

Internship at the Cyber Innovation Hub

Cybersecurity in Operational Technologies



Hyb Arloesedd Seiber
Cyber Innovation Hub







7 Avril 2025



7 Avril 2025 → 13 Juin 2025



7 Avril 2025 $\xrightarrow{10 \text{ semaines}}$ 13 Juin 2025



7 Avril 2025 $\xrightarrow{10 \text{ semaines}}$ 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

I - Host Organization & Problematic



I - Host Organization & Problematic

Legal Status: **Non-profit**



I - Host Organization & Problematic

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



CARDIFF
UNIVERSITY



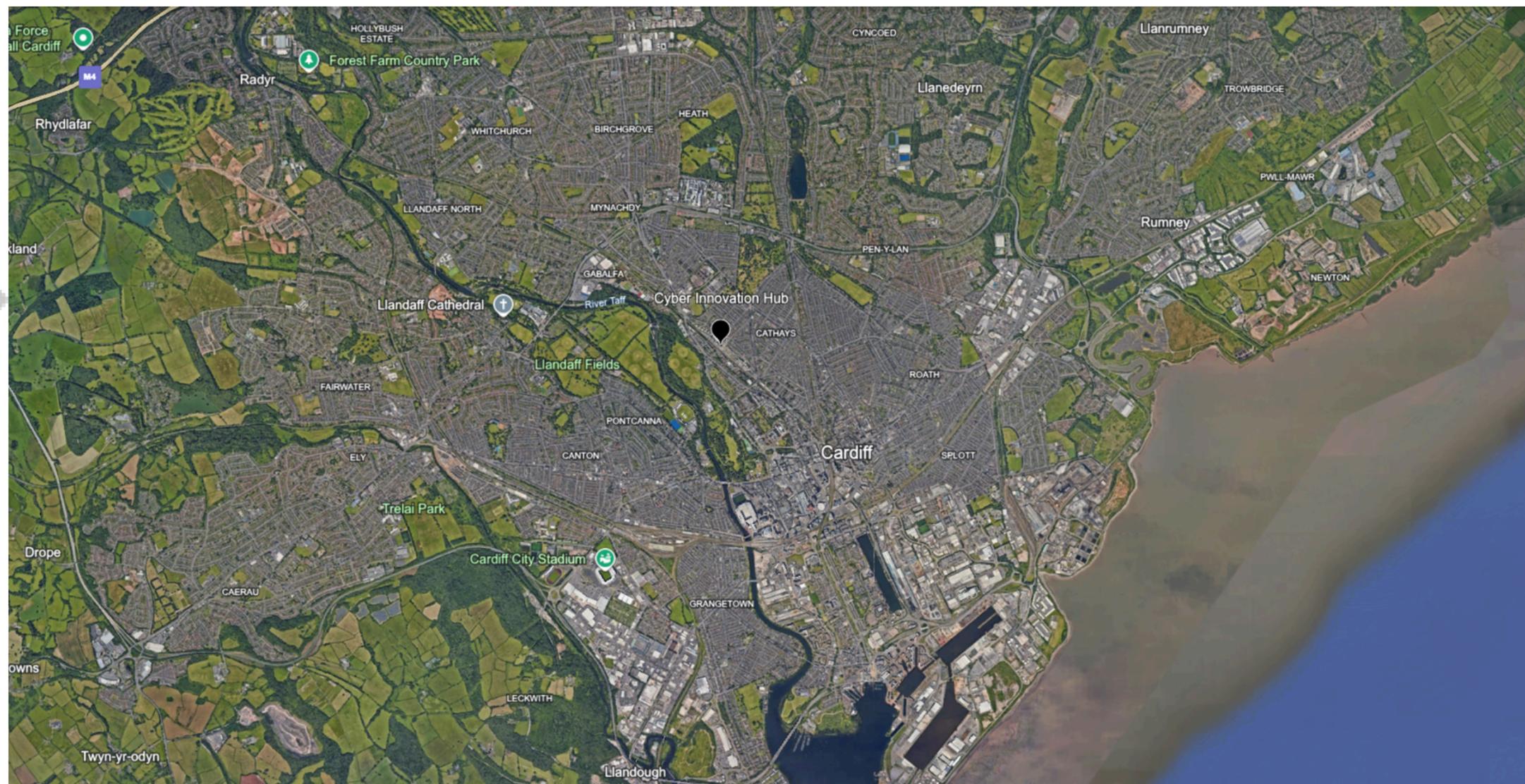
PRIFYSGOL
CAERDYDD

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

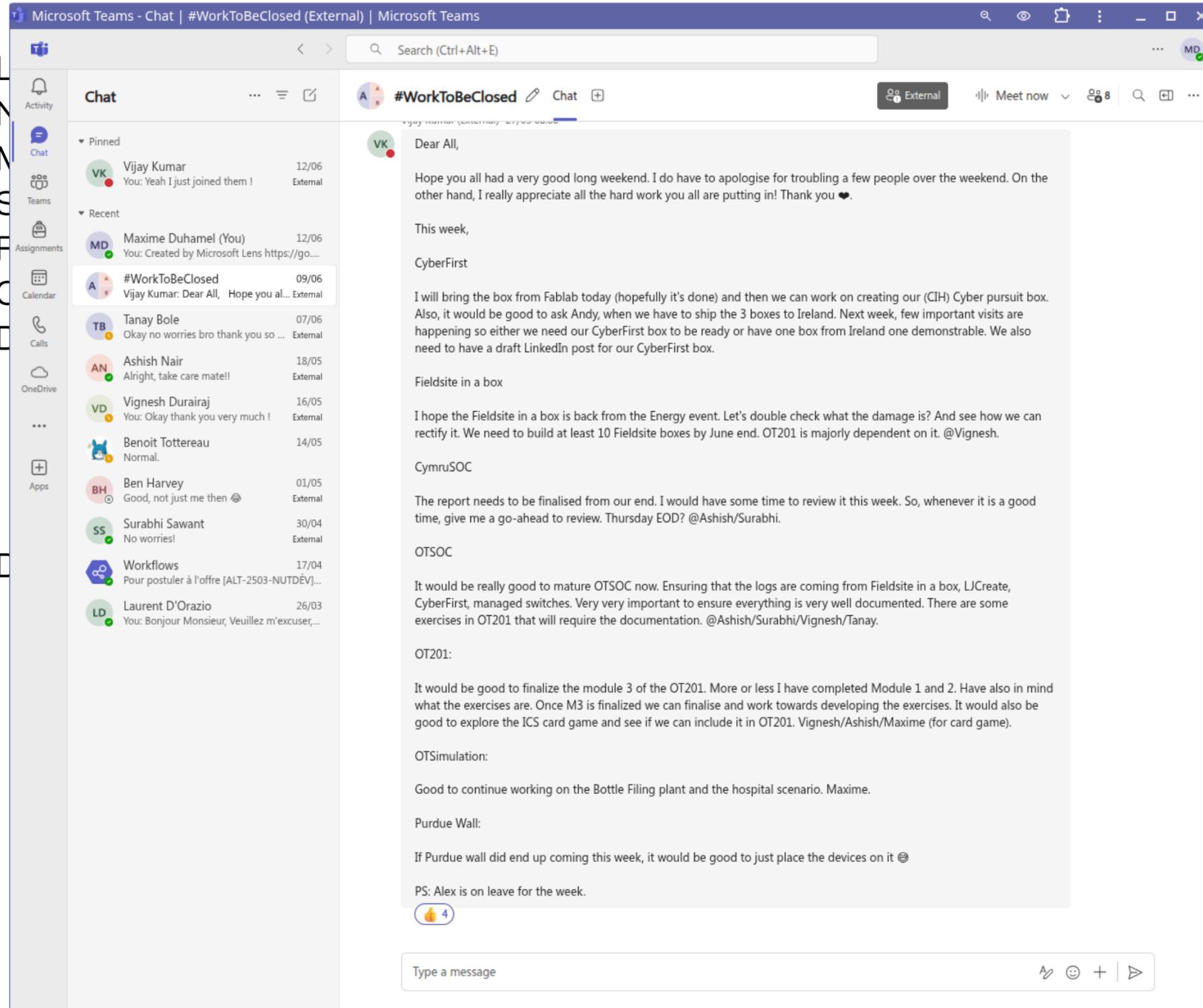
Customers: Businesses and governmental organizations

Divisions:

- Commercials
- Operations
- Strategy
- Delivery (Mine)

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

I - Host Organization & Problematic



by 2030

I - Host Organization & Problematic



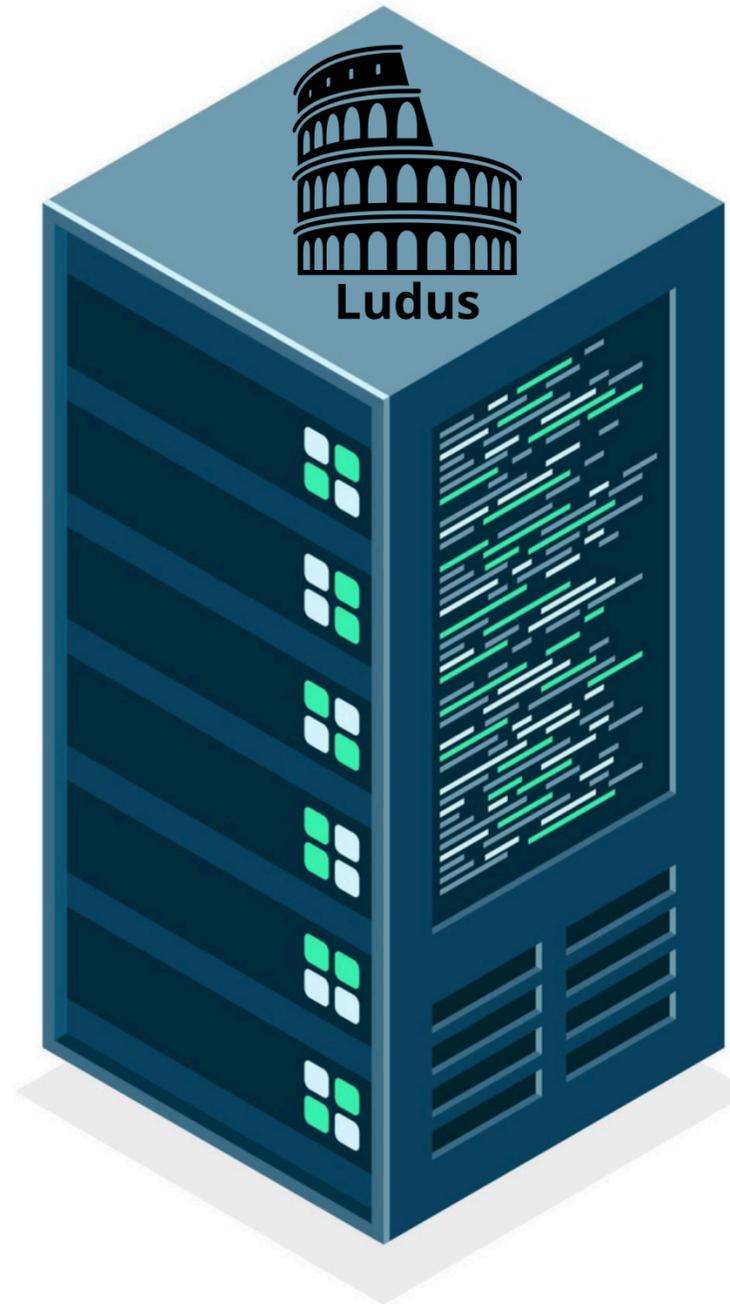
30



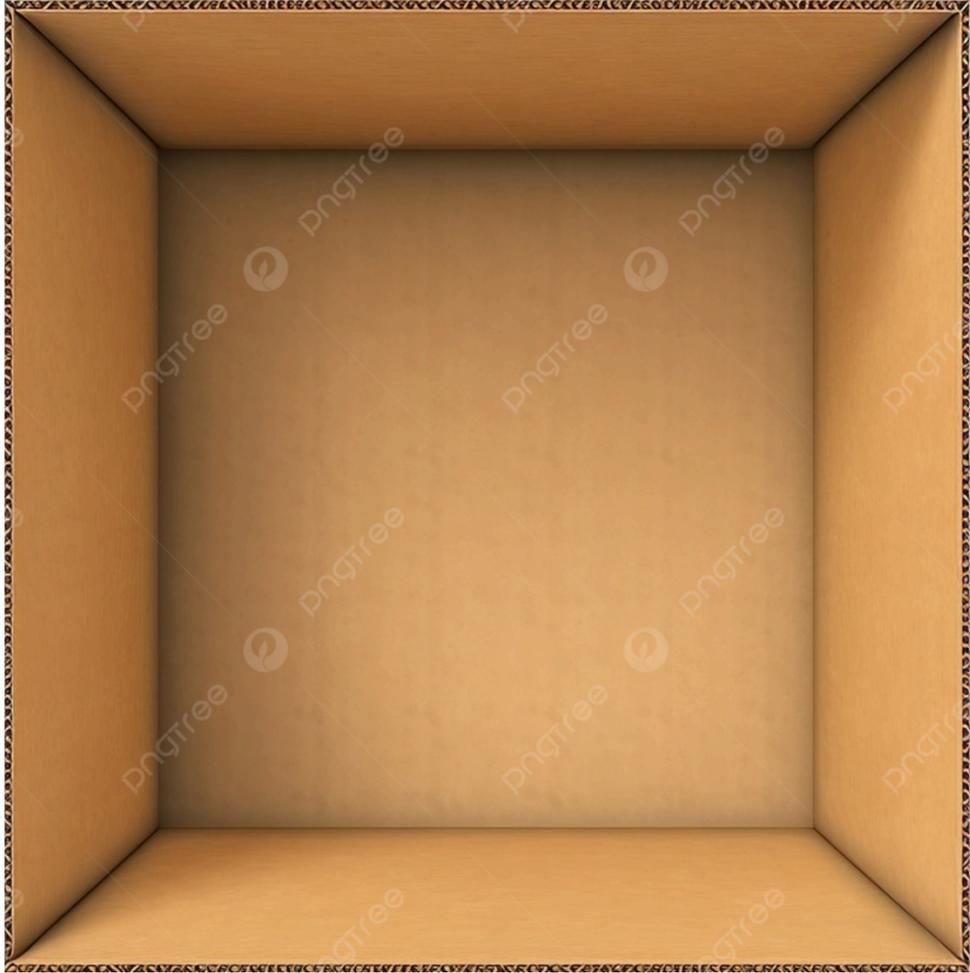
How can the CIH simulate realistic cyberattack environments to efficiently train teams in defense and incident response?

