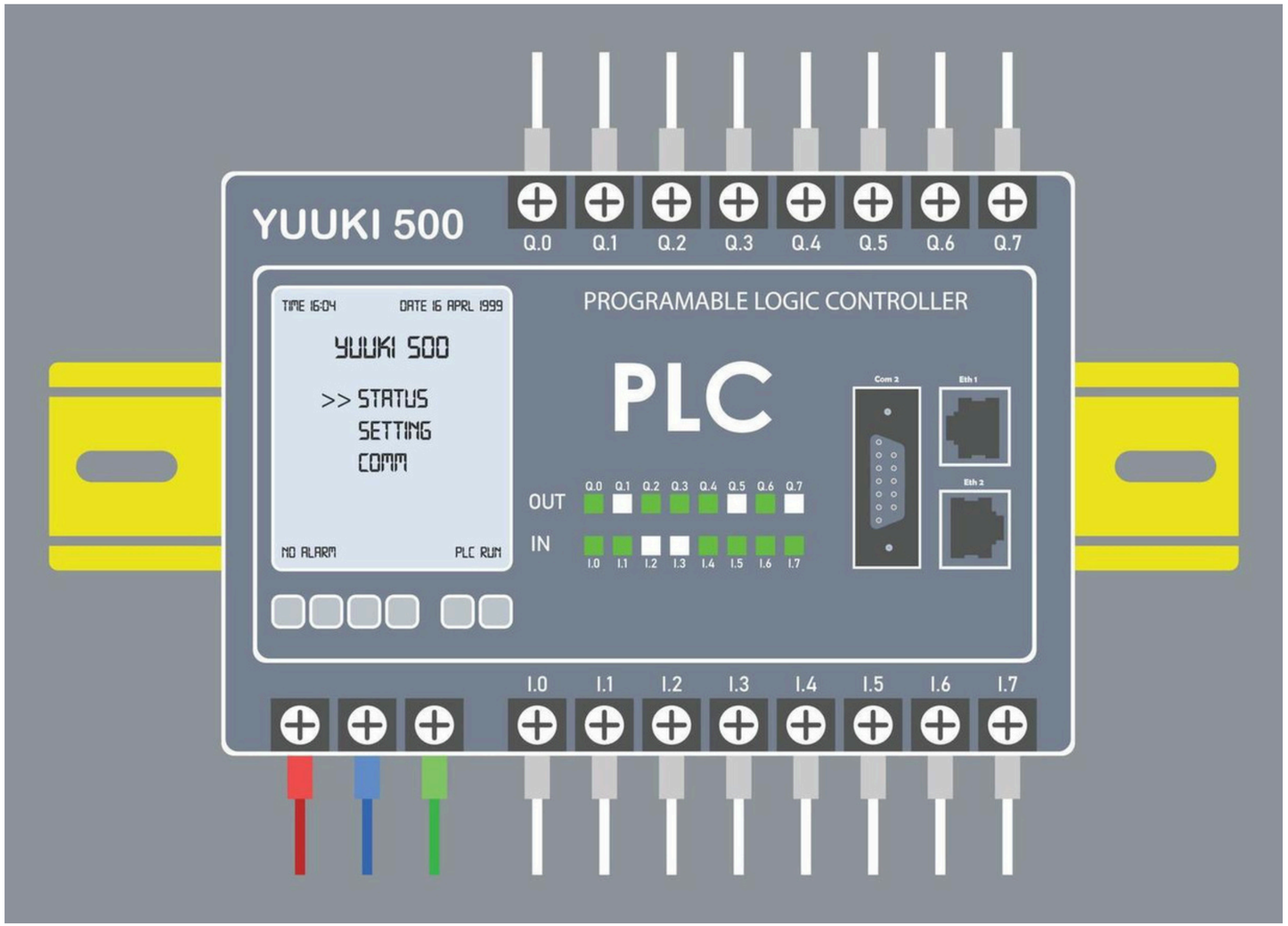


IV - The 3 main projects

1 - GRFICS (Chemical Plant)

IV - The 3 main projects

1 - GRFICS (Chemical Plant)



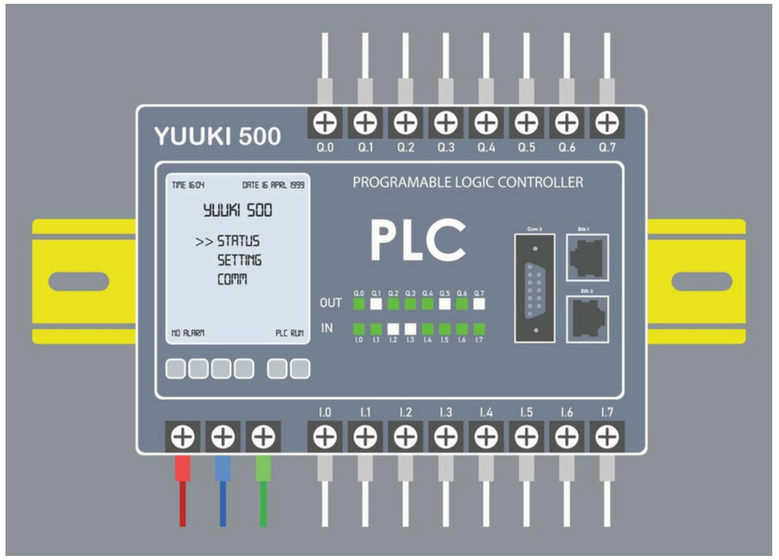
PLC = Programmable Logic Controller

IV - The 3 main projects

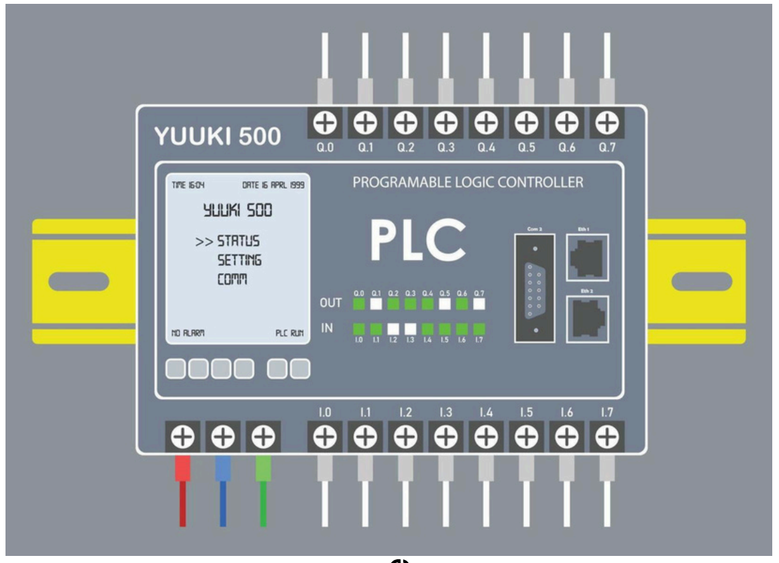
1 - GRFICS (Chemical Plant)

IV - The 3 main projects
1 - GRFICS (Chemical Plant)

IV - The 3 main projects
1 - GRFICS (Chemical Plant)

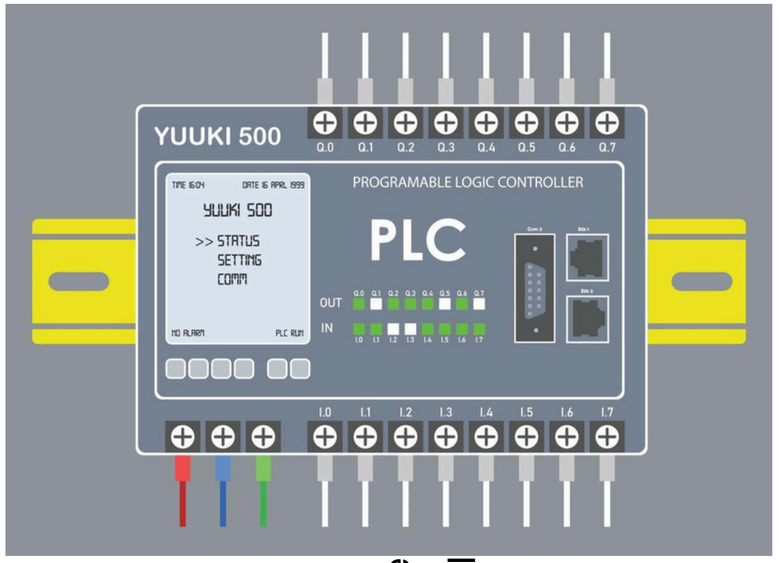


IV - The 3 main projects
1 - GRFICS (Chemical Plant)

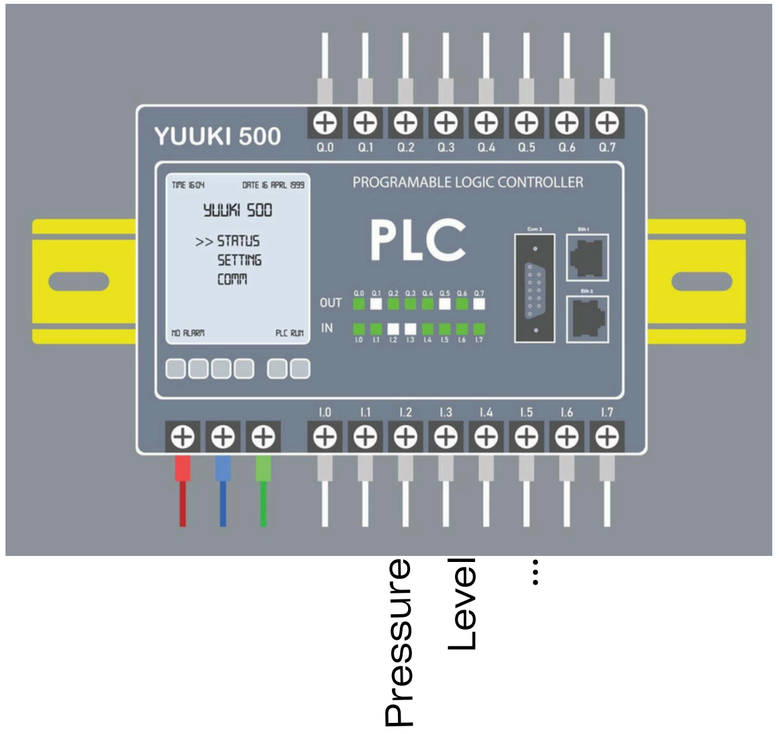


Pressure

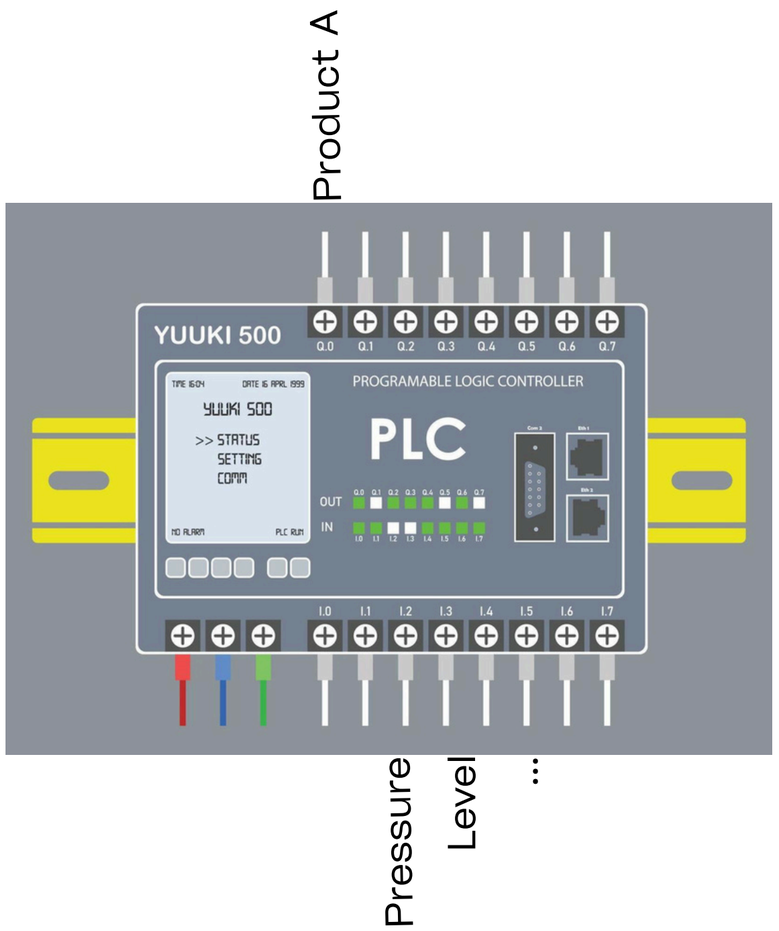
IV - The 3 main projects
1 - GRFICS (Chemical Plant)