- 
- 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

II - Existing Situation, Tasks & Difficulties

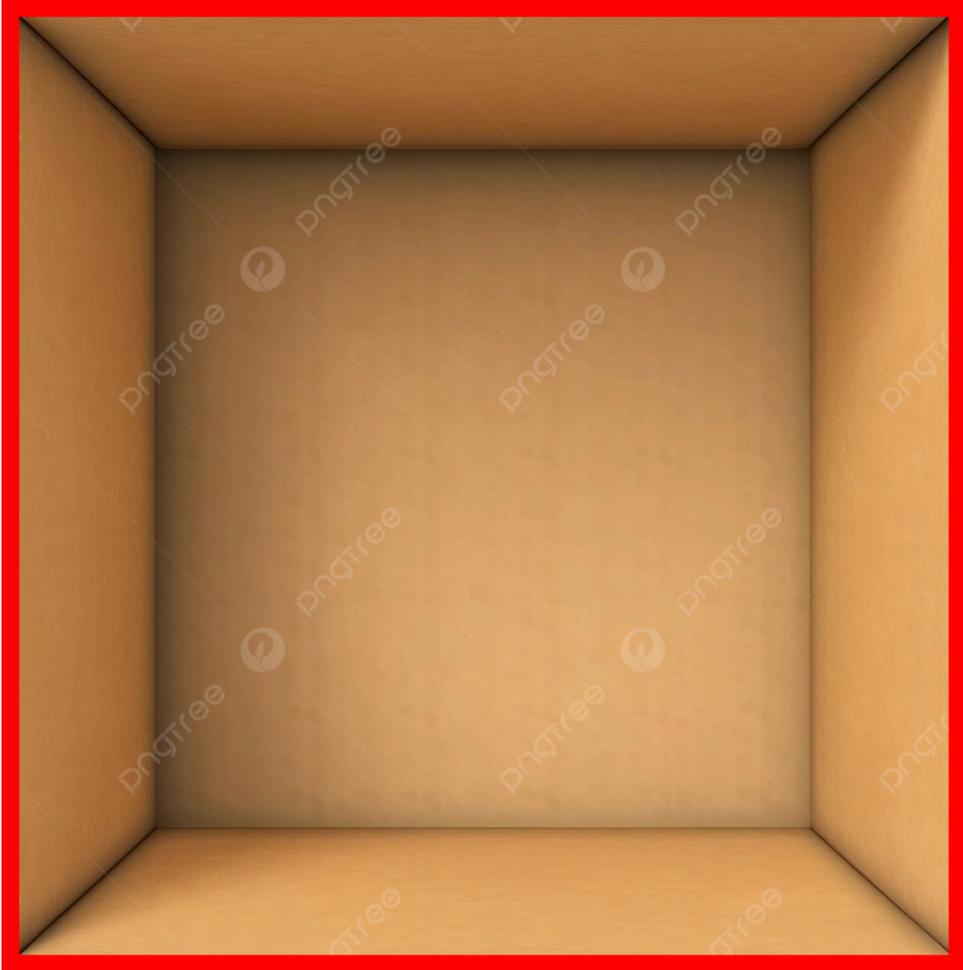


II - Existing Situation, Tasks & Difficulties



II - Existing Situation, Tasks & Difficulties

Your computer
(physical machine)



II - Existing Situation, Tasks & Difficulties

Your computer
(physical machine)



II - Existing Situation, Tasks & Difficulties

Your computer
(physical machine)



II - Existing Situation, Tasks & Difficulties

Your computer
(physical machine)



II - Existing Situation, Tasks & Difficulties

Your computer
(physical machine)



II - Existing Situation, Tasks & Difficulties

Your computer
(physical machine)



II - Existing Situation, Tasks & Difficulties

Your computer
(physical machine)



II - Existing Situation, Tasks & Difficulties

Your computer
(physical machine)



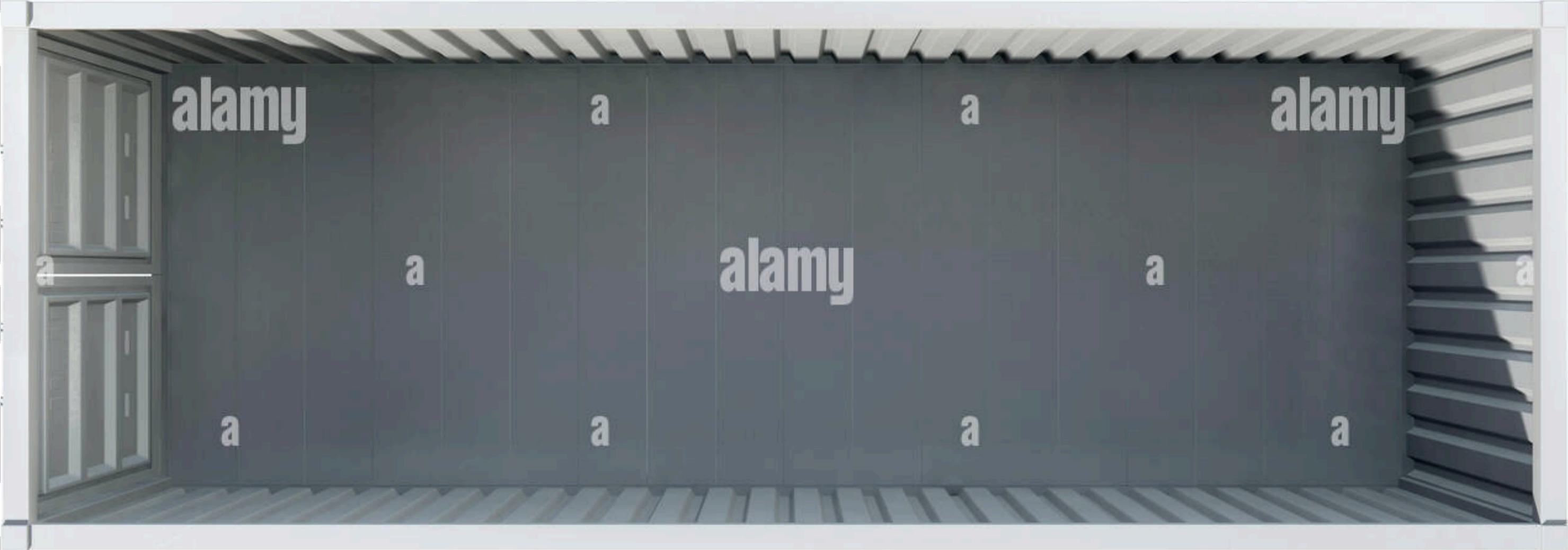
II - Existing Situation, Tasks & Difficulties

Your computer
(physical machine)



Virtual Machine

II - Existing Situation, Tasks & Difficulties

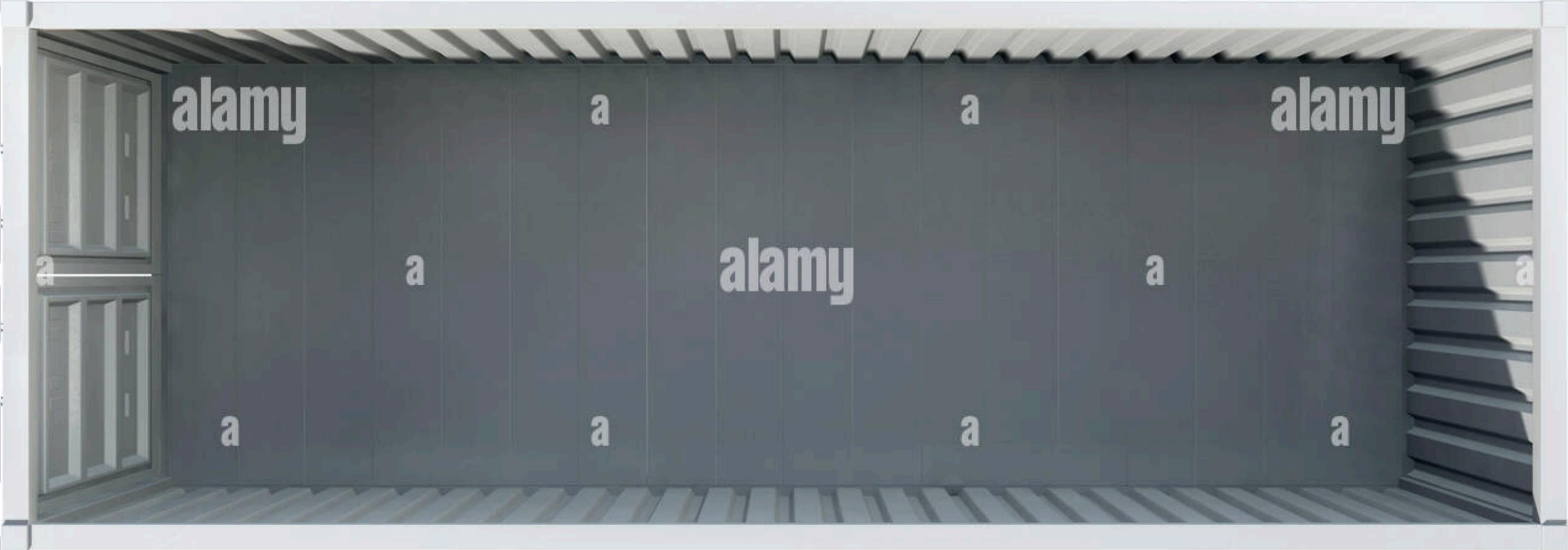


II - Existing Situation, Tasks & Difficulties

User 1

User 2

User 3

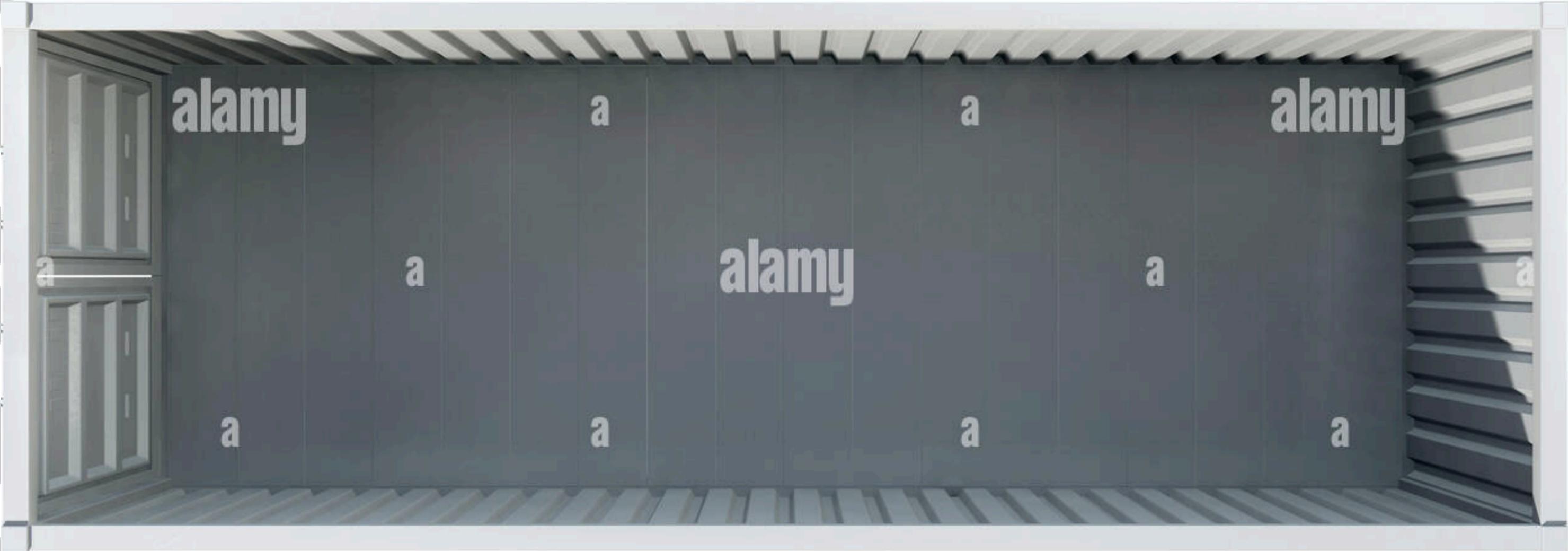


II - Existing Situation, Tasks & Difficulties

User 1

User 2

User 3



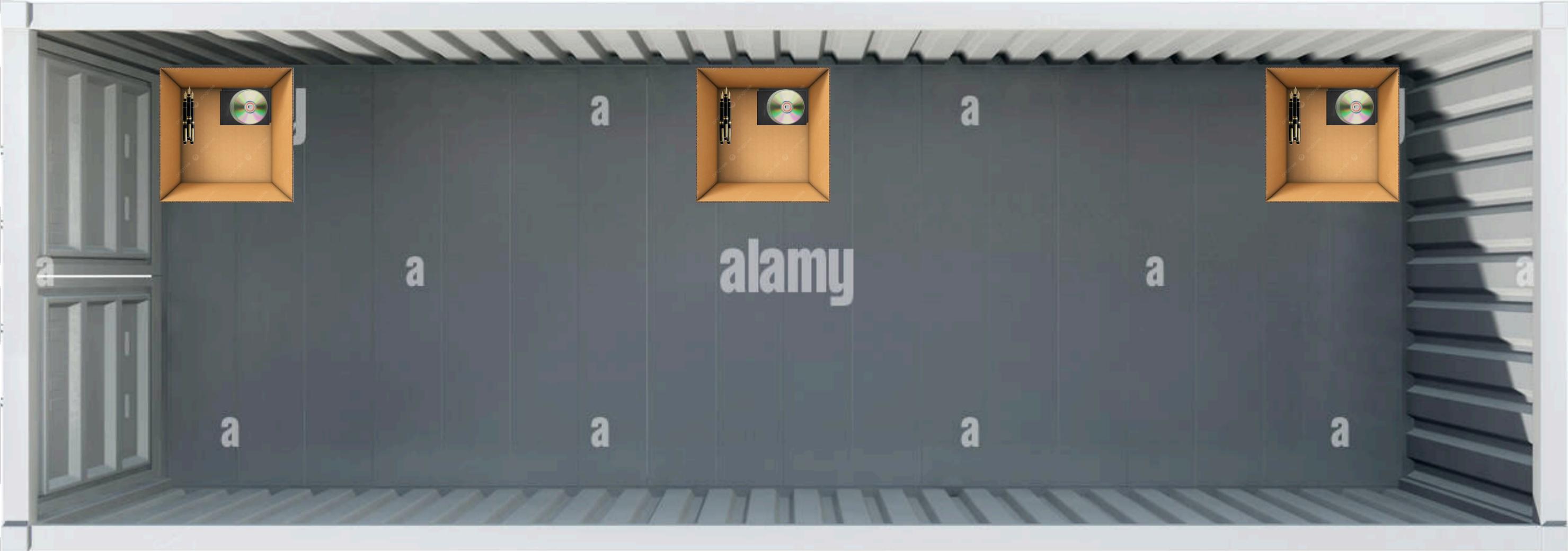
Virtual Machine 1

II - Existing Situation, Tasks & Difficulties

User 1

User 2

User 3



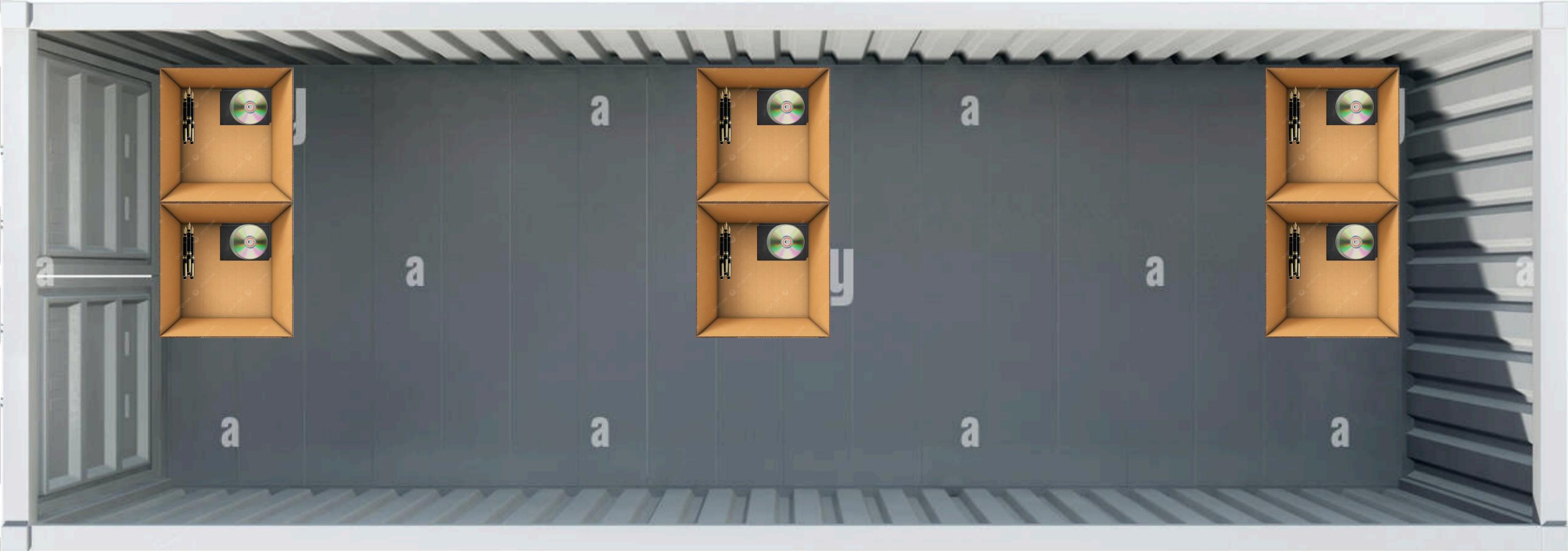
Virtual Machine 1

II - Existing Situation, Tasks & Difficulties

User 1

User 2

User 3



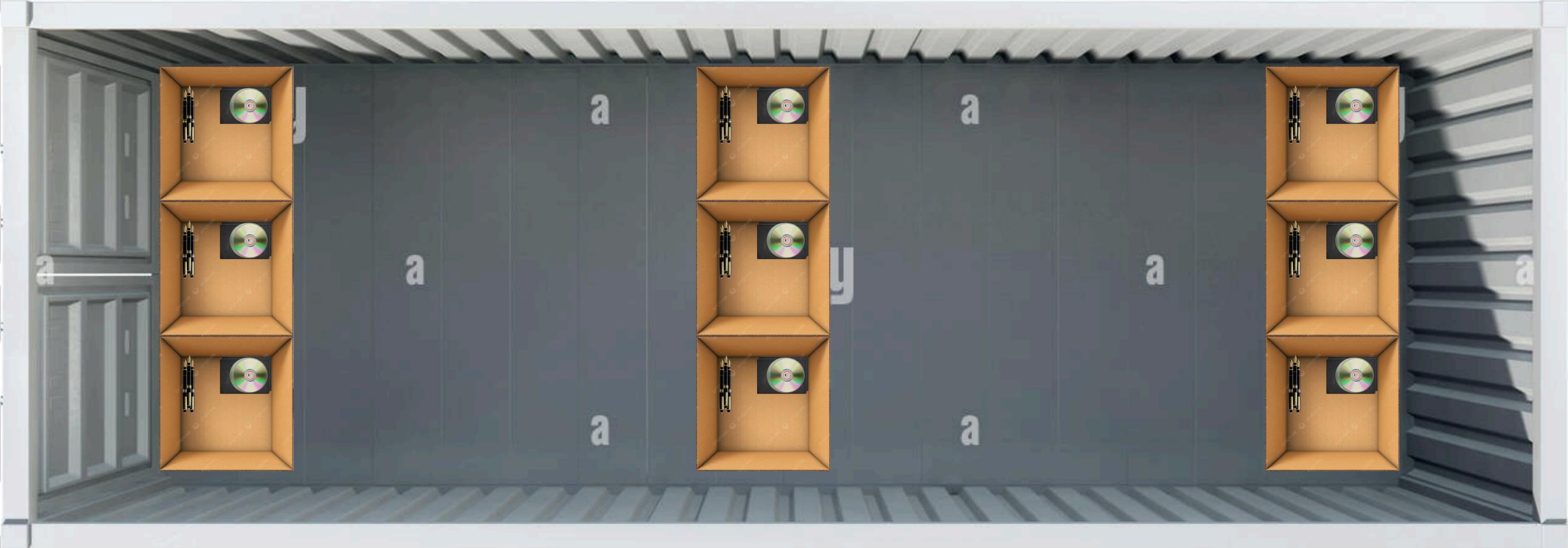
Virtual Machine 1

II - Existing Situation, Tasks & Difficulties