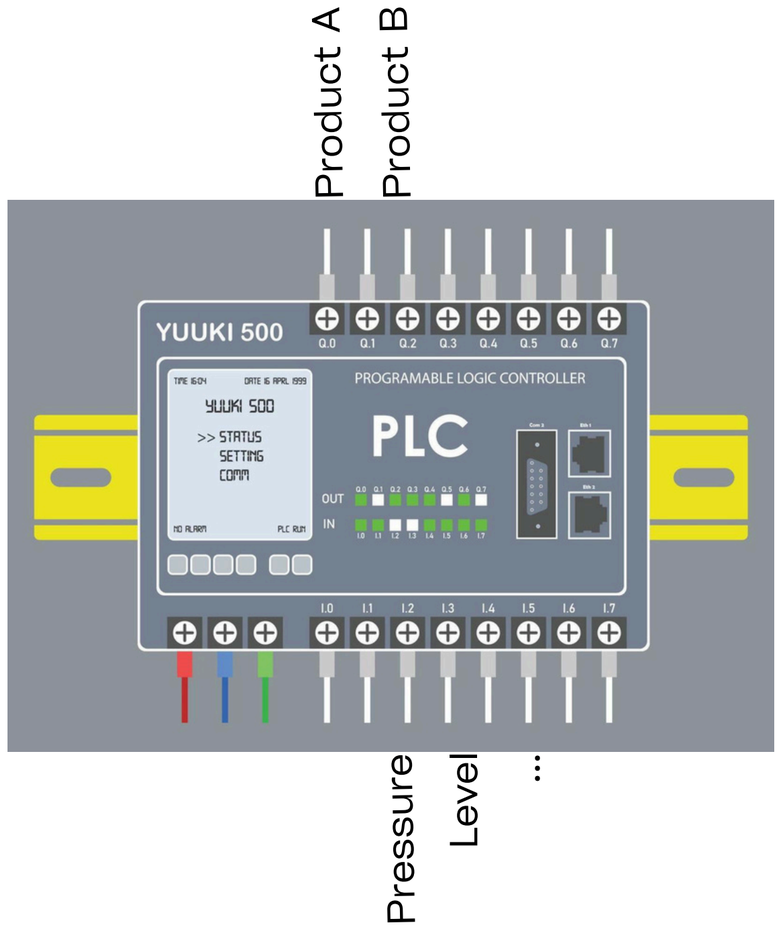
IV - The 3 main projects
1 - GRFICS (Chemical Plant)



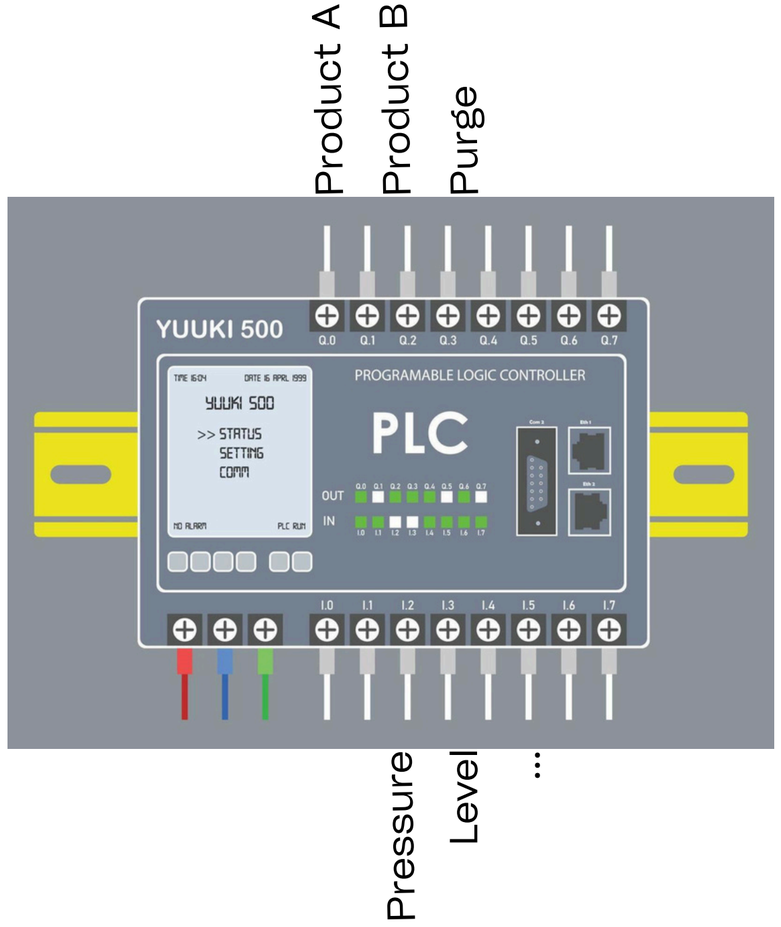
IV - The 3 main projects
1 - GRFICS (Chemical Plant)



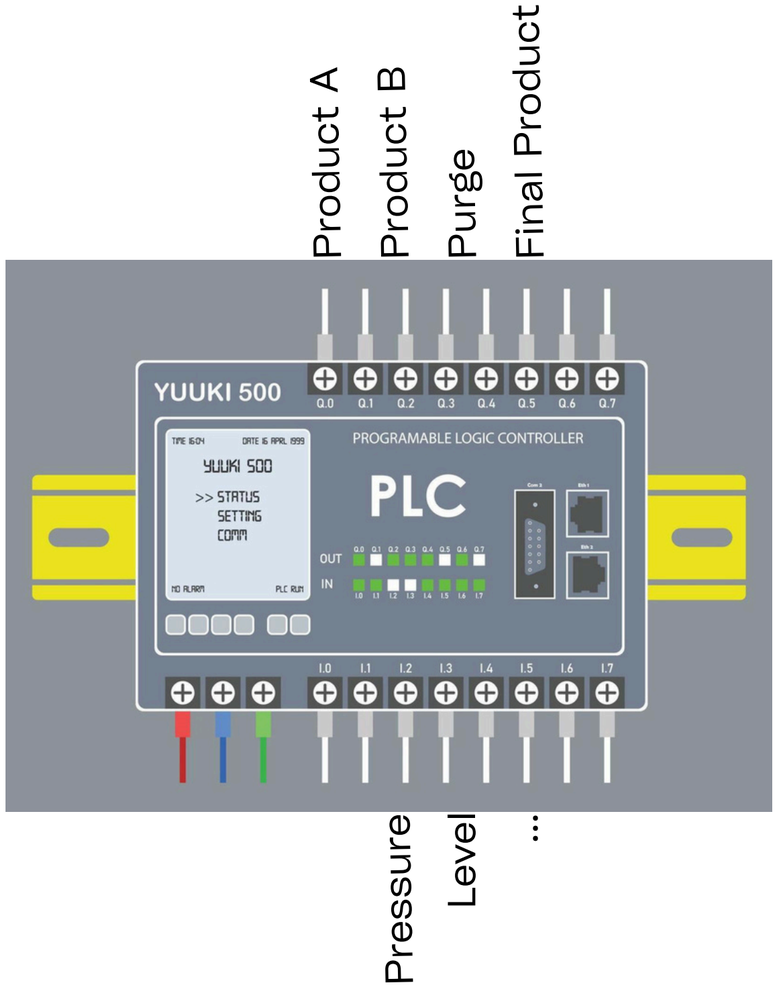
IV - The 3 main projects
1 - GRFICS (Chemical Plant)



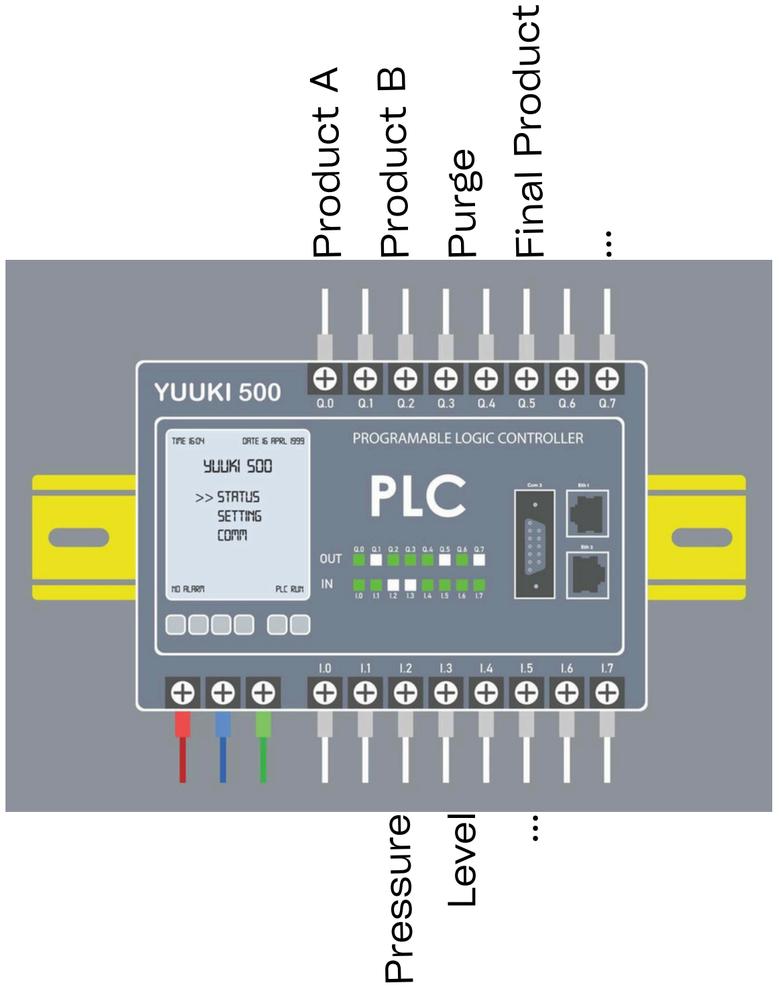
IV - The 3 main projects
1 - GRFICS (Chemical Plant)



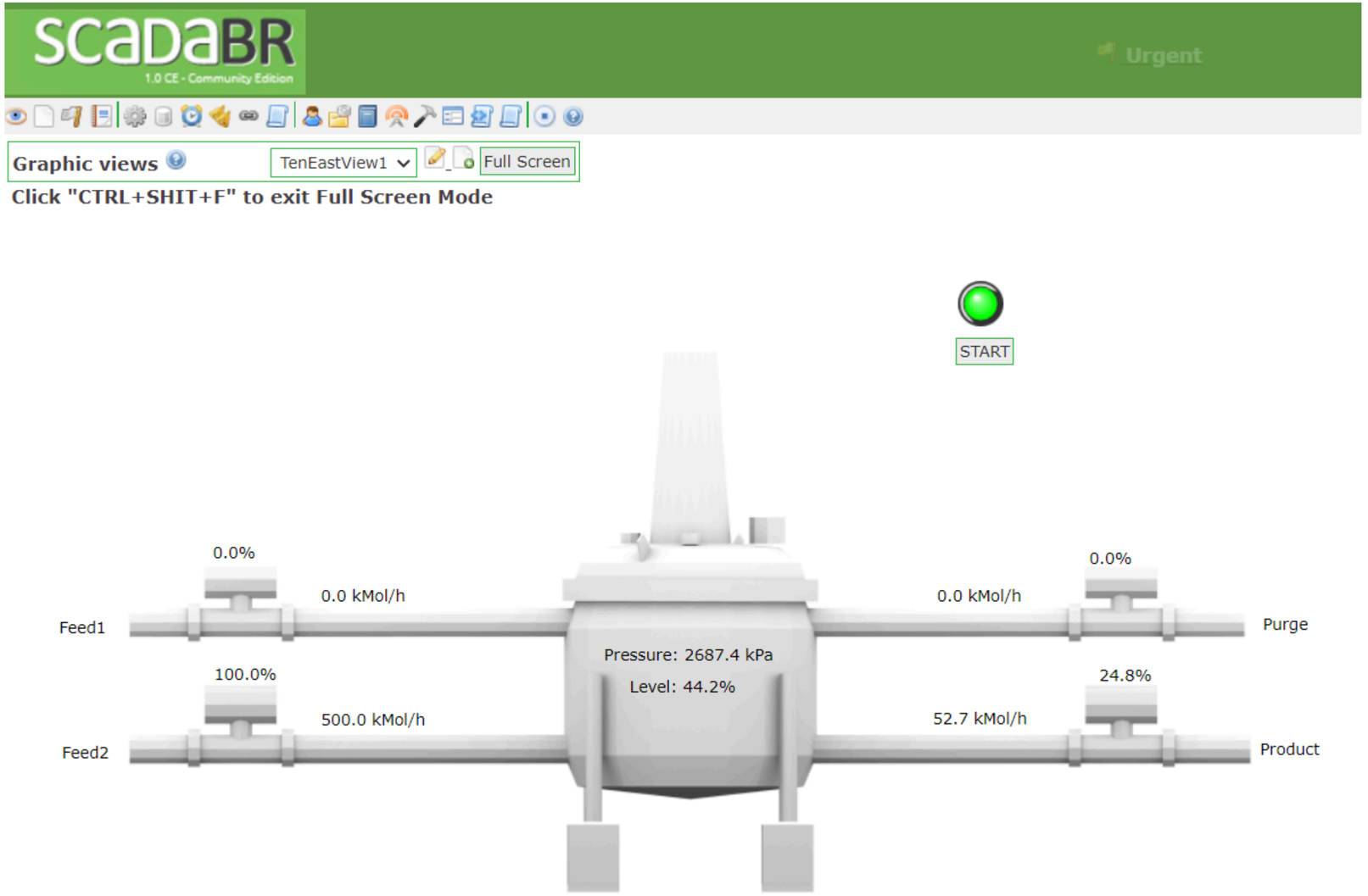
IV - The 3 main projects
1 - GRFICS (Chemical Plant)



IV - The 3 main projects
1 - GRFICS (Chemical Plant)