User 1

User 2

User 3



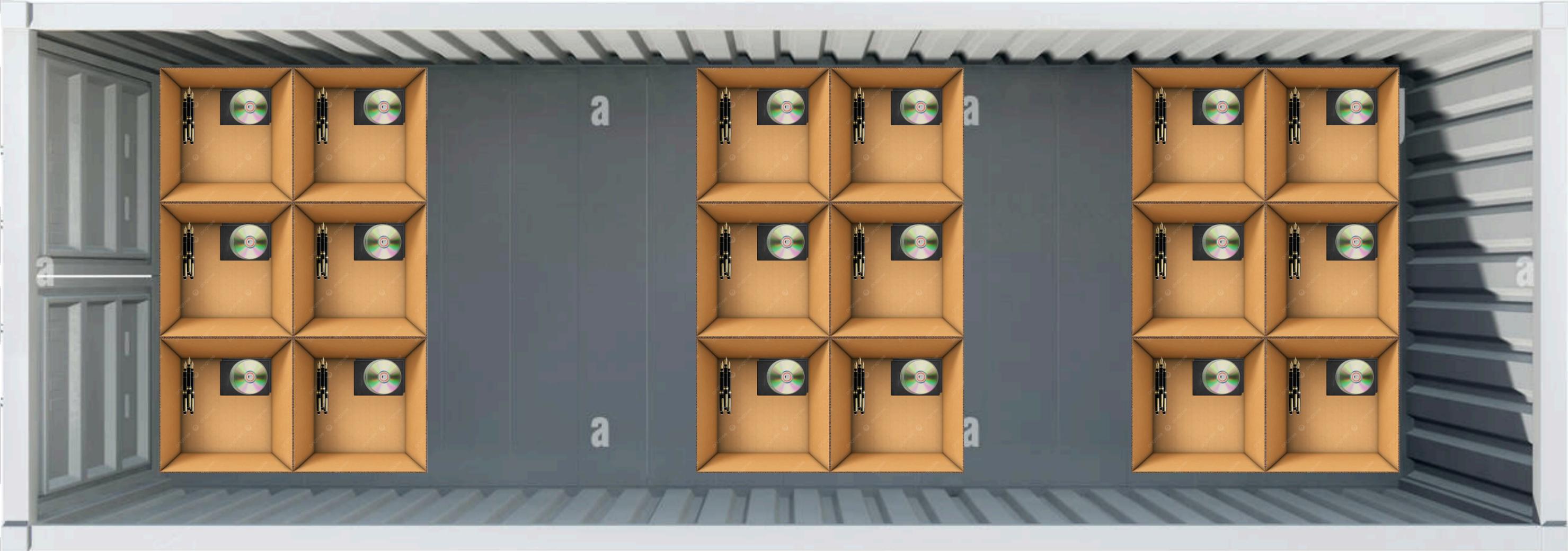
Virtual Machine 1

II - Existing Situation, Tasks & Difficulties

User 1

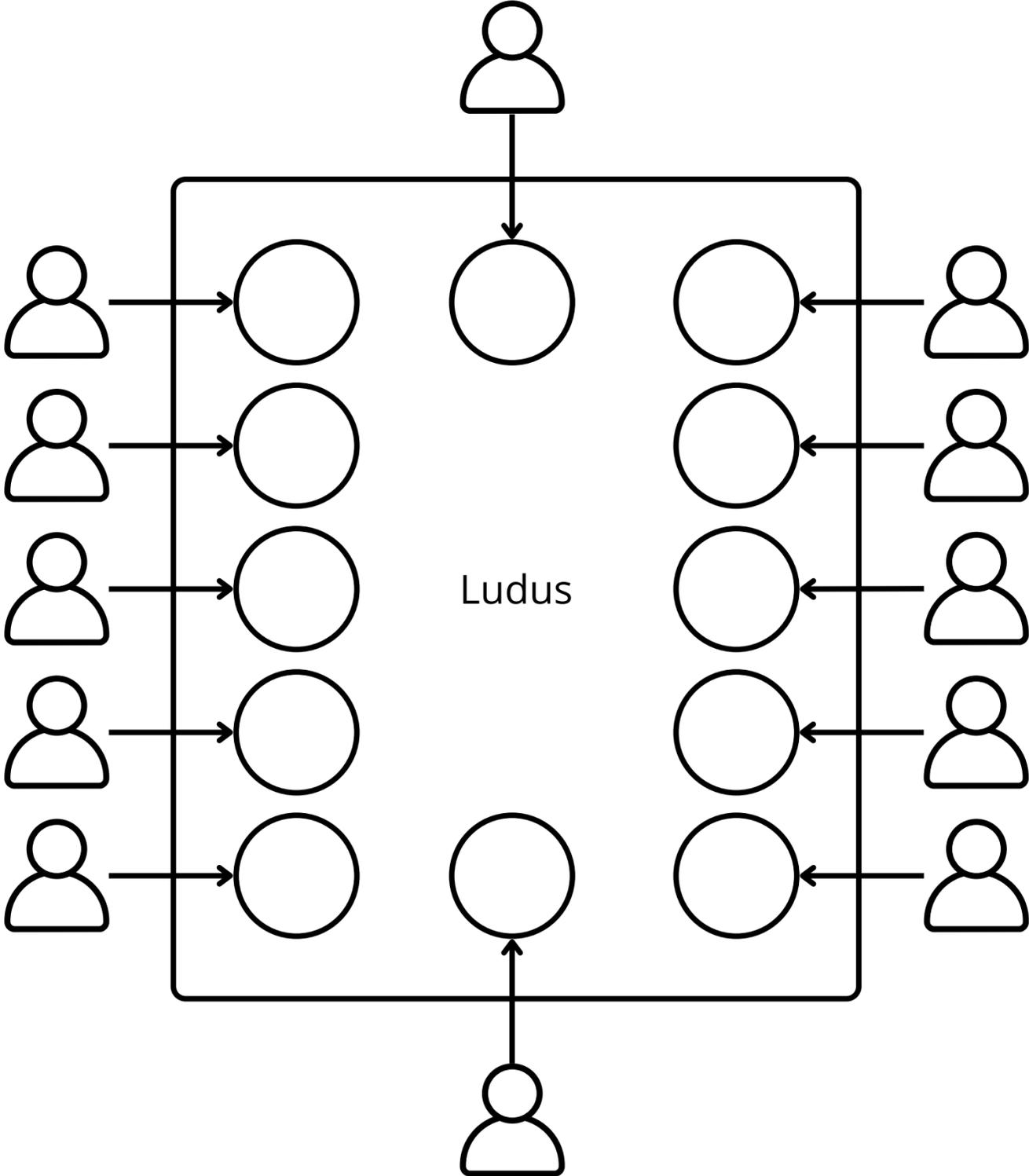
User 2

User 3

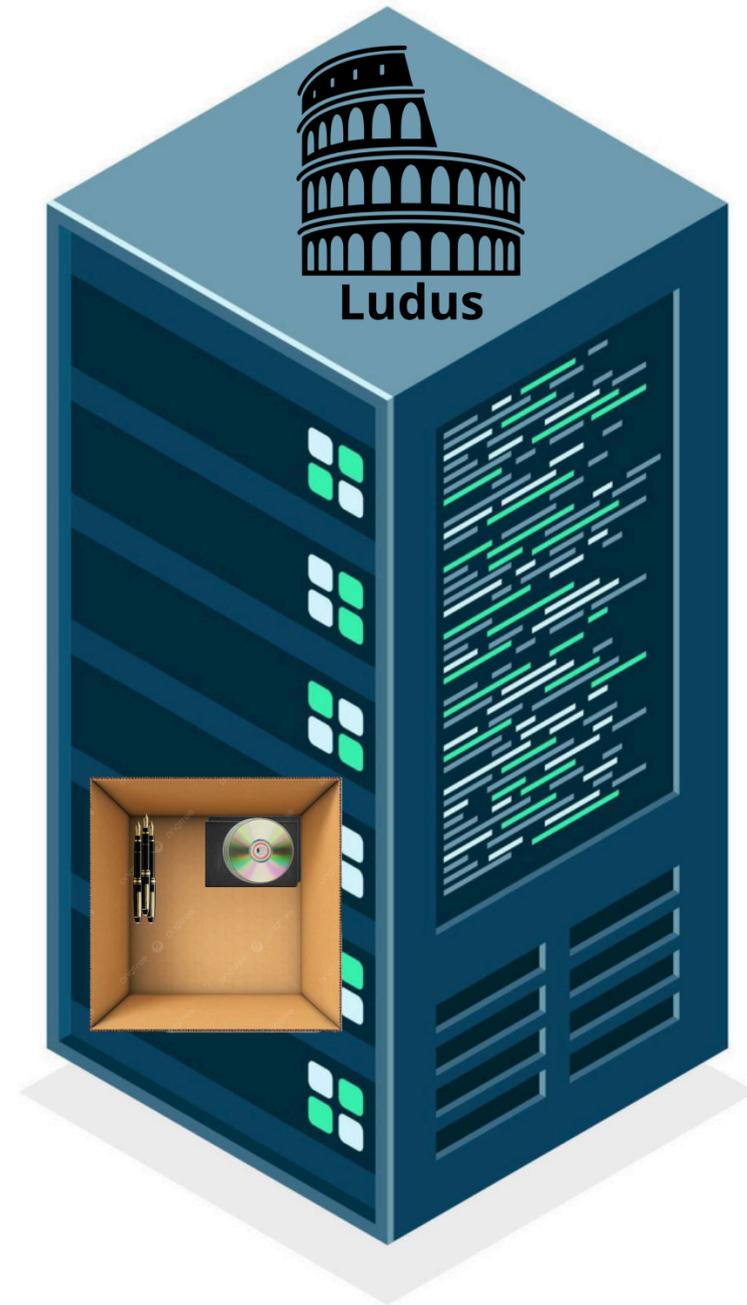


Virtual Machine 1

II - Existing Situation, Tasks & Difficulties



II - Existing Situation, Tasks & Difficulties



- 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



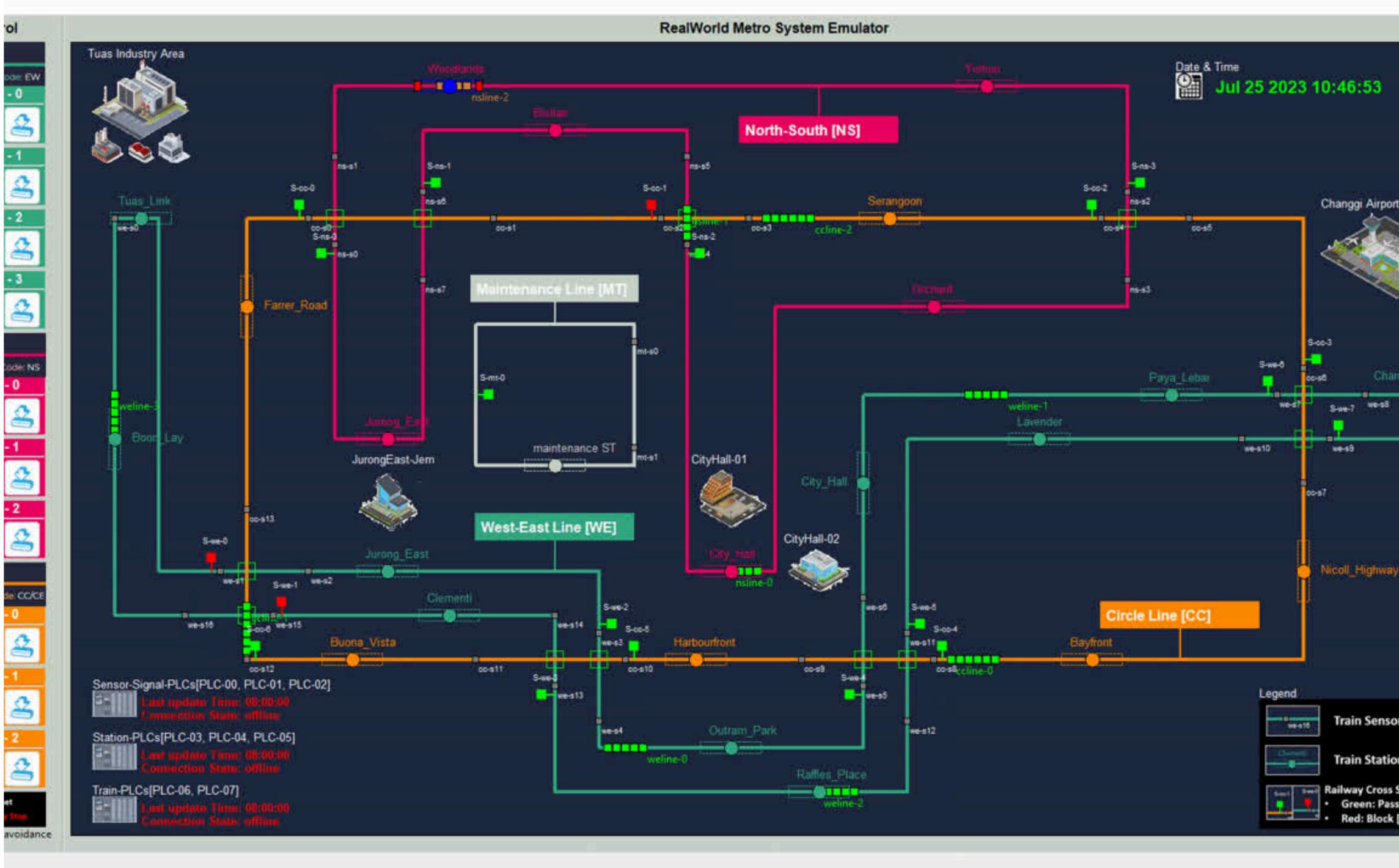
II - Existing Situation, Tasks & Difficulties

1 - Installing and configuring the simulations



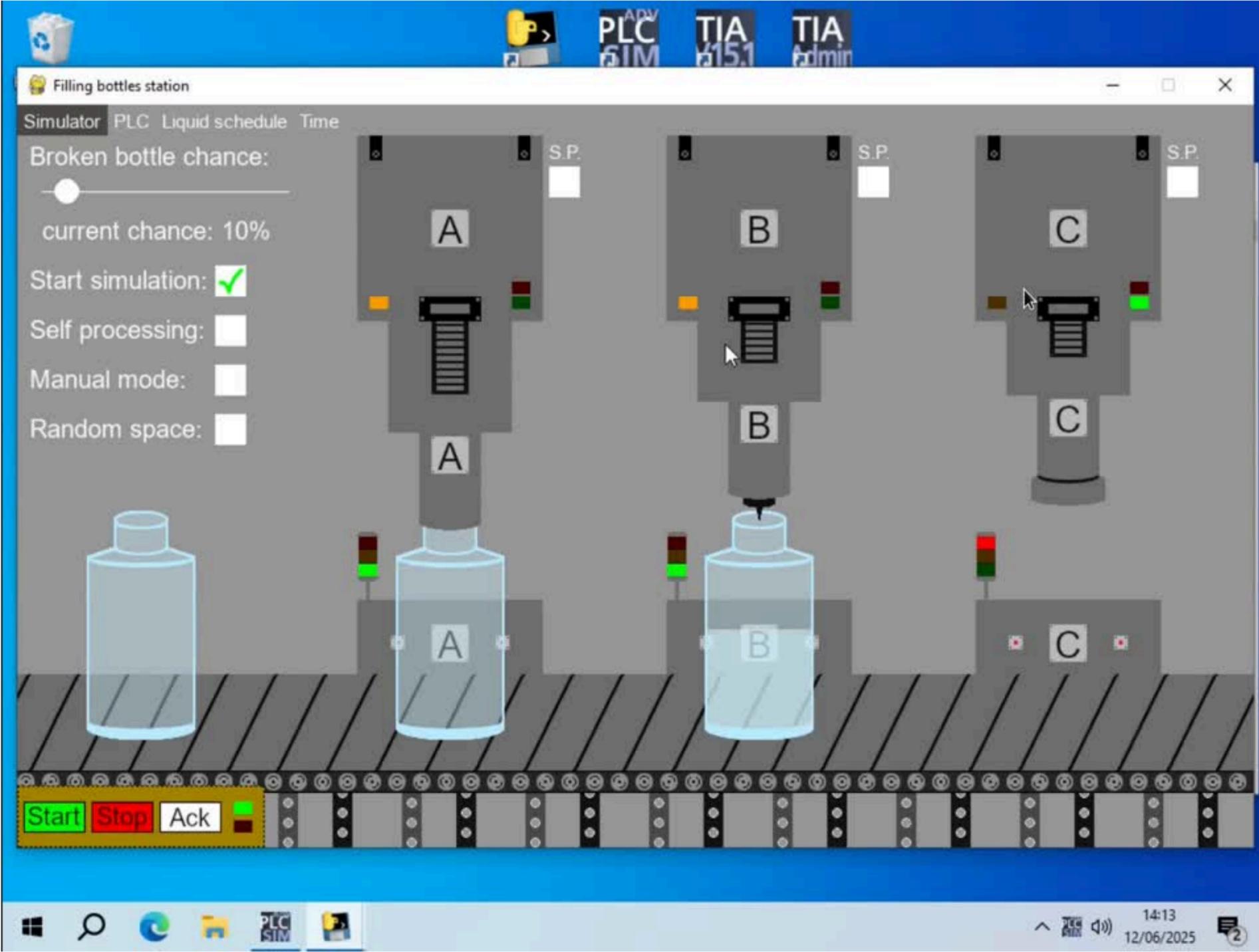
II - Existing Situation, Tasks & Difficulties

1 - Installing and configuring the simulations



II - Existing Situation, Tasks & Difficulties

1 - Installing and configuring the simulations

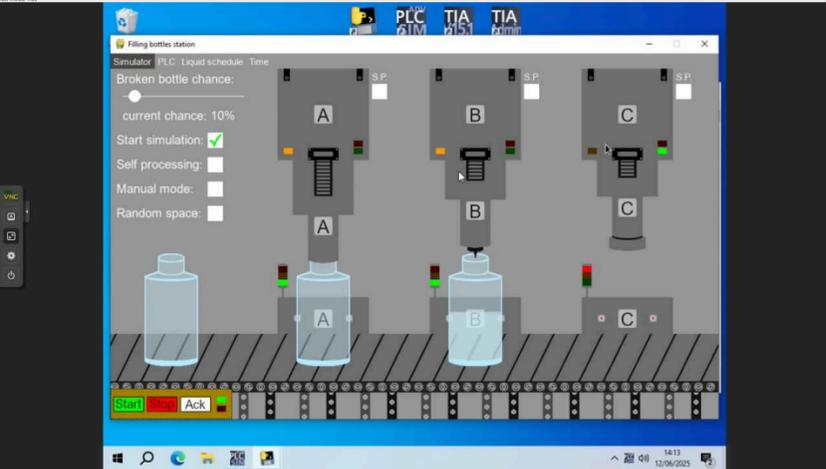
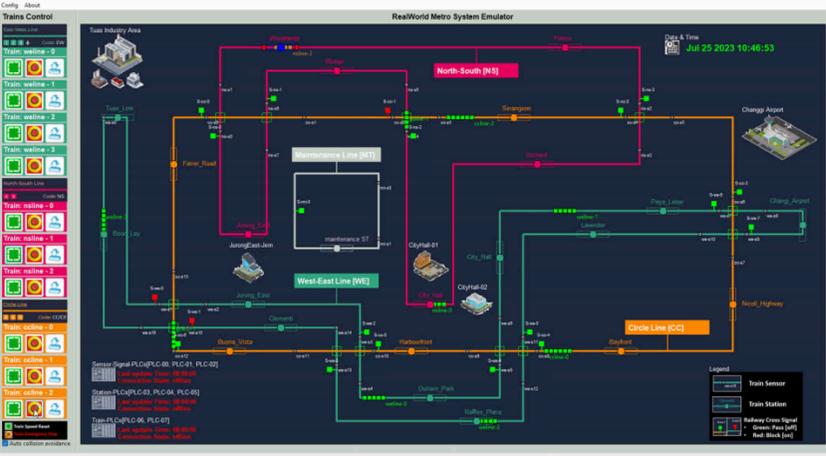


II - Existing Situation, Tasks & Difficulties

1 - Installing and configuring the simulations



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

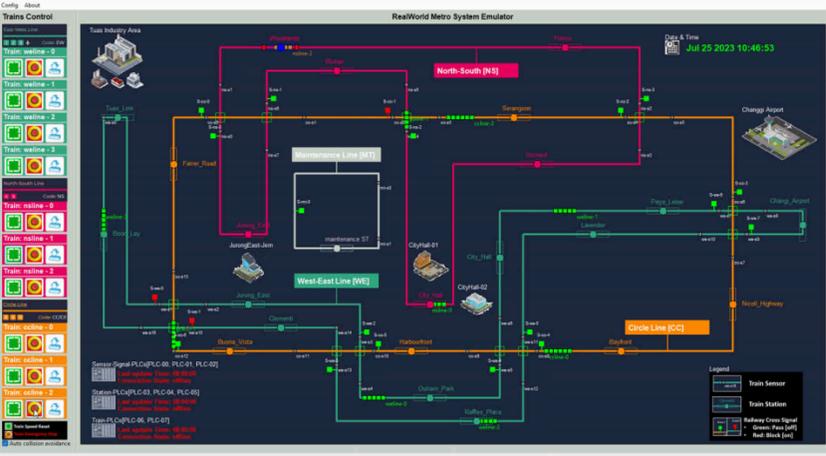


II - Existing Situation, Tasks & Difficulties

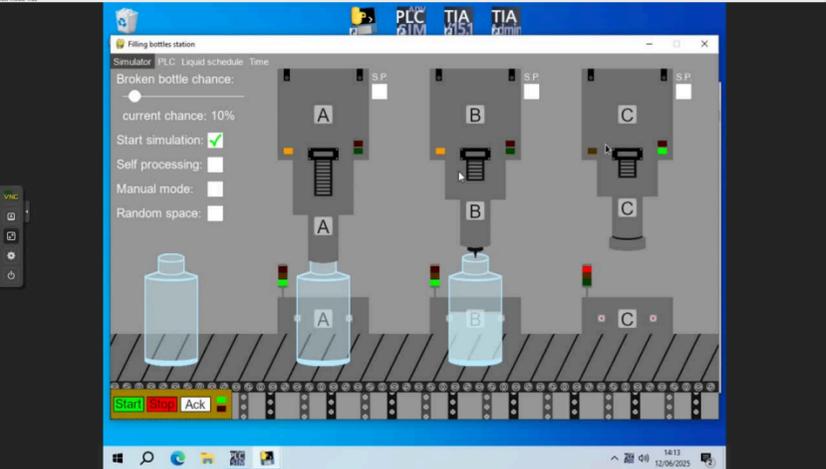
1 - Installing and configuring the simulations



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



Steep **learning curve**

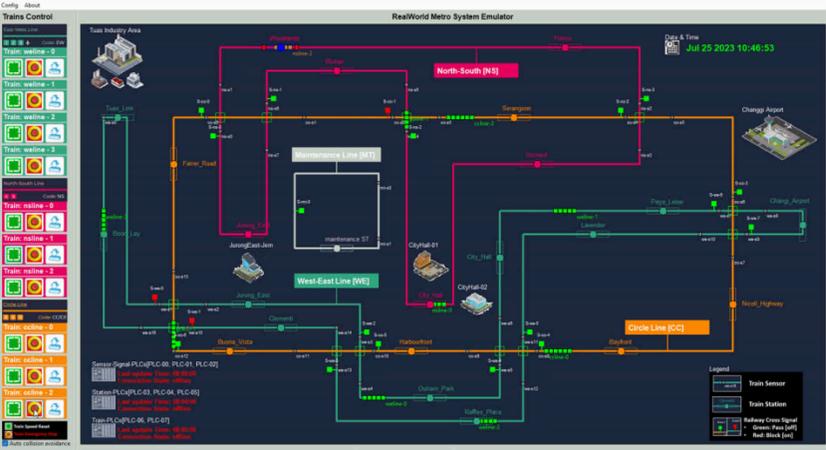


II - Existing Situation, Tasks & Difficulties

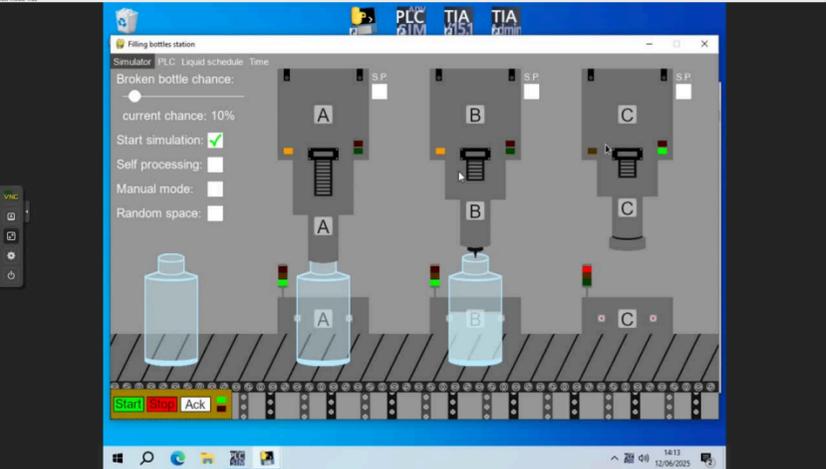
1 - Installing and configuring the simulations



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



II - Existing Situation, Tasks & Difficulties

1 - Installing and configuring the simulations

2 - Deploying and managing the ranges

3 - Documenting the processes

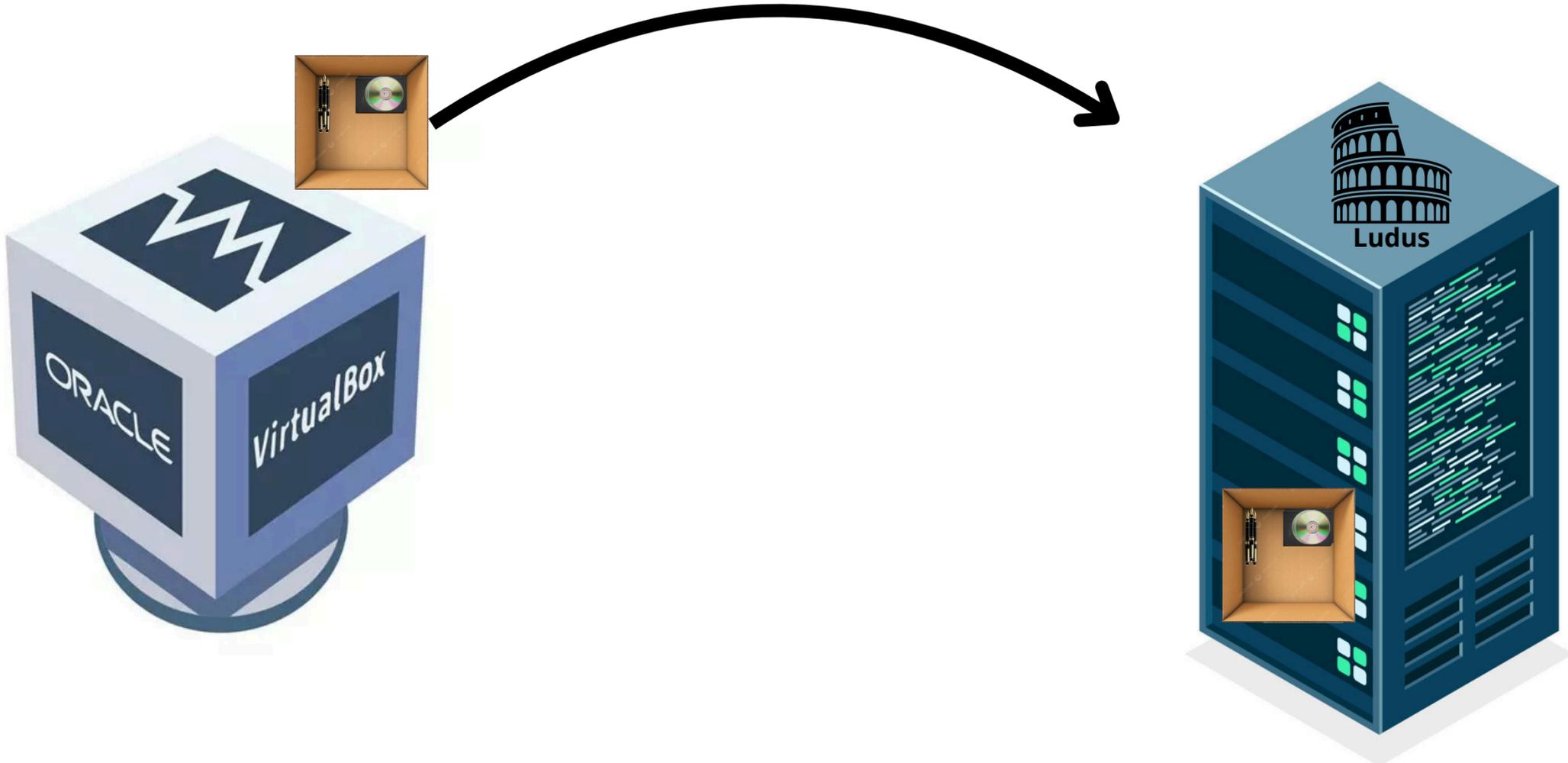
II - Existing Situation, Tasks & Difficulties

2 - Deploying and managing the ranges



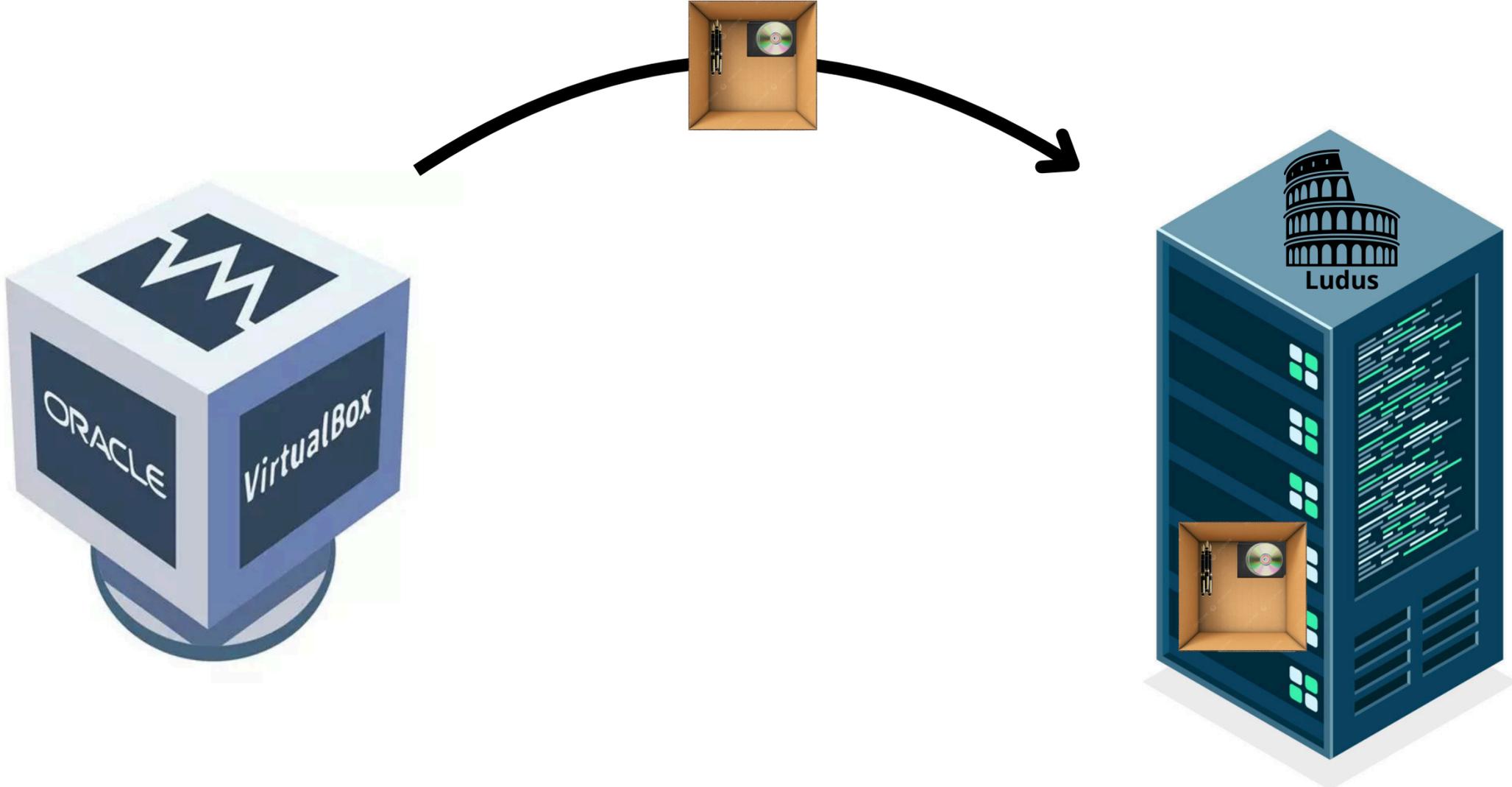
II - Existing Situation, Tasks & Difficulties