IV - The 3 main projects
1 - GRFICS (Chemical Plant)



IV - The 3 main projects
1 - GRFICS (Chemical Plant)

My work:

My work:

- Understand the project

My work:

- Understand the project
- Install it

My work:

- Understand the project
- Install it
- Make it work locally

My work:

- Understand the project
- Install it
- Make it work locally
- Understand how it can be attacked

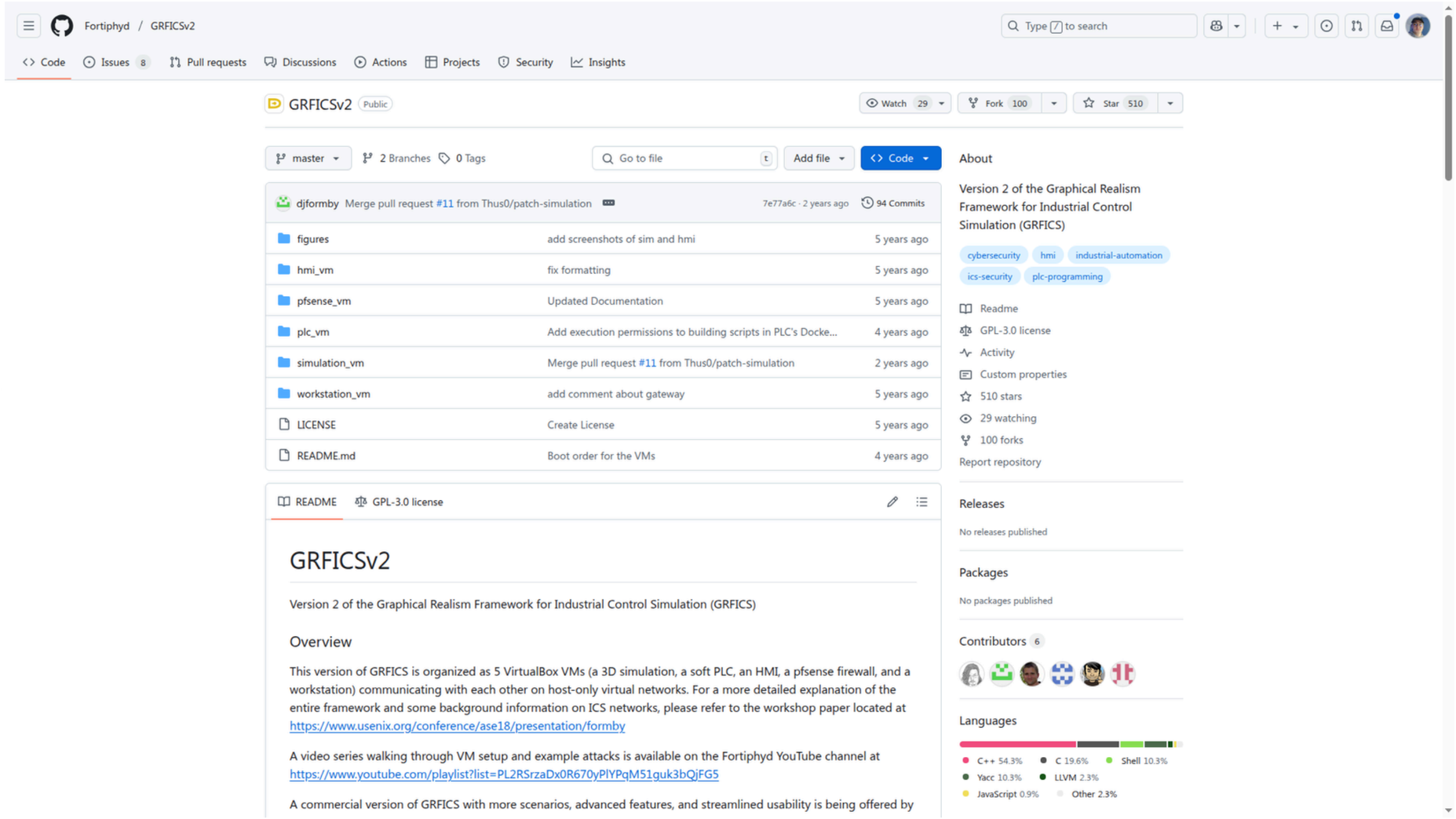
My work:

- Understand the project
- Install it
- Make it work locally
- Understand how it can be attacked
- Export it to the Ludus

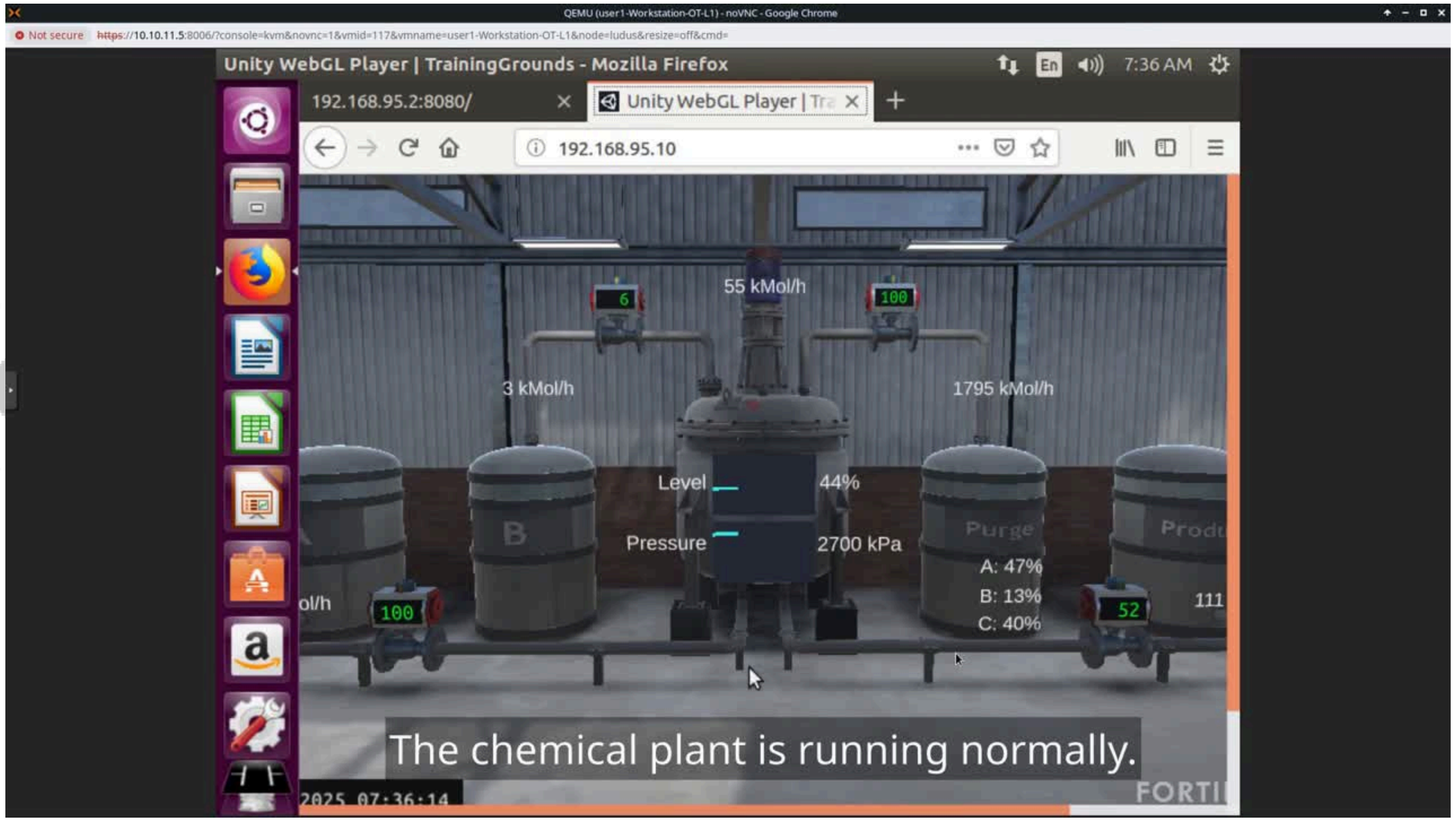
My work:

- Understand the project
- Install it
- Make it work locally
- Understand how it can be attacked
- Export it to the Ludus
- Make it duplicable

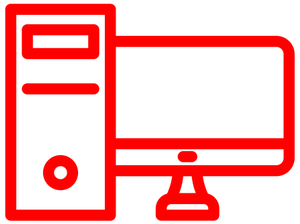
IV - The 3 main projects
1 - GRFICS (Chemical Plant)



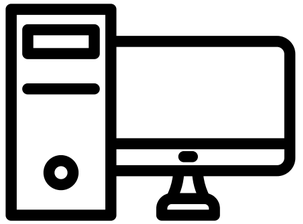
IV - The 3 main projects
1 - GRFICS (Chemical Plant)



IV - The 3 main projects
1 - GRFICS (Chemical Plant)

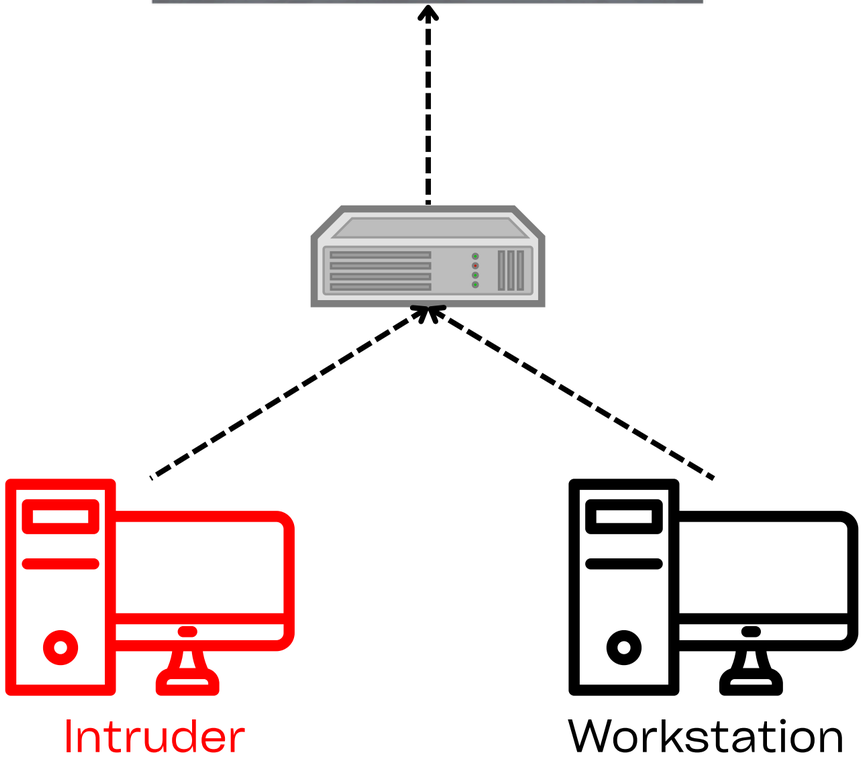


Intruder

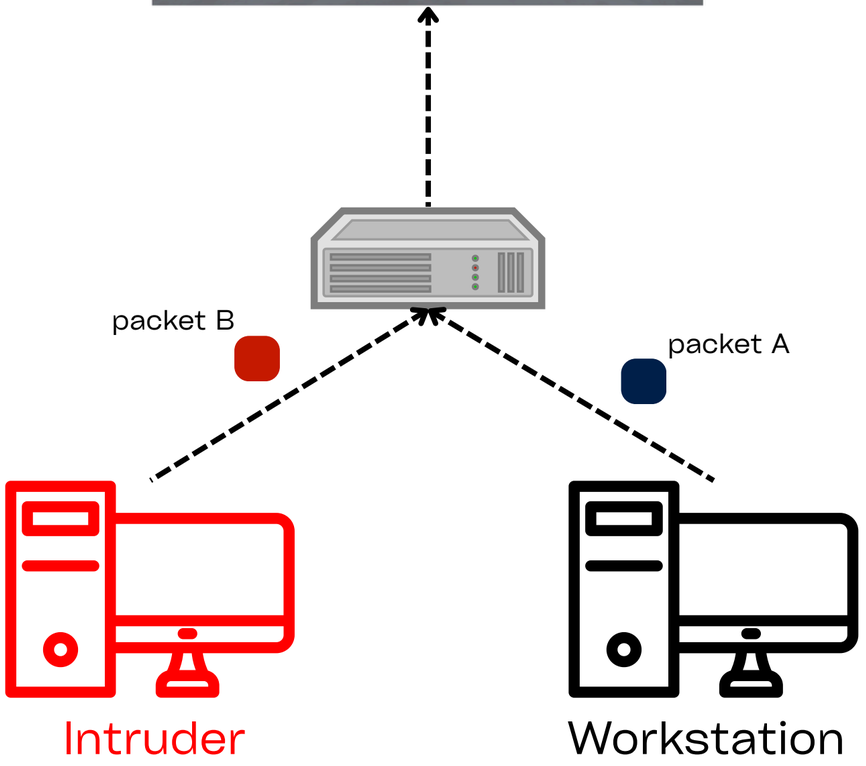


Workstation

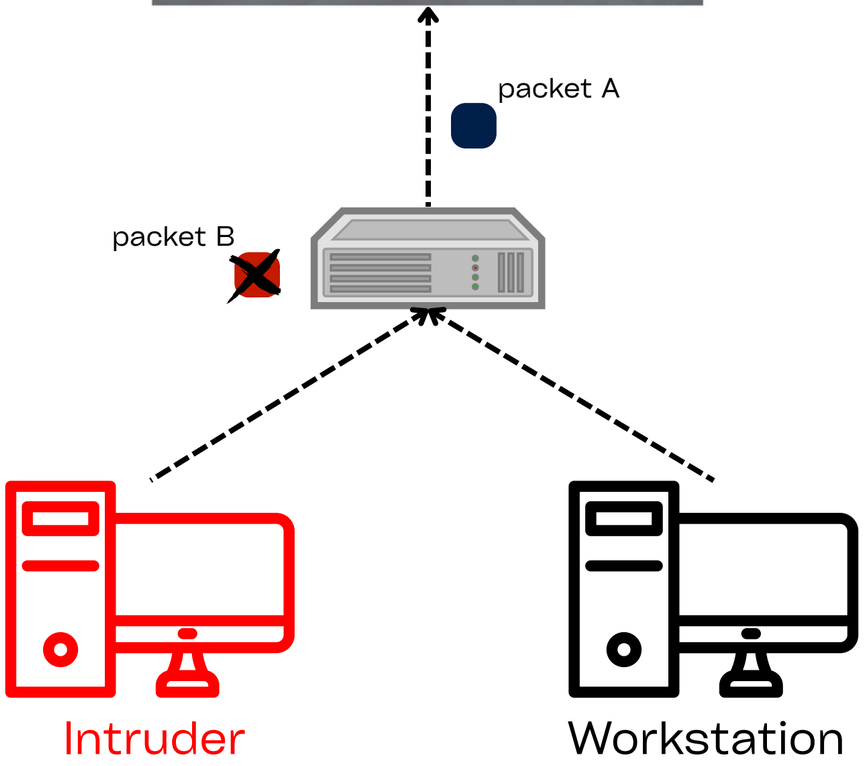
IV - The 3 main projects
1 - GRFICS (Chemical Plant)



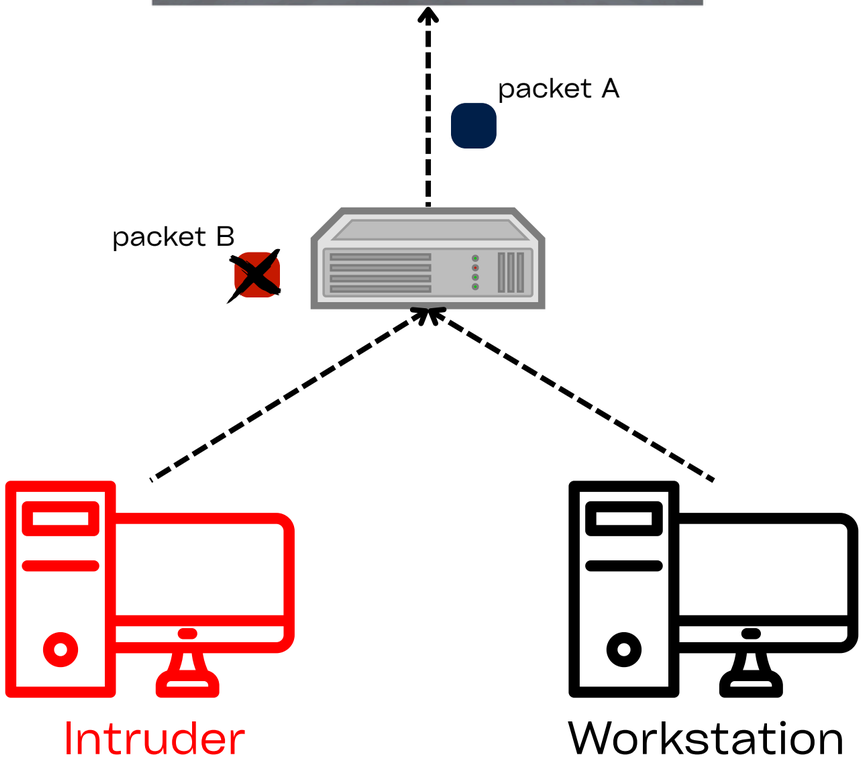
IV - The 3 main projects
1 - GRFICS (Chemical Plant)



IV - The 3 main projects
1 - GRFICS (Chemical Plant)



IV - The 3 main projects
1 - GRFICS (Chemical Plant)



Benefits

Benefits

Already installed, so no direct benefit for the CIH

Benefits

Already installed, so no direct benefit for the CIH

I understood what the CIH was working on

Benefits

Already installed, so no direct benefit for the CIH

I understood what the CIH was working on

Get hands-on practice on the Ludus

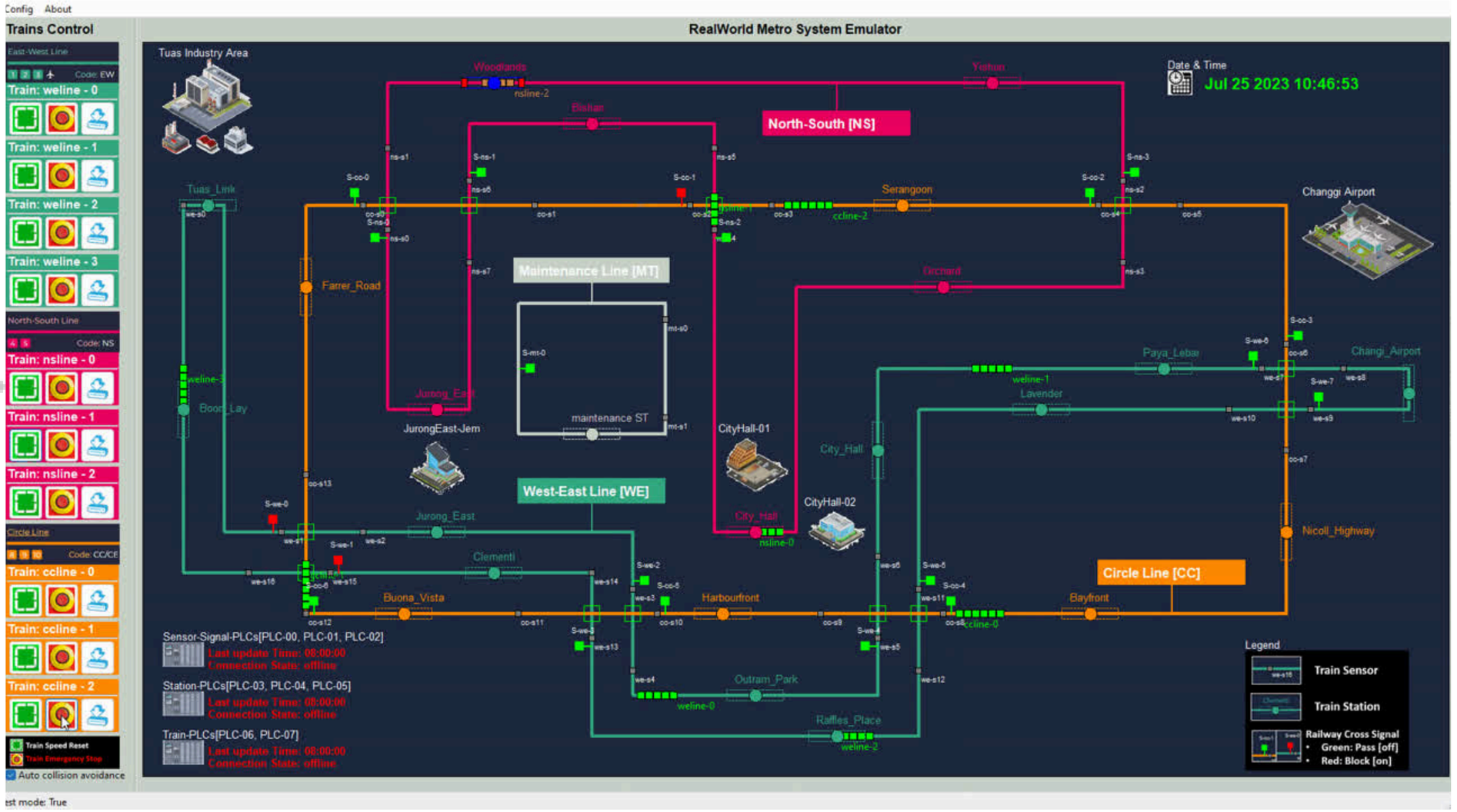
IV - The 3 main projects

1 - GRFICS (Chemical Plant)