2 - Deploying and managing the ranges

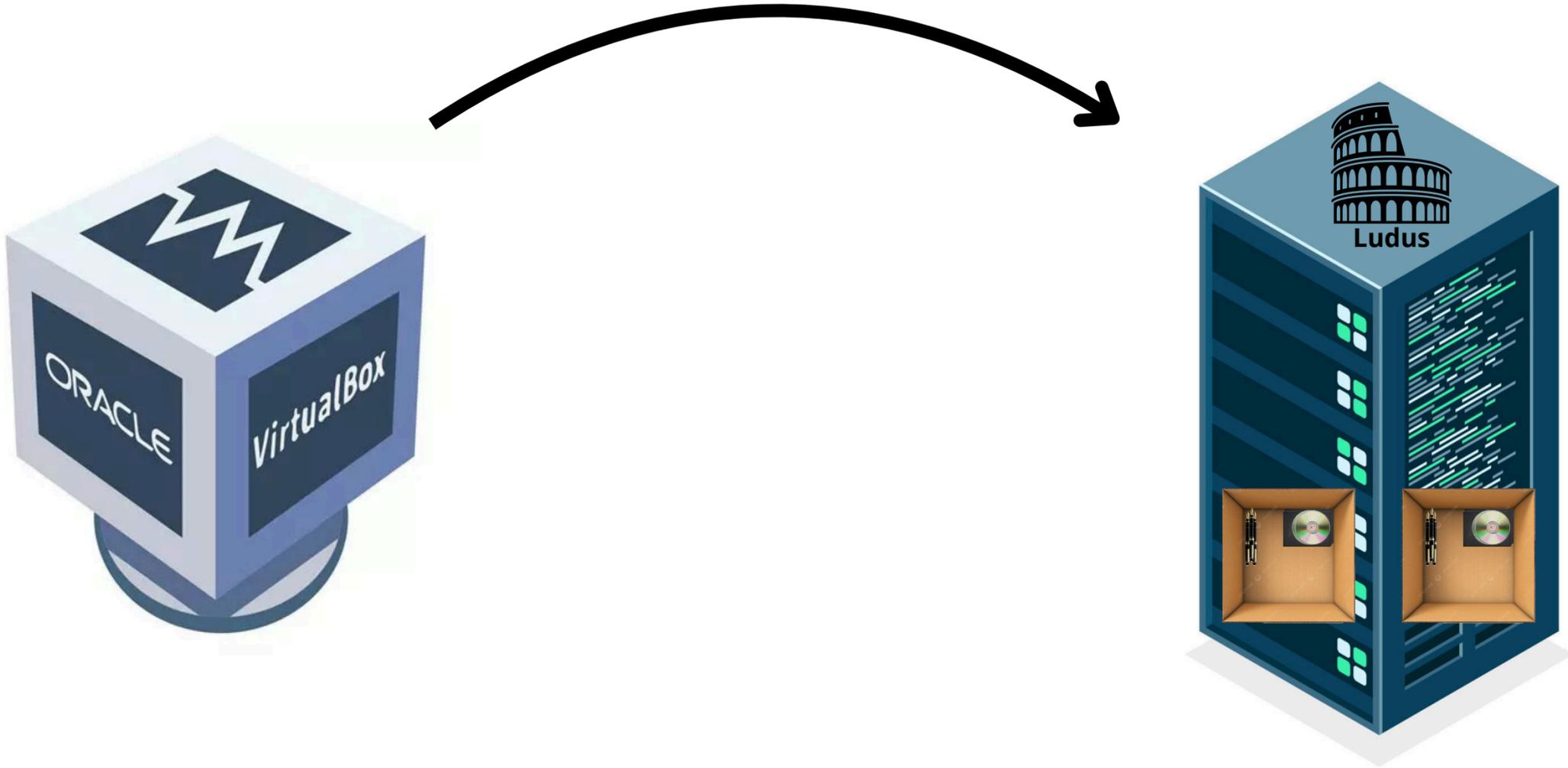


II - Existing Situation, Tasks & Difficulties

2 - Deploying and managing the ranges



II - Existing Situation, Tasks & Difficulties
2 - Deploying and managing the ranges

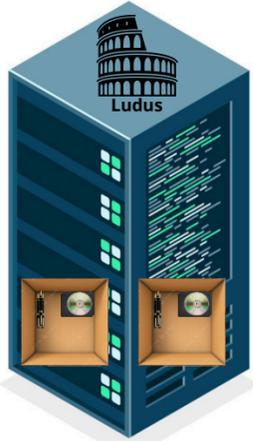
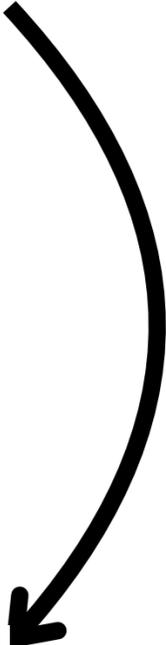


II - Existing Situation, Tasks & Difficulties

2 - Deploying and managing the ranges

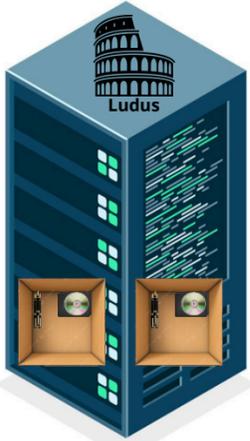
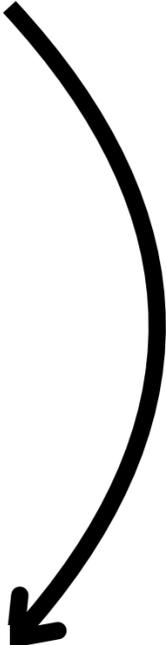


Ensure the range could be **easily duplicated** for different users



II - Existing Situation, Tasks & Difficulties

2 - Deploying and managing the ranges

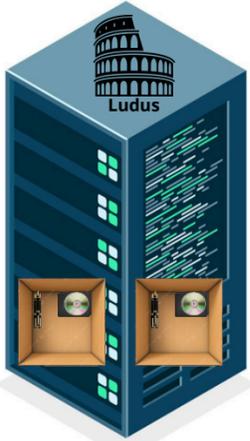
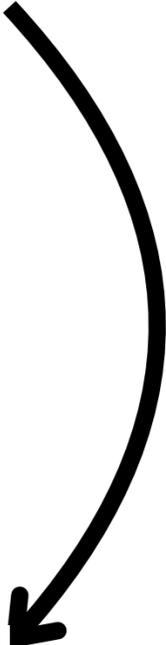


Ensure the range could be **easily duplicated** for different users

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

II - Existing Situation, Tasks & Difficulties

2 - Deploying and managing the ranges



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



II - Existing Situation, Tasks & Difficulties

- 1 - Installing and configuring the simulations
- 2 - Deploying and managing the ranges
- 3 - Documenting the processes**

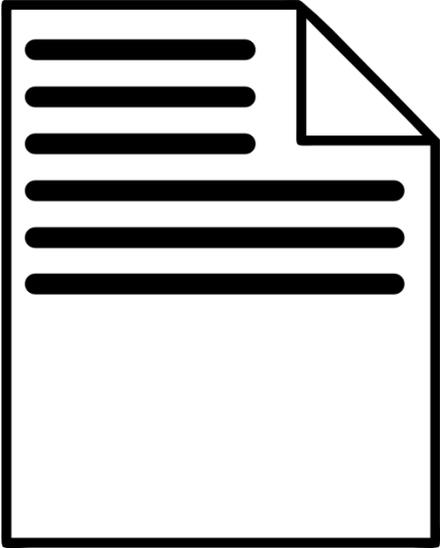
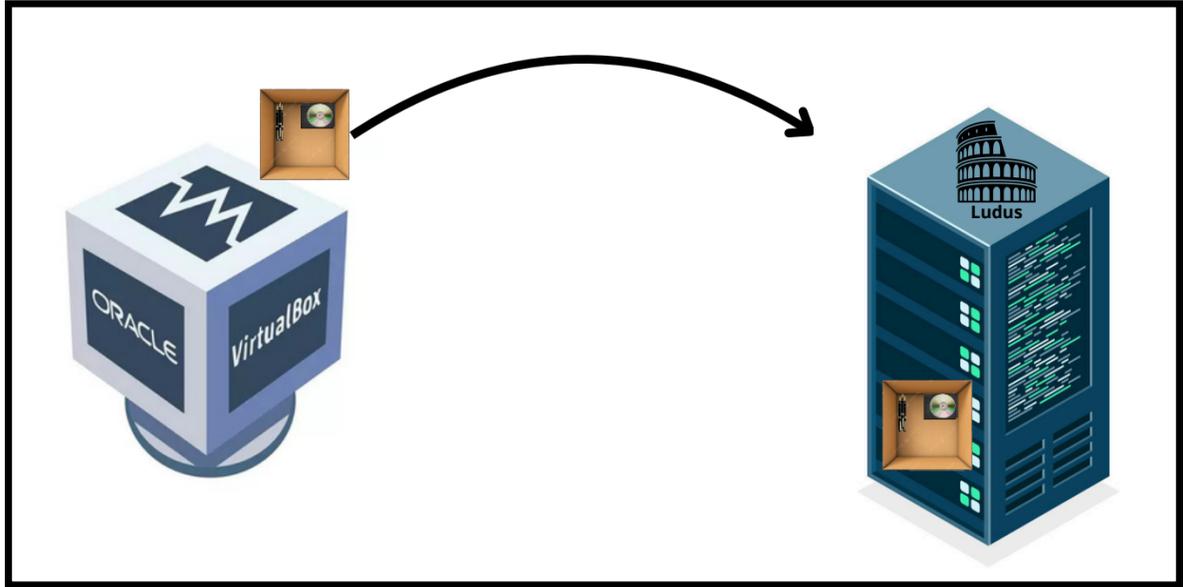
II - Existing Situation, Tasks & Difficulties