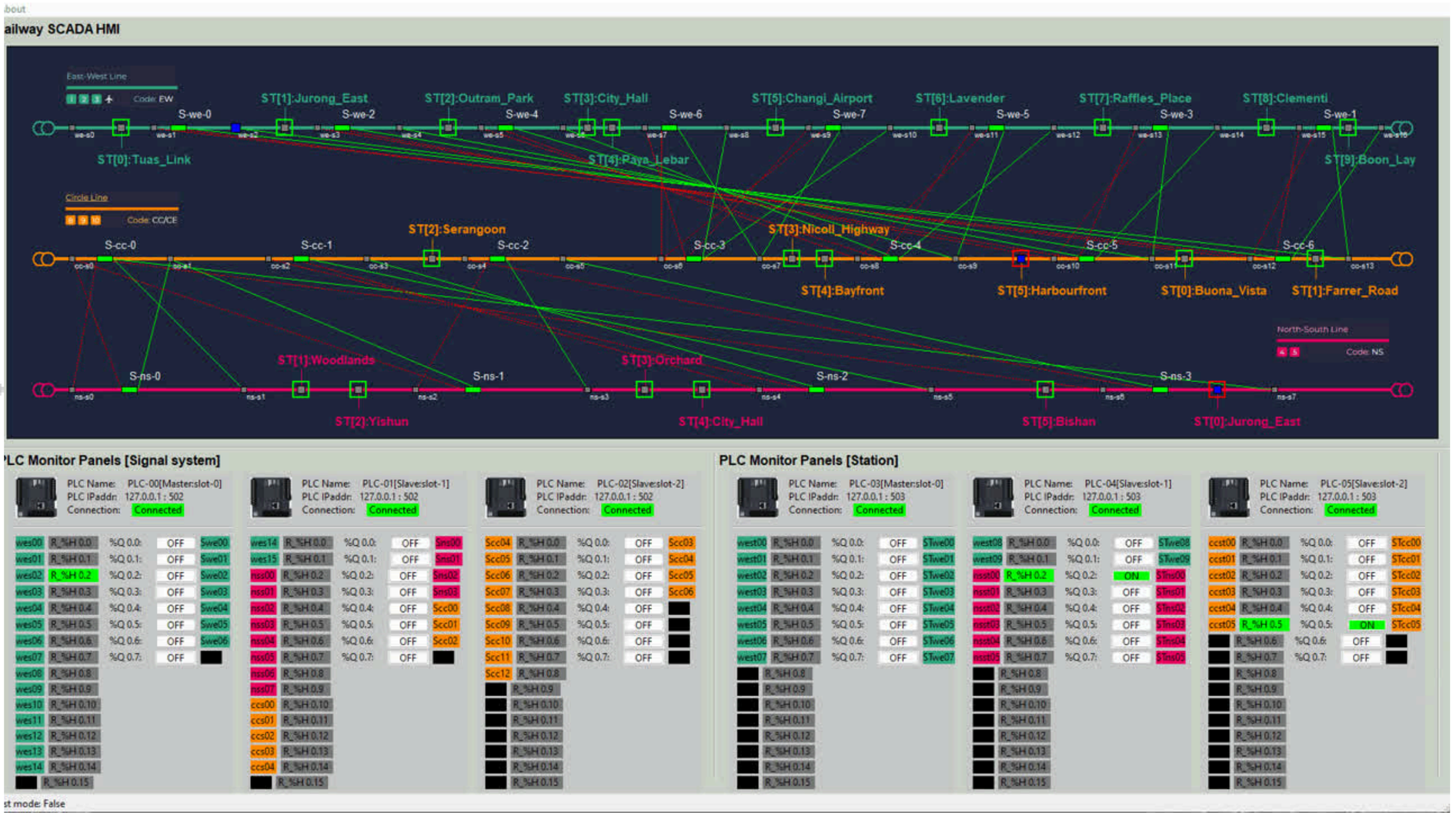
2 - Cardiff Metro Emulator

3 - Bottle Filling Plant

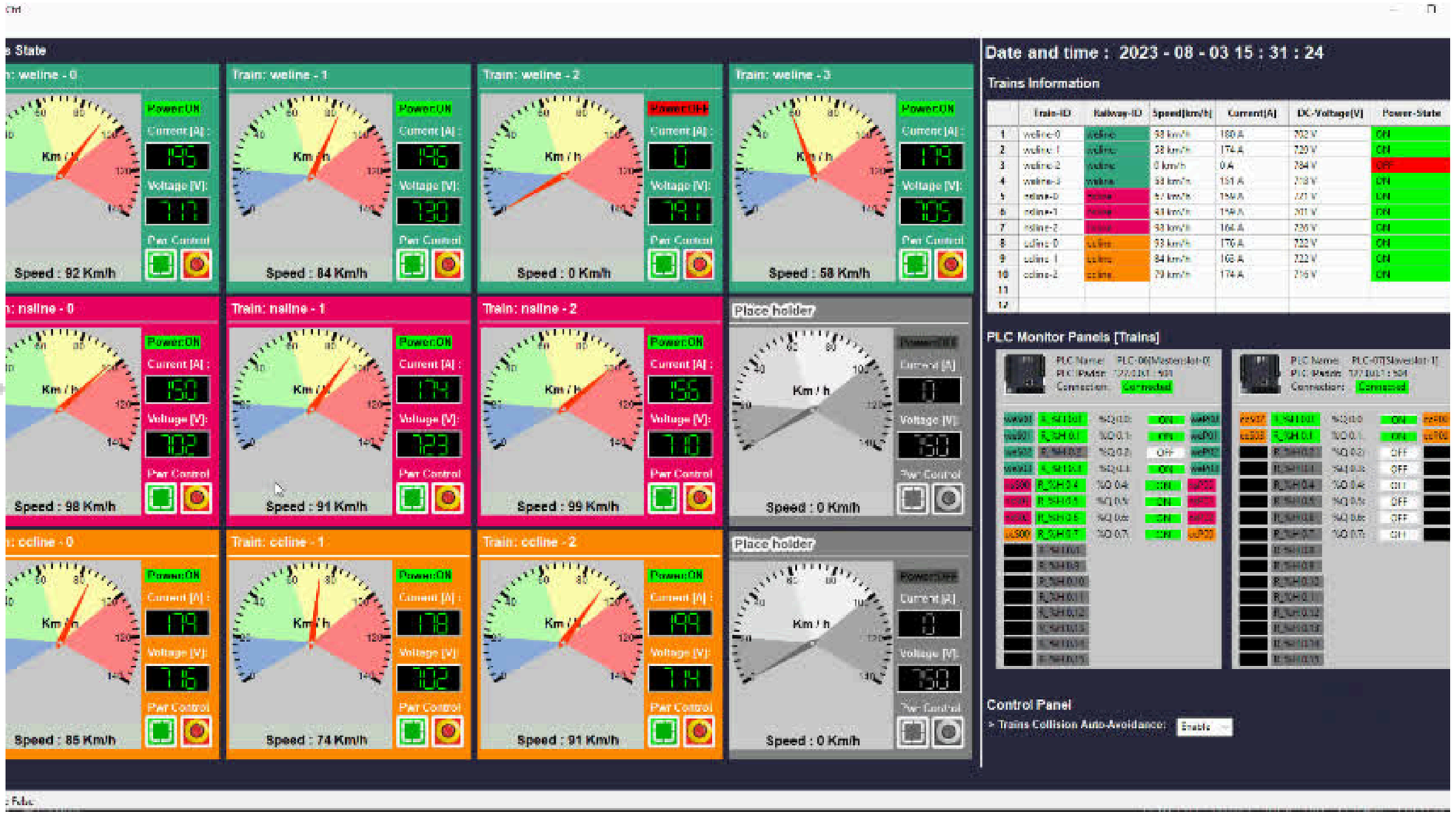
IV - The 3 main projects
2 - Cardiff Metro Emulator



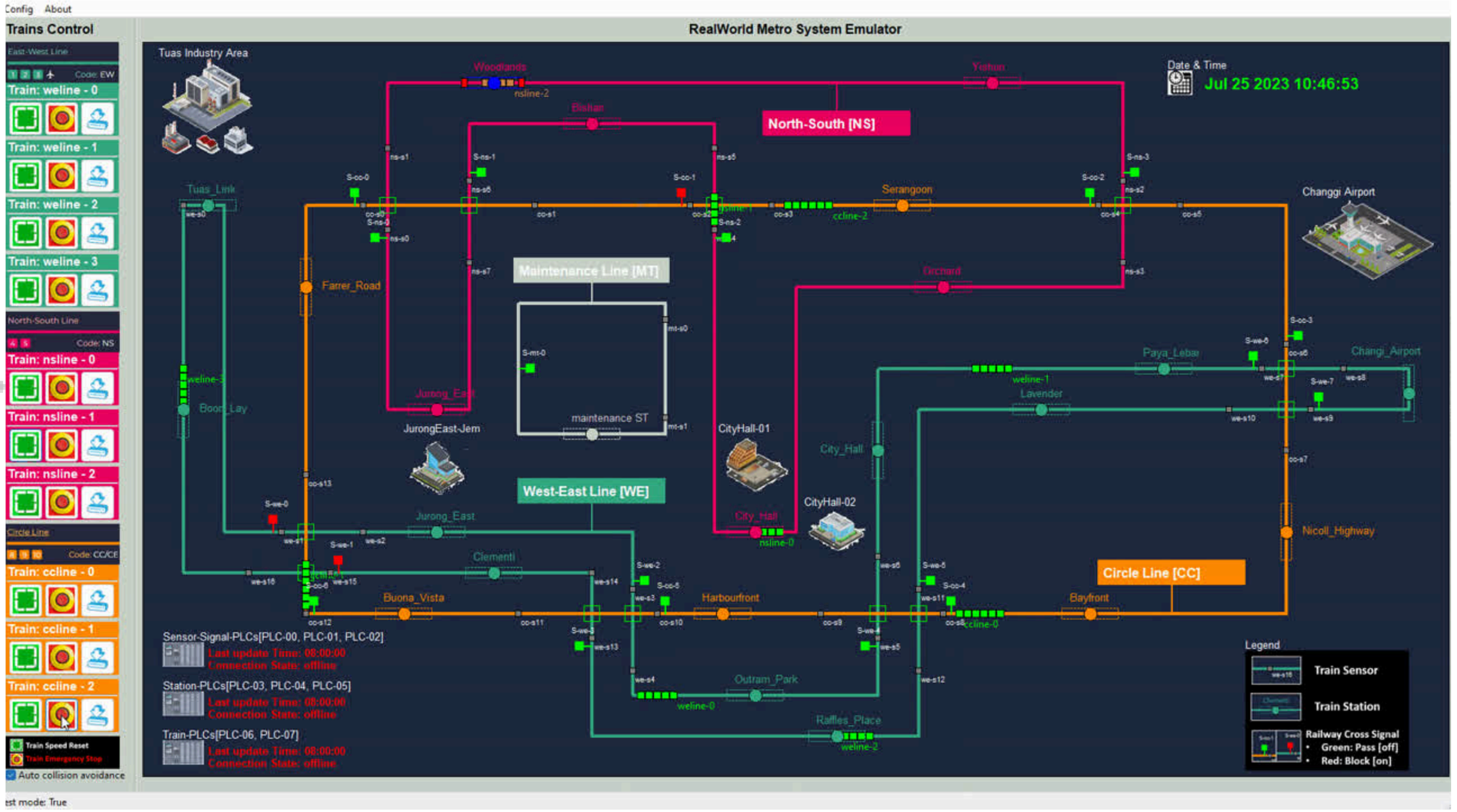
IV - The 3 main projects
2 - Cardiff Metro Emulator



IV - The 3 main projects
2 - Cardiff Metro Emulator



IV - The 3 main projects
2 - Cardiff Metro Emulator



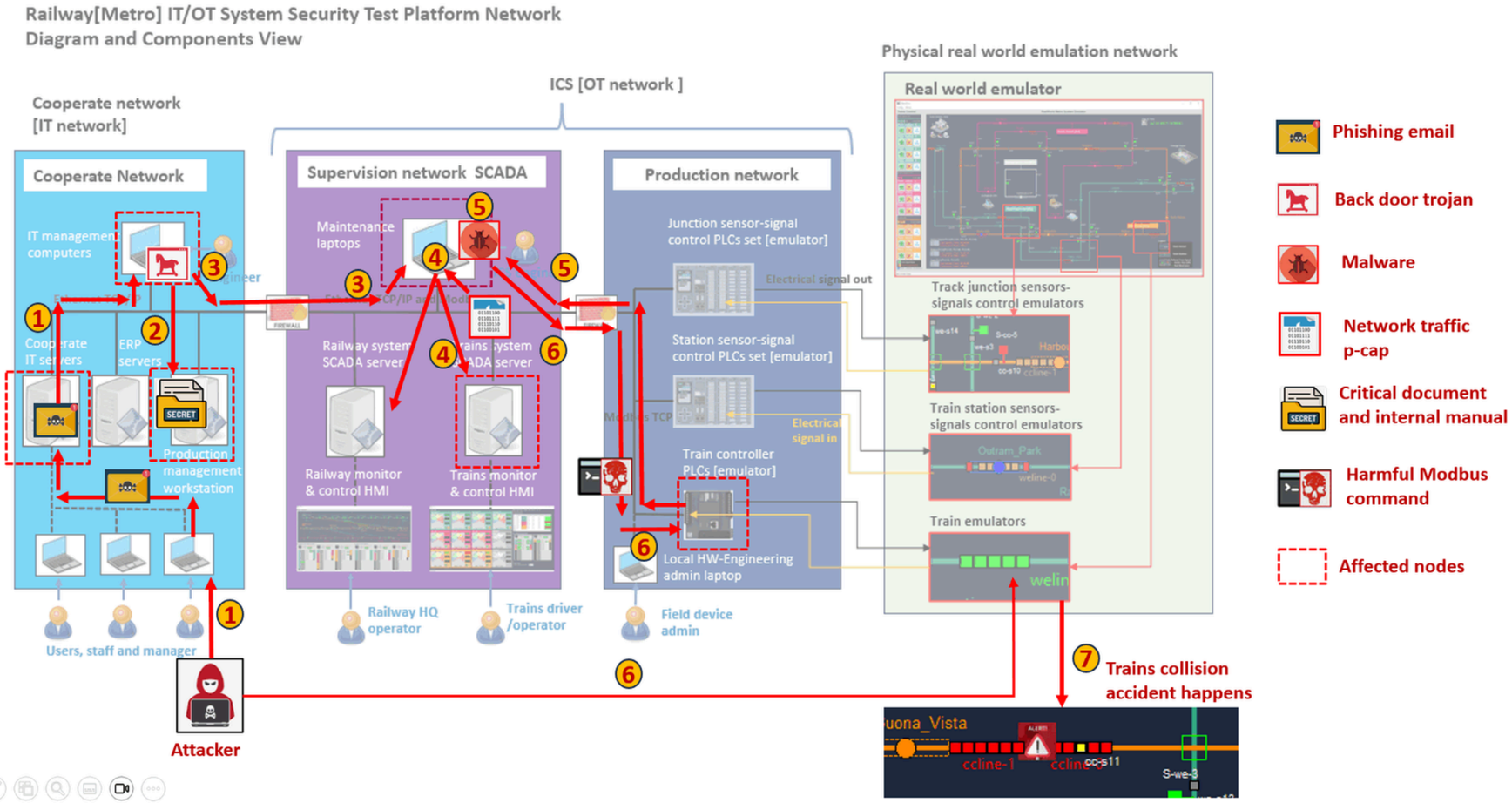
My work:

- Understand the project
- Install it
- Make it work locally
- Understand how it can be attacked
- Export it to the Ludus
- Make it duplicable

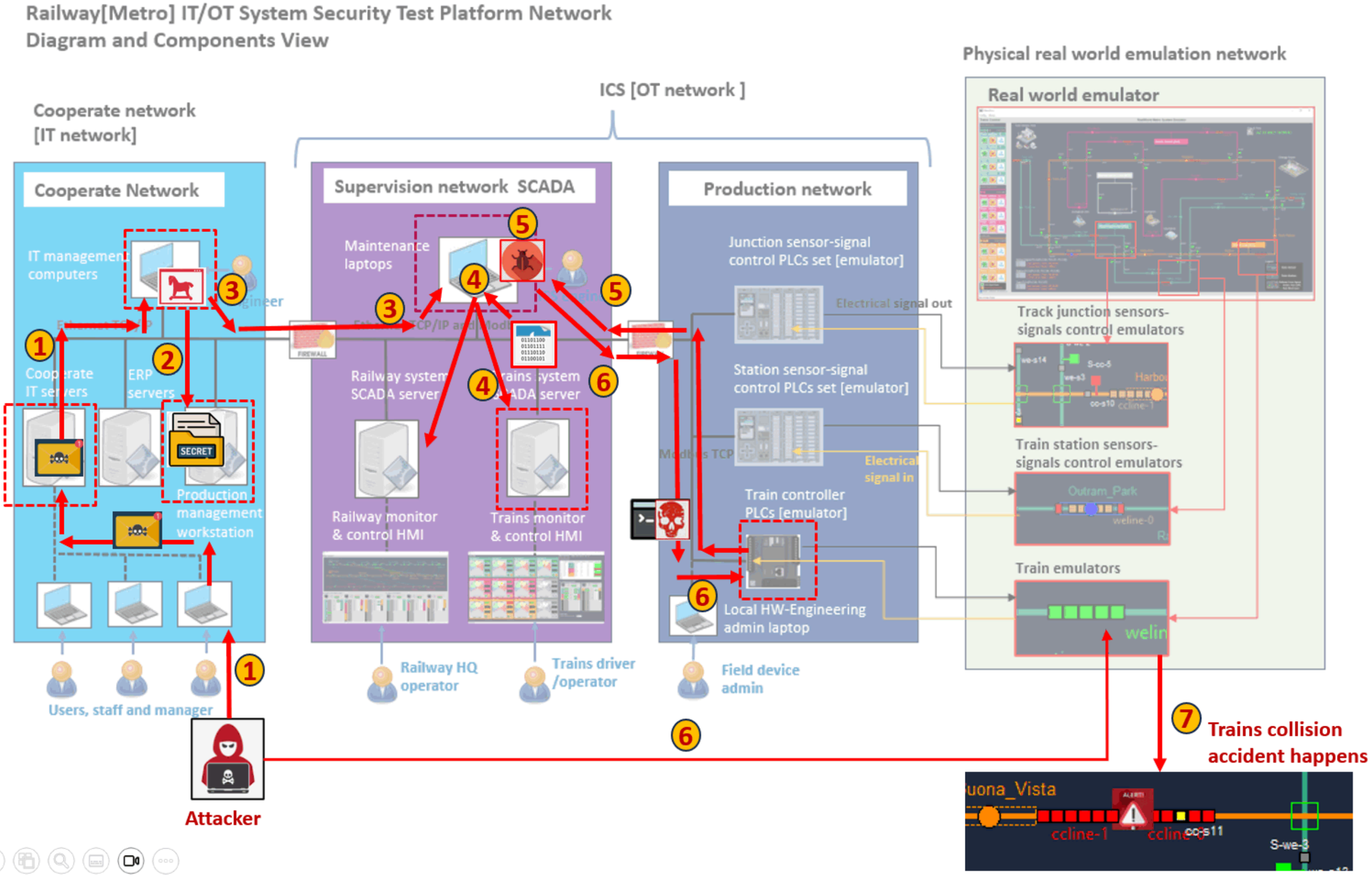
My work:

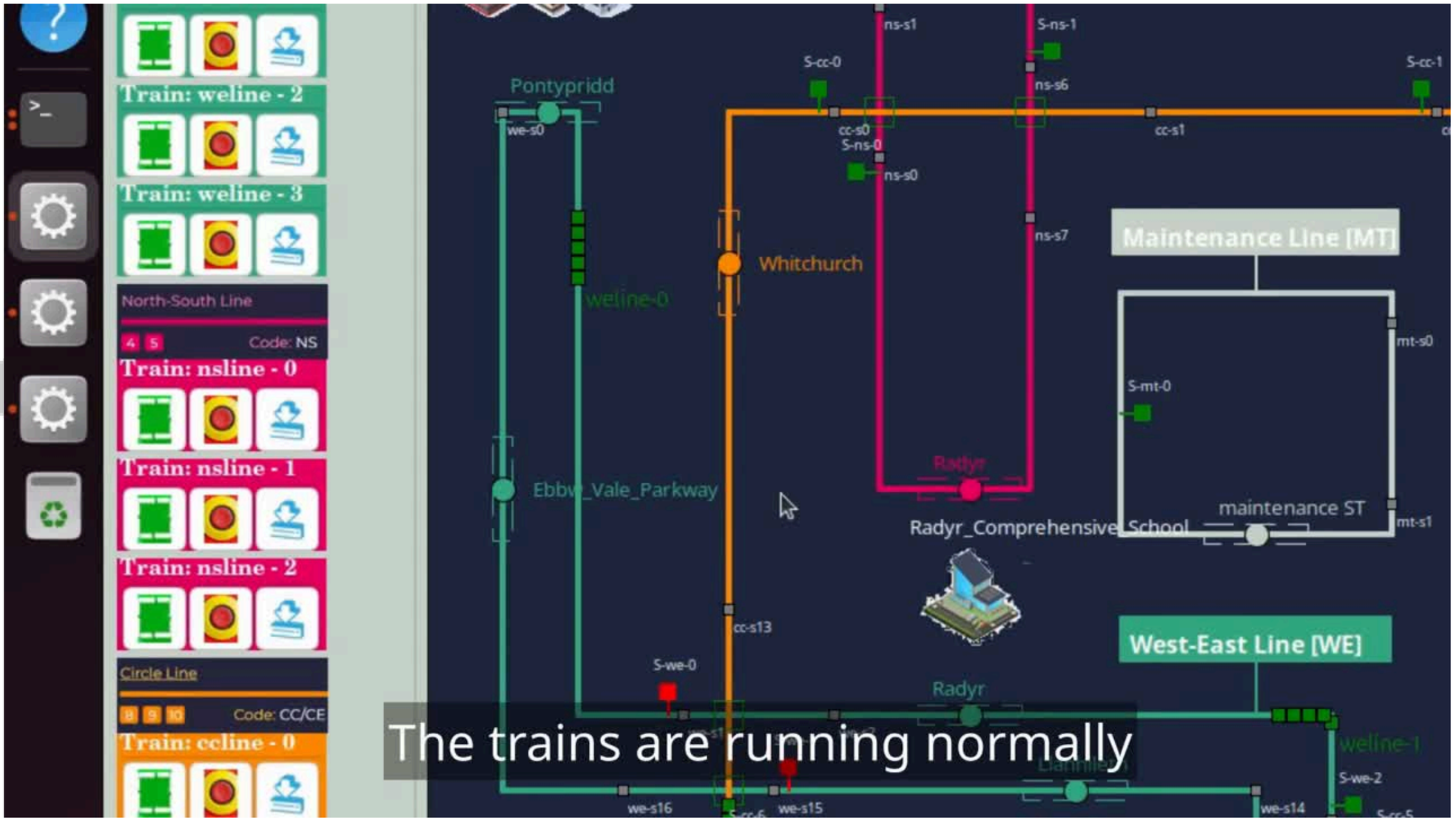
- Understand the project
- Install it
- Make it work locally
- Understand how it can be attacked
- Export it to the Ludus
- Make it duplicable

Attack Scenario 1: False command injection attack via phishing email and Backdoor Trojan



Attack Scenario 1: False command injection attack via phishing email and Backdoor Trojan




Train: weline - 2
Train: weline - 3
North-South Line
Code: NS
Train: nsline - 0
Train: nsline - 1
Train: nsline - 2
Circle Line
Code: CC/CE
Train: ccline - 0
Pontypridd
we-s0
weline-0
Whitchurch
Ebbw_Vale_Parkway
Radyr
Radyr_Comprehensive_School
ns-s1
S-ns-1
S-cc-0
S-cc-1
ns-s6
cc-s0
cc-s1
S-ns-0
ns-s0
ns-s7
Maintenance Line [MT]
mt-s0
S-mt-0
maintenance ST
mt-s1
cc-s13
S-we-0
West-East Line [WE]
Radyr
weline-1
S-we-2
we-s16
we-s15
we-s14
The trains are running normally

IV - The 3 main projects

1 - GRFICS (Chemical Plant)

2 - Cardiff Metro Emulator

3 - Bottle Filling Plant

IV - The 3 main projects

3 - Bottle Filling Plant

2 main problems:

2 main problems:

- The PLC should be programmed using ladder logic

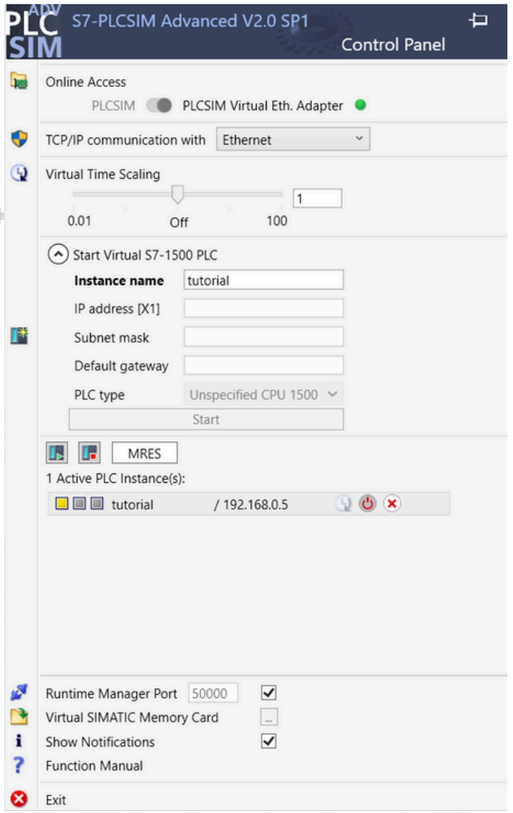
2 main problems:

- The PLC should be programmed using ladder logic
- The PLC program was not explicitly explained