3 - Documenting the processes

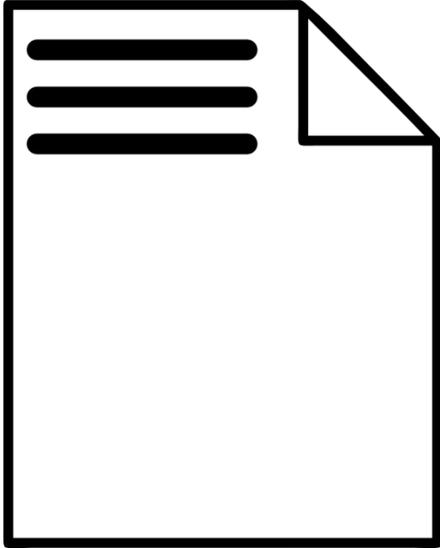
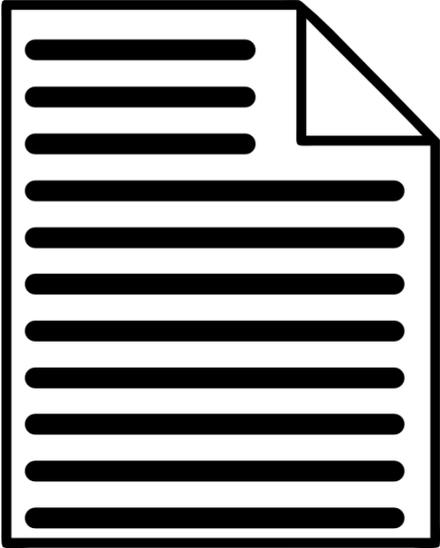
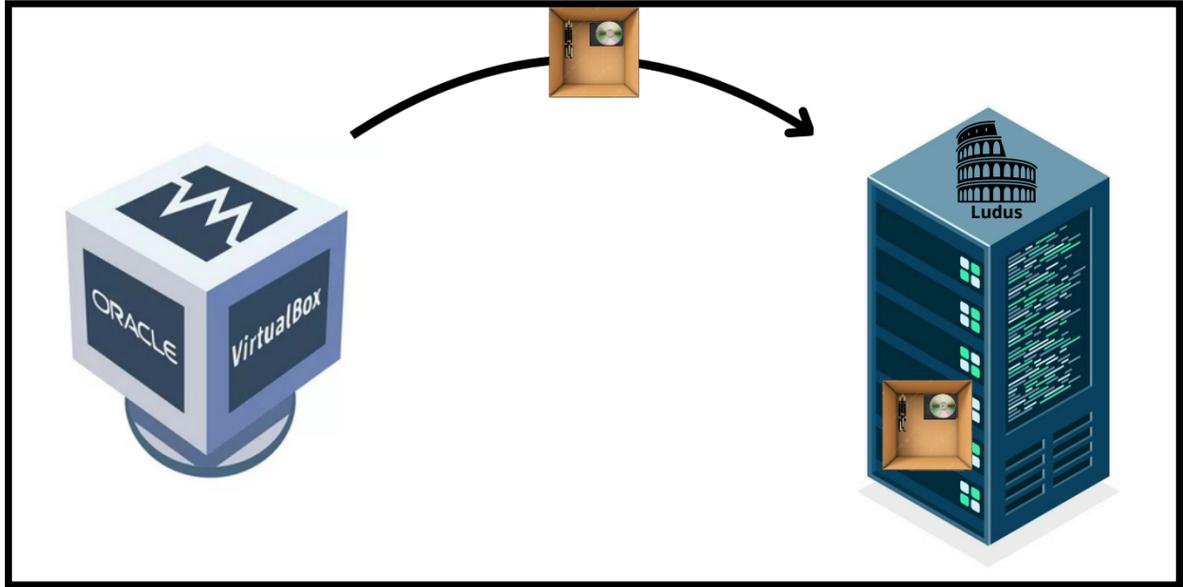


II - Existing Situation, Tasks & Difficulties

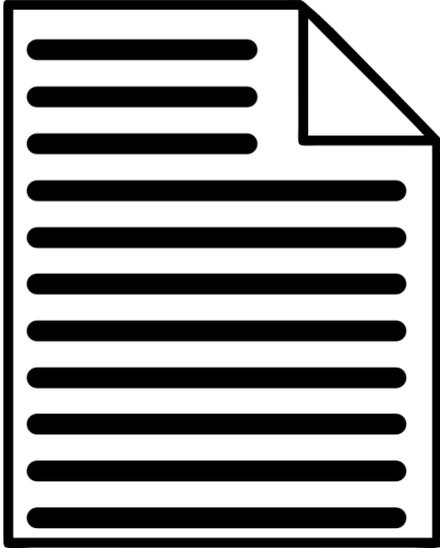
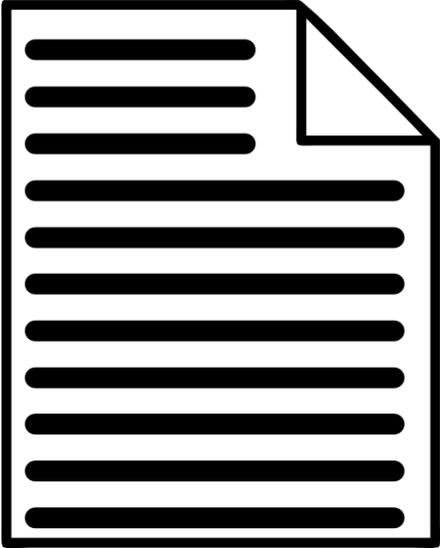
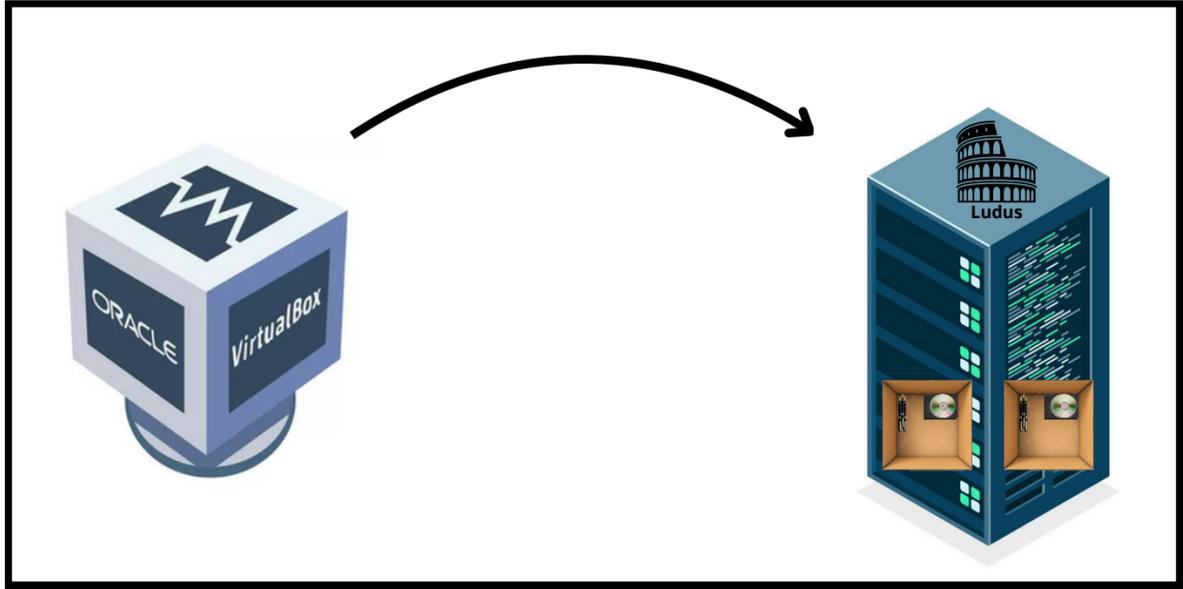
3 - Documenting the processes



II - Existing Situation, Tasks & Difficulties
3 - Documenting the processes

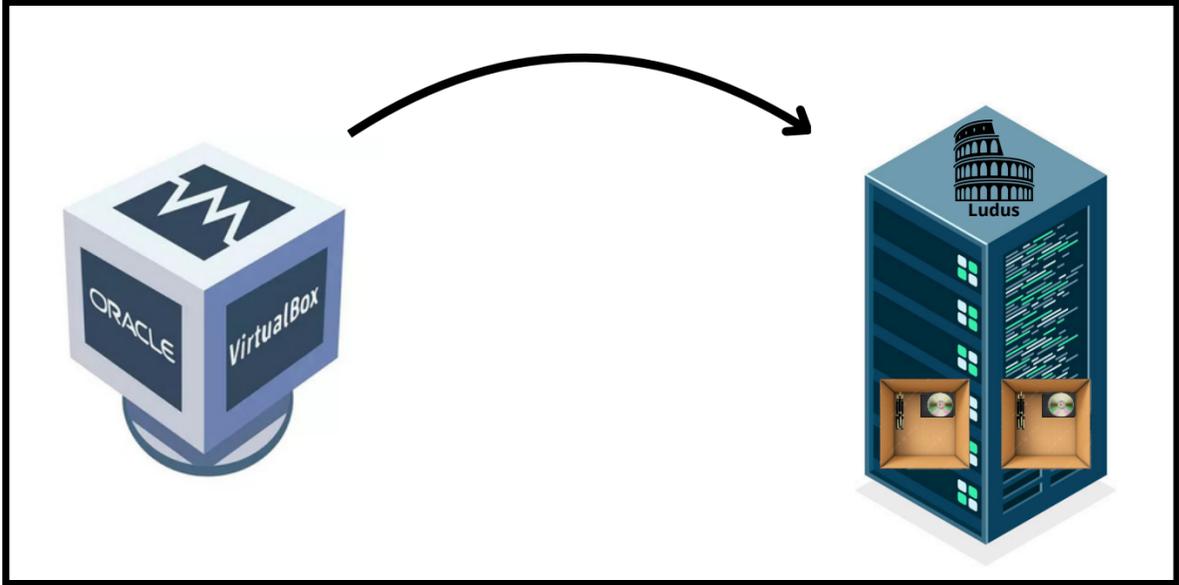


II - Existing Situation, Tasks & Difficulties
3 - Documenting the processes

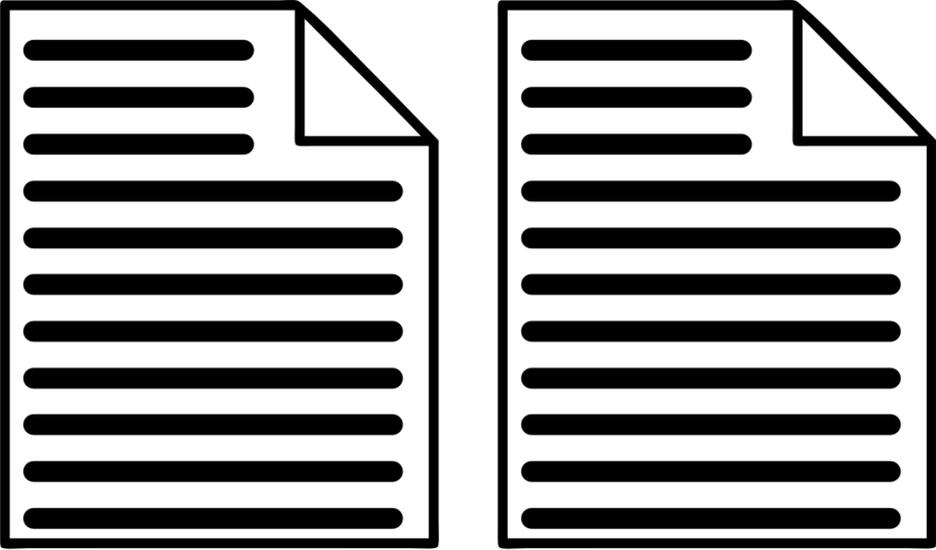


II - Existing Situation, Tasks & Difficulties

3 - Documenting the processes

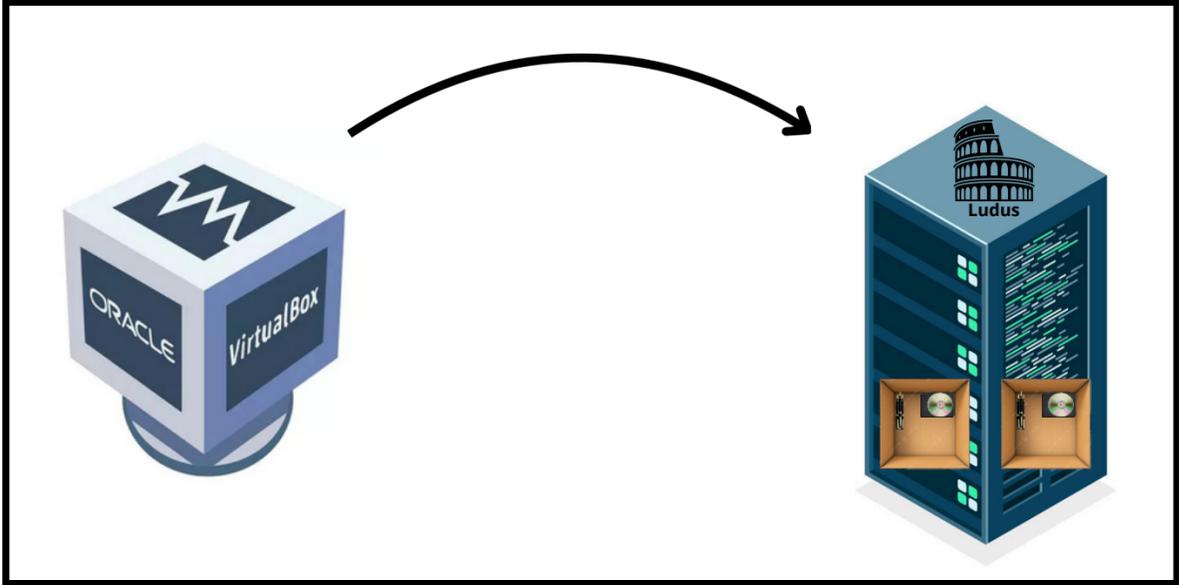


Anyone on the team could **easily replicate** what I had done



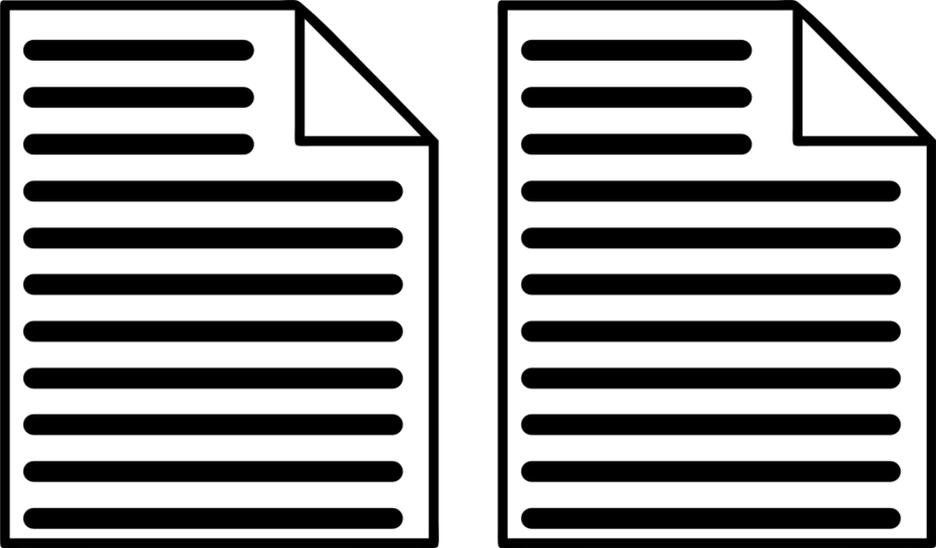
II - Existing Situation, Tasks & Difficulties