SIEMENS

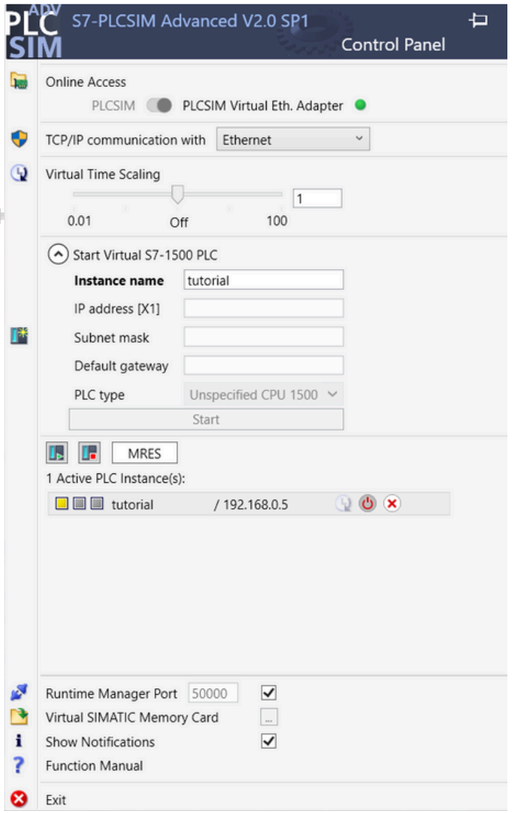
SIEMENS

PLC Simulator

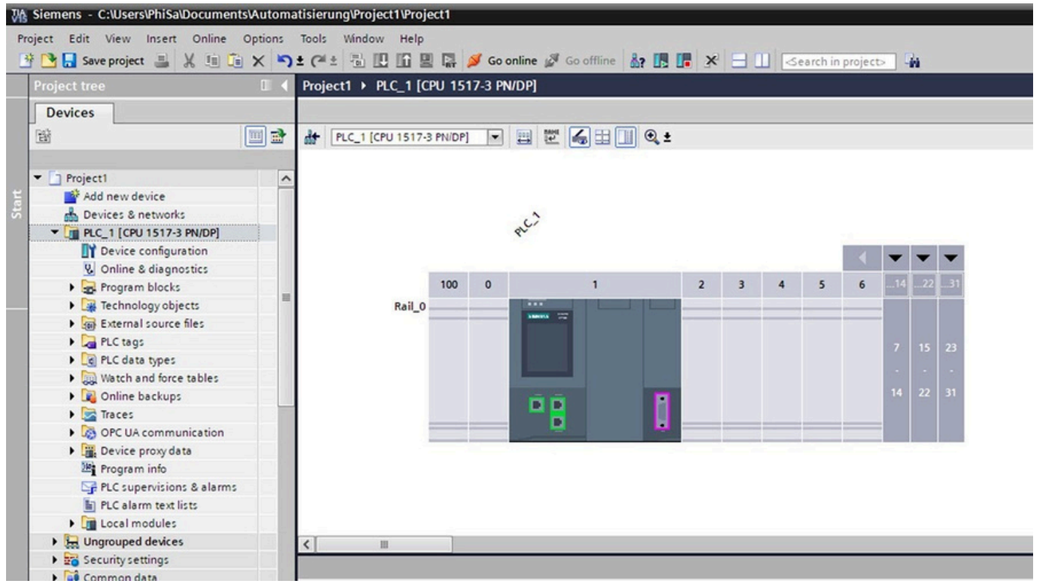


SIEMENS

PLC Simulator

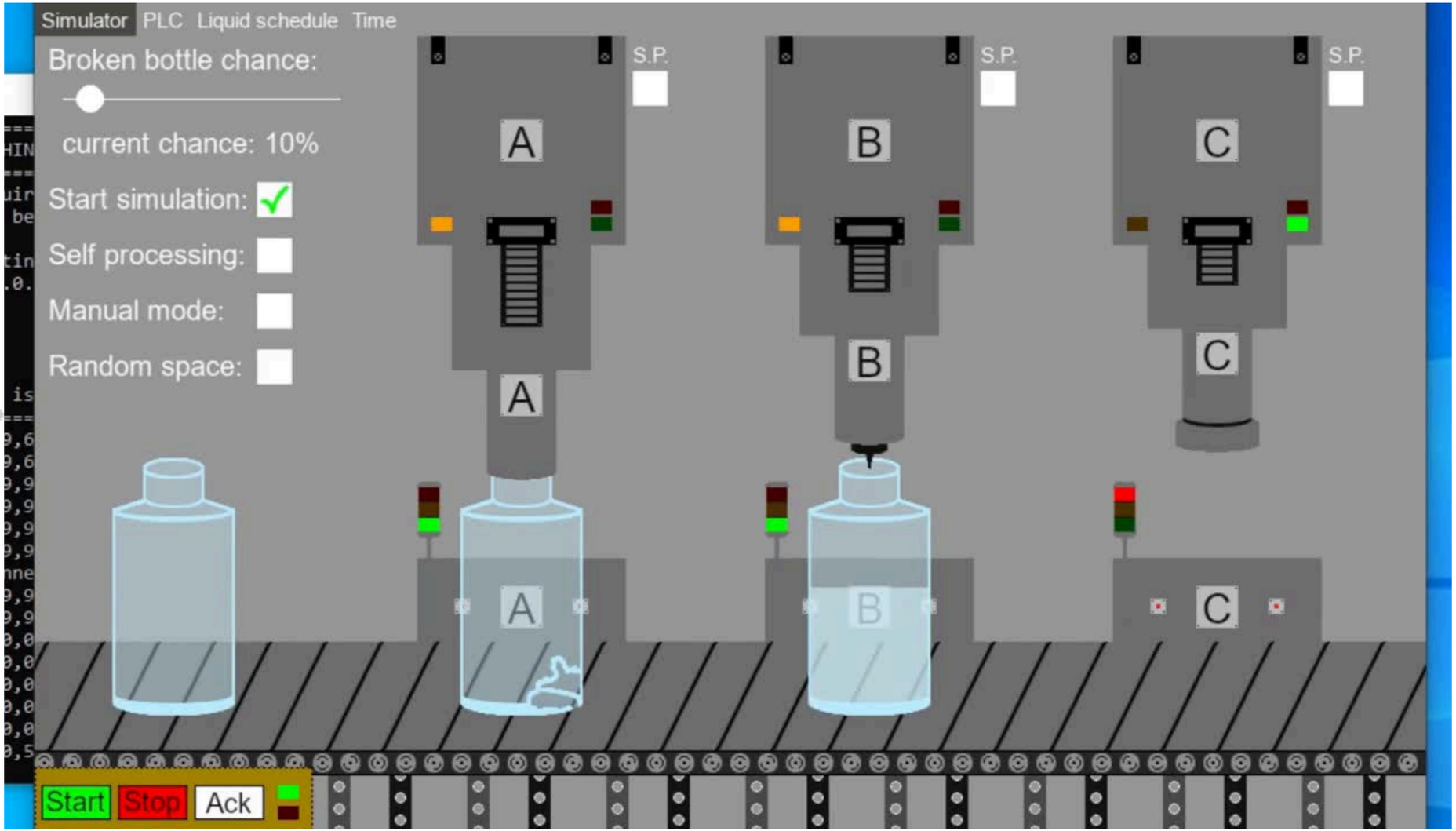


TIA Portal



IV - The 3 main projects

3 - Bottle Filling Plant



IV - The 3 main projects

3 - Bottle Filling Plant

Python = 170 lines

IV - The 3 main projects

3 - Bottle Filling Plant

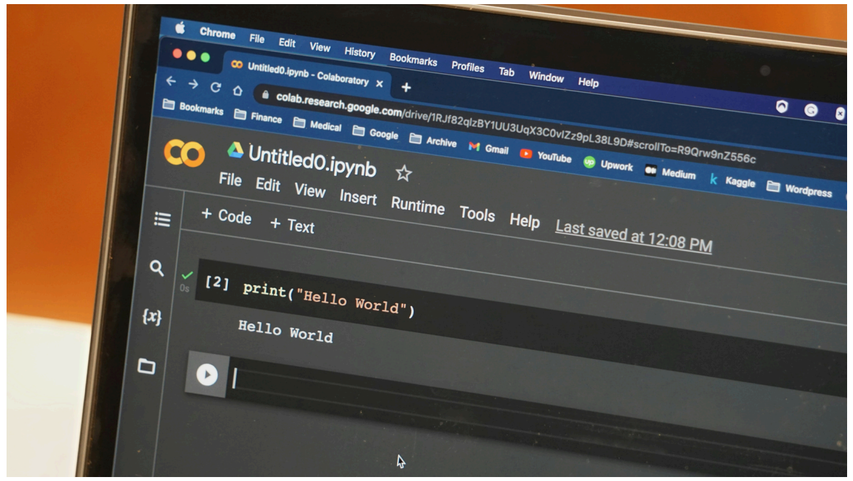
Python = 170 lines

Ladder logic = 7 days of 8 hours

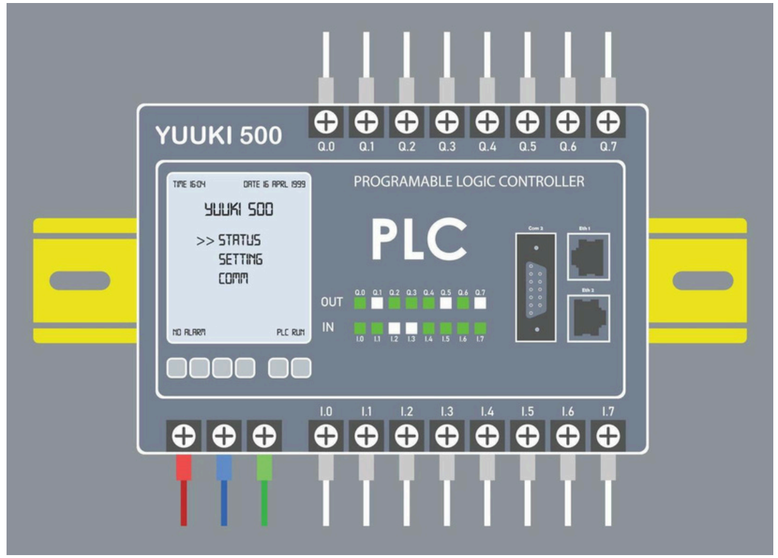
IV - The 3 main projects

3 - Bottle Filling Plant

Python = 170 lines



Ladder logic = 7 days of 8 hours

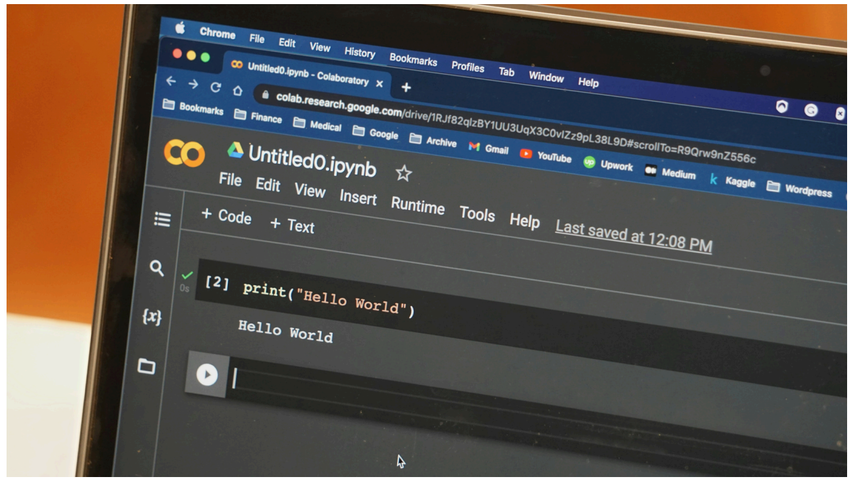


IV - The 3 main projects

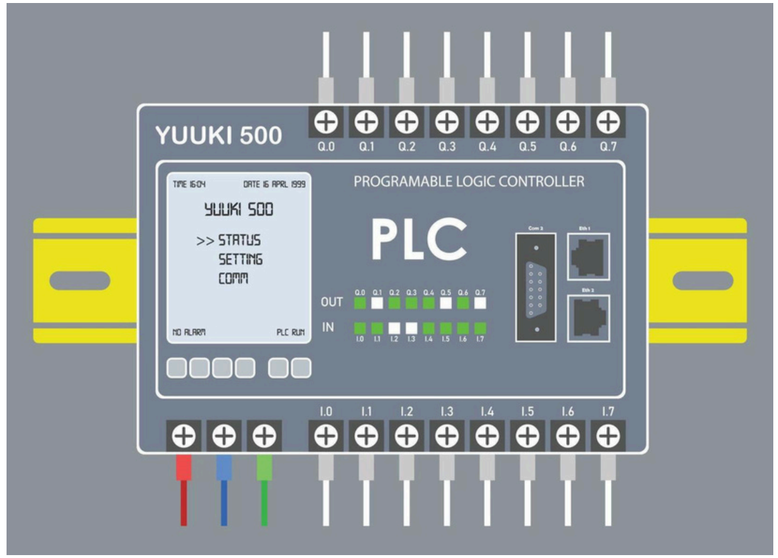
3 - Bottle Filling Plant

Python = 170 lines

Written programming language



Ladder logic = 7 days of 8 hours

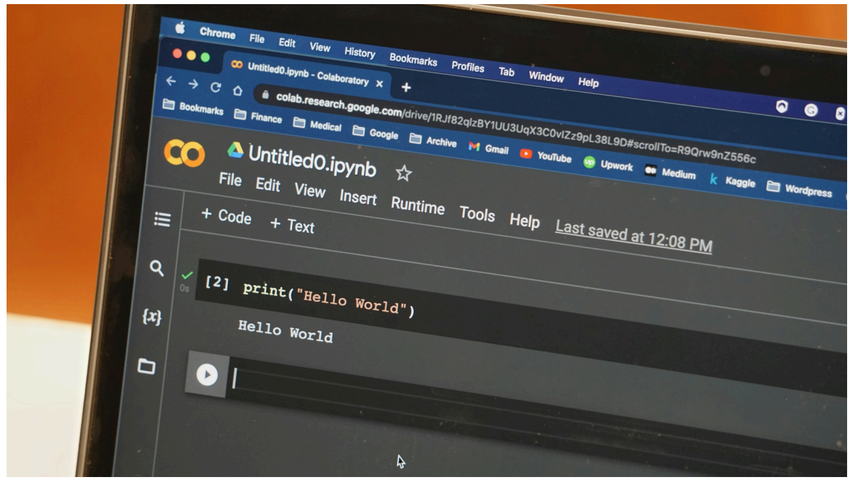


IV - The 3 main projects

3 - Bottle Filling Plant

Python = 170 lines

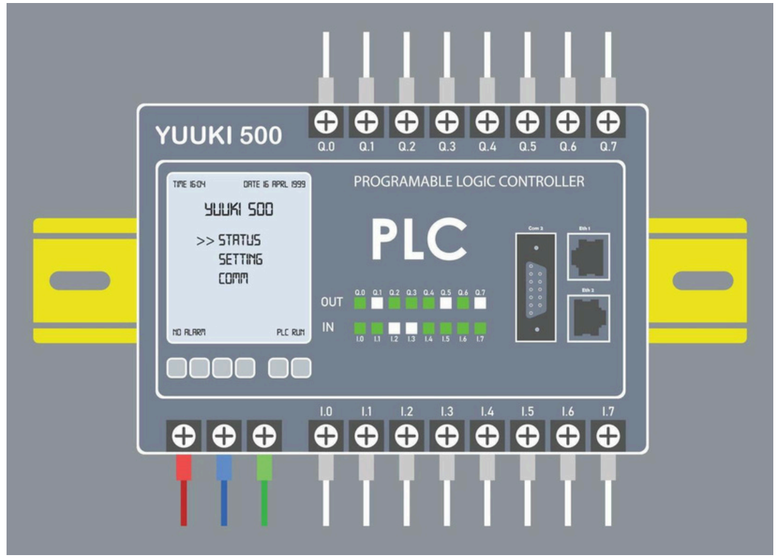
Written programming language



Ladder logic = 7 days of 8 hours

Visual programming language

Mainly conditions

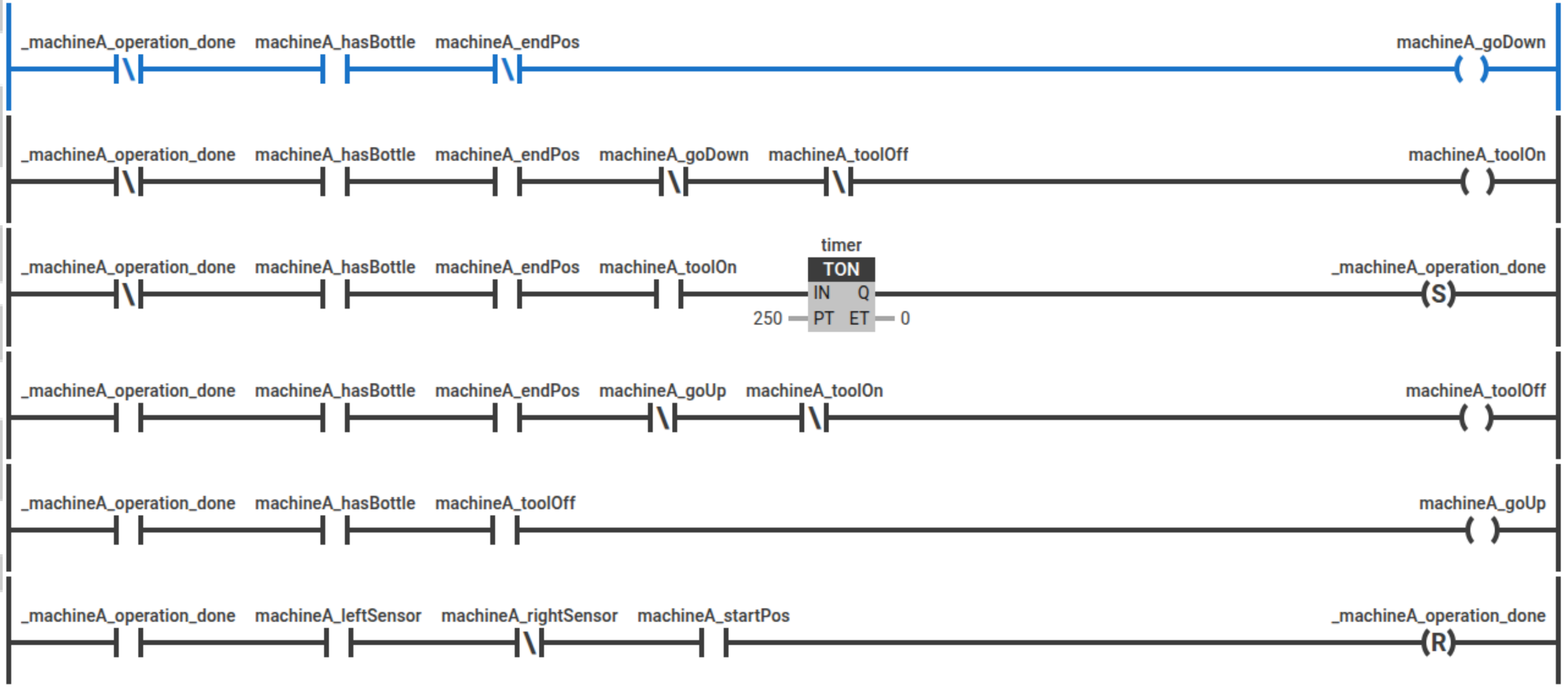


IV - The 3 main projects

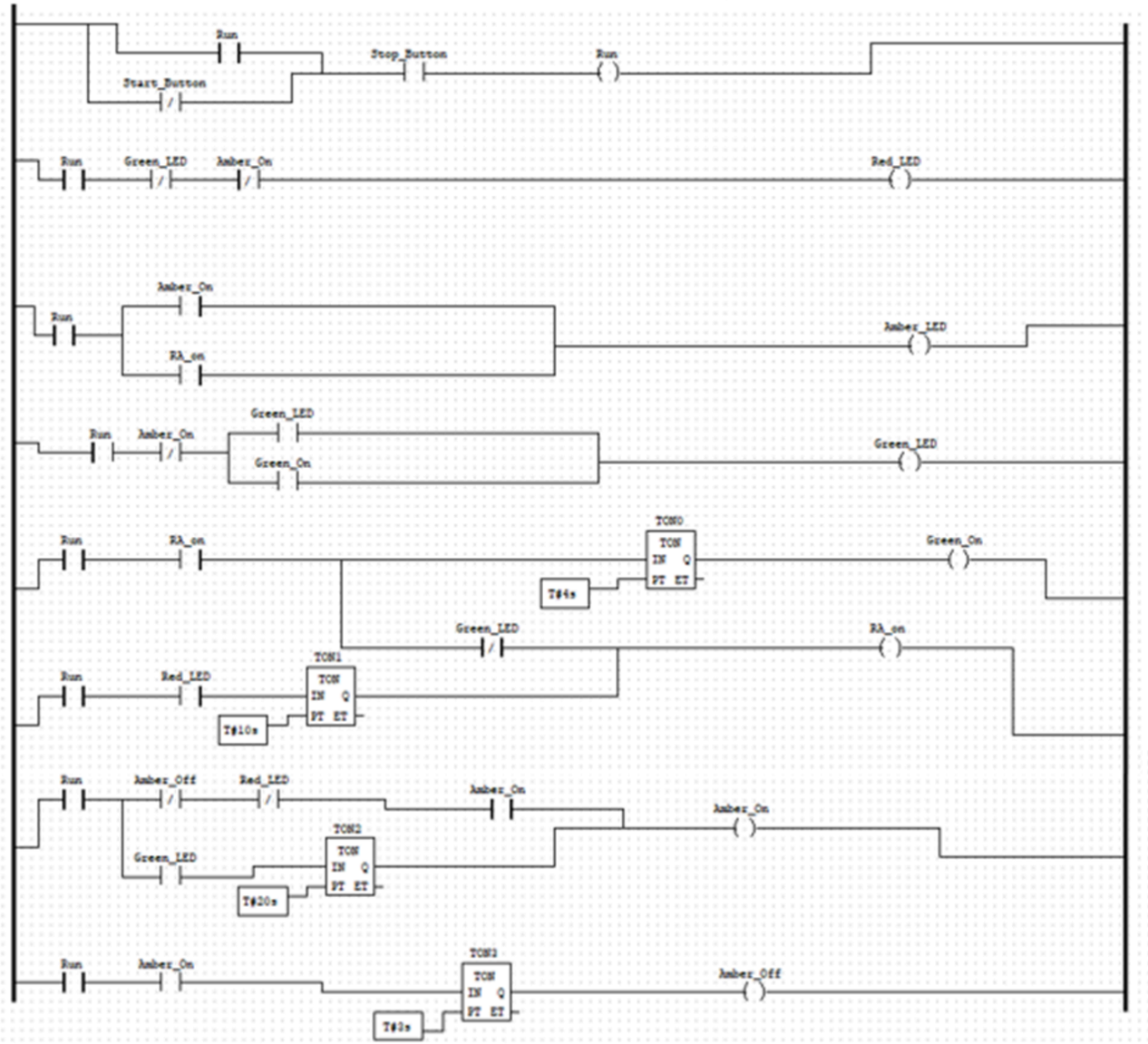
3 - Bottle Filling Plant

=


input_personInFront
input_doorIsClosing
input_doorIsClosed
output_openTheDoor

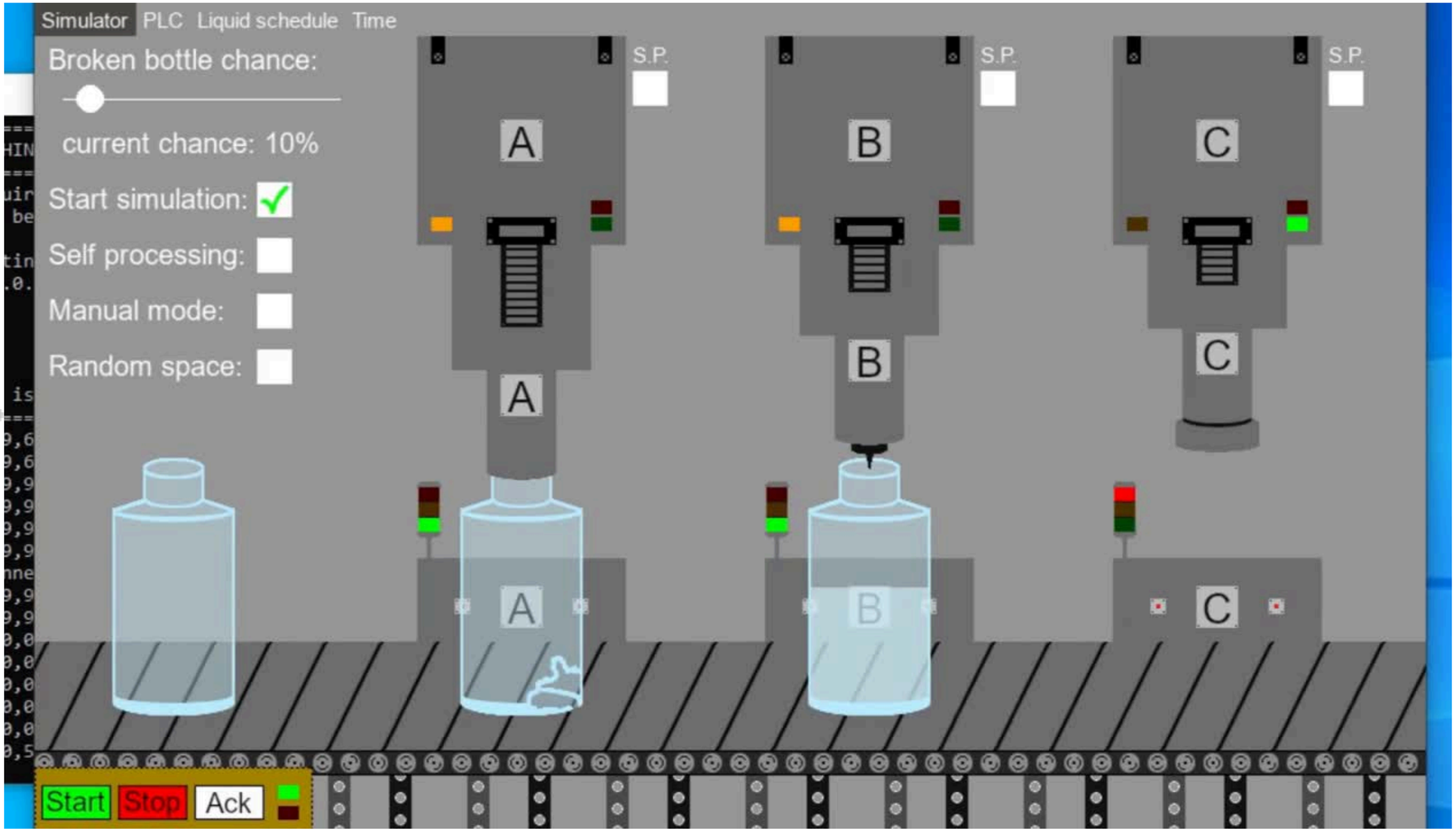

_machineA_operation_done
machineA_hasBottle
machineA_endPos
machineA_goDown
_machineA_operation_done
machineA_hasBottle
machineA_endPos
machineA_goDown
machineA_toolOff
machineA_toolOn
_machineA_operation_done
machineA_hasBottle
machineA_endPos
machineA_toolOn
timer
TON
IN
Q
250
PT
ET
0
_machineA_operation_done
S
_machineA_operation_done
machineA_hasBottle
machineA_endPos
machineA_goUp
machineA_toolOn
machineA_toolOff
_machineA_operation_done
machineA_hasBottle
machineA_toolOff
machineA_goUp
_machineA_operation_done
machineA_leftSensor
machineA_rightSensor
machineA_startPos
_machineA_operation_done
R

IV - The 3 main projects



IV - The 3 main projects

3 - Bottle Filling Plant



I - Host Organization & Problematic

II - Existing Situation, Tasks & Difficulties

III - Tools, Gantt Planning & Personal Organization

IV - The 3 main projects

V - Current VS Initial situation, Technical & Human Assessment

V - Current VS Initial situation, Technical & Human Assessment

Before

After

Before

1 simulation

After

3 simulations

V - Current VS Initial situation, Technical & Human Assessment

Before

1 simulation

No documentation

After

3 simulations

Documentation on:

- Ludus Installation
- Chemical Plant installation and utilisation
- Cardiff Metro Emulator installation and utilisation
- Bottle Filling Plant installation

V - Current VS Initial situation, Technical & Human Assessment

Before	After
1 simulation	3 simulations
No documentation	Documentation on: • Ludus Installation • Chemical Plant installation and utilisation • Cardiff Metro Emulator installation and utilisation • Bottle Filling Plant installation
No videos for presentations	Videos for: • Chemical Plant • Cardiff Metro Emulator • Bottle Filling Plant

V - Current VS Initial situation, Technical & Human Assessment

Before	After
1 simulation	3 simulations
No documentation	Documentation on: • Ludus Installation • Chemical Plant installation and utilisation • Cardiff Metro Emulator installation and utilisation • Bottle Filling Plant installation
No videos for presentations	Videos for: • Chemical Plant • Cardiff Metro Emulator • Bottle Filling Plant
No way to control the screen wall	A simple webpage to control all the screens

V - Current VS Initial situation, Technical & Human Assessment

Before	After
1 simulation	3 simulations
No documentation	Documentation on: • Ludus Installation • Chemical Plant installation and utilisation • Cardiff Metro Emulator installation and utilisation • Bottle Filling Plant installation
No videos for presentations	Videos for: • Chemical Plant • Cardiff Metro Emulator • Bottle Filling Plant
No way to control the screen wall	A simple webpage to control all the screens
No easy and educative way to approach cybersecurity	8 scenarios in the Backdoors&Breaches game

V - Current VS Initial situation, Technical & Human Assessment

Became comfortable with Virtual Machines

V - Current VS Initial situation, Technical & Human Assessment

Became comfortable with Virtual Machines

Learned how to install and use a Ludus server

V - Current VS Initial situation, Technical & Human Assessment

Became comfortable with Virtual Machines

Learned how to install and use a Ludus server

Cybersecurity knowledge expanded

V - Current VS Initial situation, Technical & Human Assessment

Became comfortable with Virtual Machines

Learned how to install and use a Ludus server

Cybersecurity knowledge expanded

What is a PLC & how to program it with ladder logic

V - Current VS Initial situation, Technical & Human Assessment

Became comfortable with Virtual Machines

Learned how to install and use a Ludus server

Cybersecurity knowledge expanded

What is a PLC & how to program it with ladder logic

Modbus command

V - Current VS Initial situation, Technical & Human Assessment

Became comfortable with Virtual Machines

Learned how to install and use a Ludus server

Cybersecurity knowledge expanded

What is a PLC & how to program it with ladder logic

Modbus command

Typical cyber-attacks & how to defend them

V - Current VS Initial situation, Technical & Human Assessment

Discovered people and a new culture

Discovered people and a new culture

Discovered the work environment in a new and modern company

V - Current VS Initial situation, Technical & Human Assessment

Discovered people and a new culture

Discovered the work environment in a new and modern company

Loved working with the whole team

V - Current VS Initial situation, Technical & Human Assessment

Discovered people and a new culture

Discovered the work environment in a new and modern company

Loved working with the whole team

Discovered the Cardiff city

V - Current VS Initial situation, Technical & Human Assessment

Discovered people and a new culture

Discovered the work environment in a new and modern company

Loved working with the whole team

Discovered the Cardiff city

Discovered what it is to live in a foreign country on my own

Cybersecurity in Operational Technologies

Final words

FONDATION RENNES 1
Progresser Innover Entreprendre

Hyb Arloesedd Seiber
Cyber Innovation Hub

iut Lannion