3 - Documenting the processes



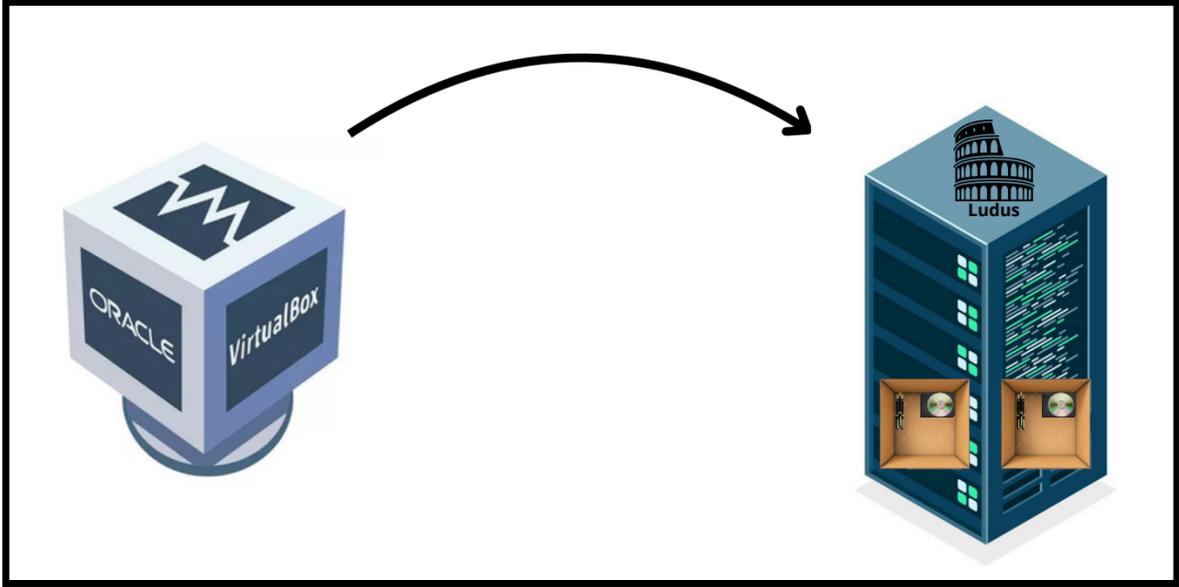
Anyone on the team could **easily replicate** what I had done

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



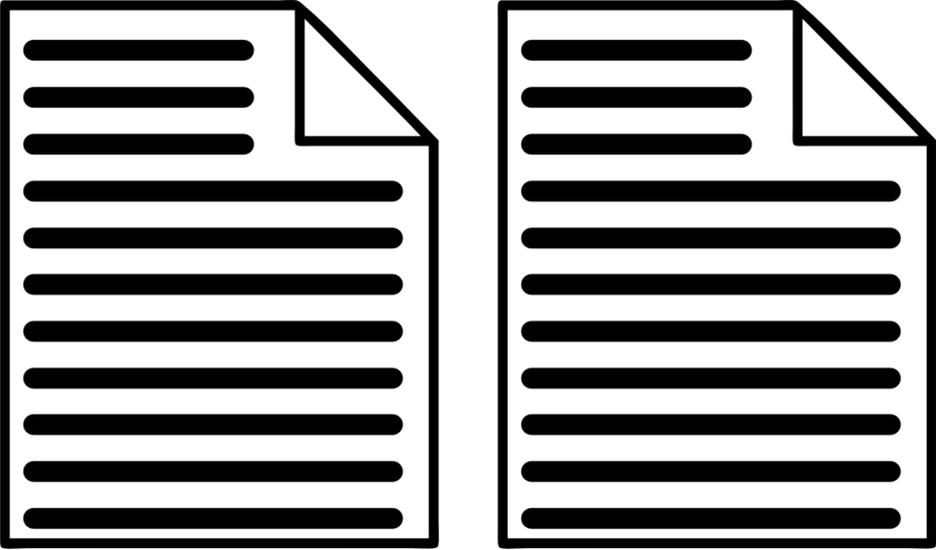
II - Existing Situation, Tasks & Difficulties

3 - Documenting the processes



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**



II - Existing Situation, Tasks & Difficulties

- 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
- 2 - Deploying and managing the ranges
- 3 - Documenting the processes

Bonus - Others

II - Existing Situation, Tasks & Difficulties
Bonus - Others



Backdoors & Breaches

II - Existing Situation, Tasks & Difficulties

Bonus - Others



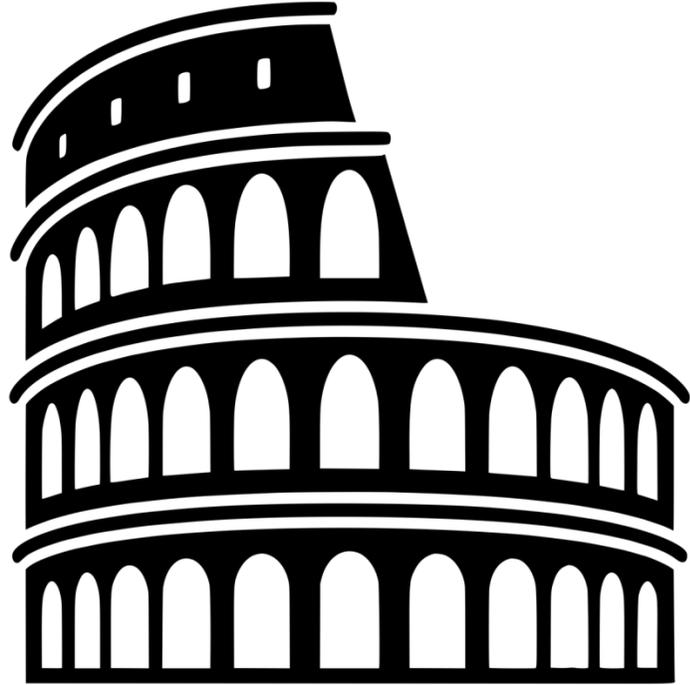
- 
- I - Host Organization & Problematic
 - II - Existing Situation, Tasks & Difficulties
 - III - Tools, Gantt Planning & Personal Organization
 - IV - The 3 main projects
 - V - Current VS Initial situation, Technical & Human Assessment

III - Tools, Gantt Planning & Personal Organization

- 1 - Tools and programming languages
- 2 - Gantt diagram
- 3 - Personal Organisation

III - Tools, Gantt Planning & Personal Organization

1 - Tools and programming languages

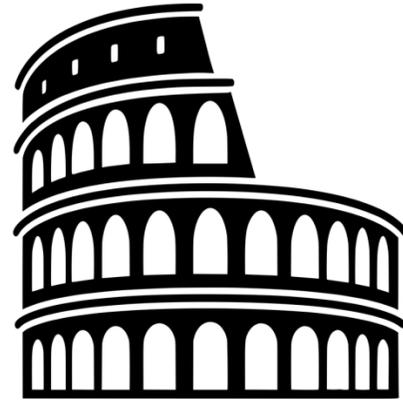


Cyber range
management and
deployment

Ludus

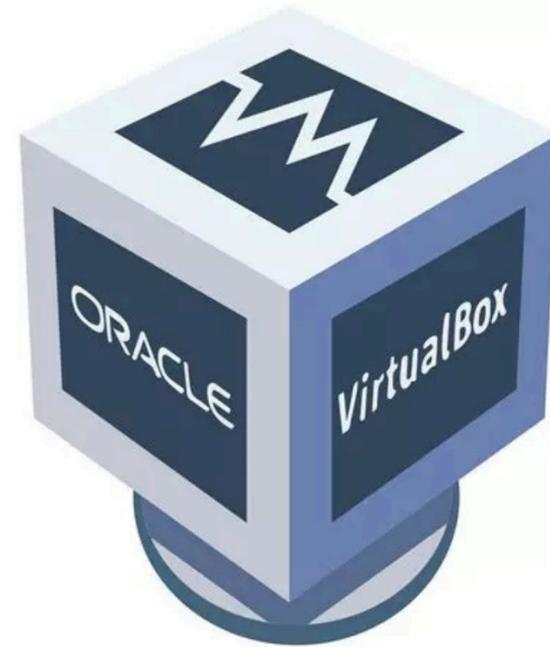
III - Tools, Gantt Planning & Personal Organization

1 - Tools and programming languages



Ludus

Cyber range
man
depl

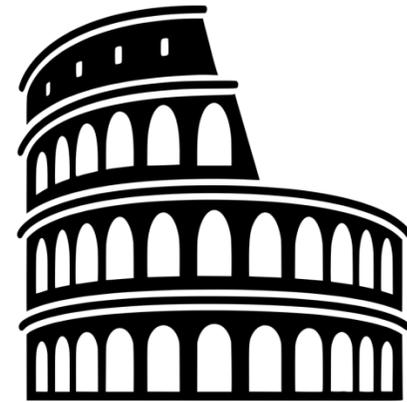


Local virtual
machine
management and
simulation

VirtualBox

III - Tools, Gantt Planning & Personal Organization

1 - Tools and programming languages



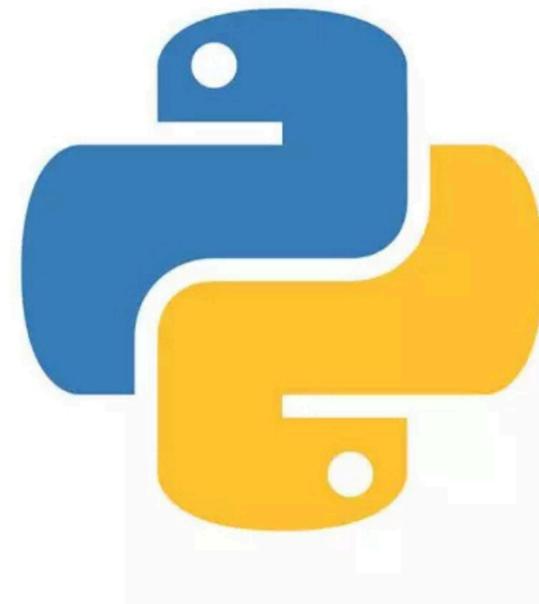
Ludus

Cyber range

man
depl



Local virtual

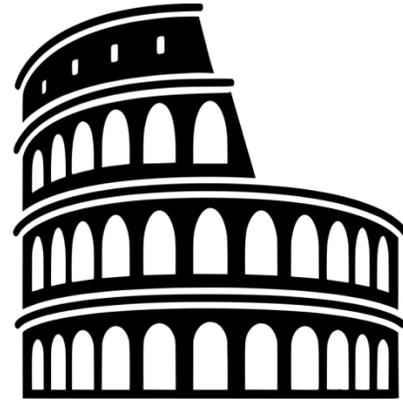


Very easy and complete programming language used in most projects

Python

III - Tools, Gantt Planning & Personal Organization

1 - Tools and programming languages



Ludus

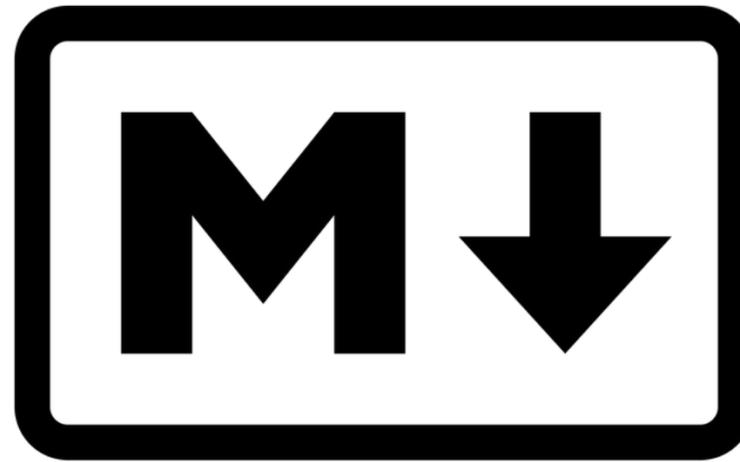
Cyber range
man
depl



Local virtual



Very easy and complete programming language used in most projects

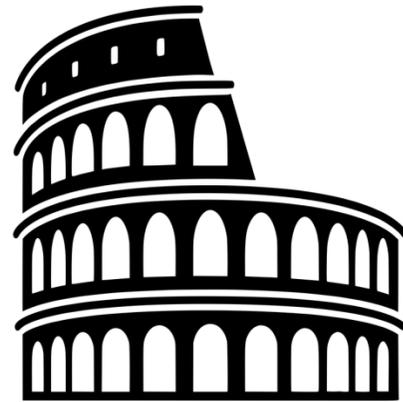


Format documentation before converting into Sphinx

Markdown

III - Tools, Gantt Planning & Personal Organization

1 - Tools and programming languages



Ludus



Markdown

Cyber range
man
depl



Local virtual



Very easy and complete programming language used in most projects



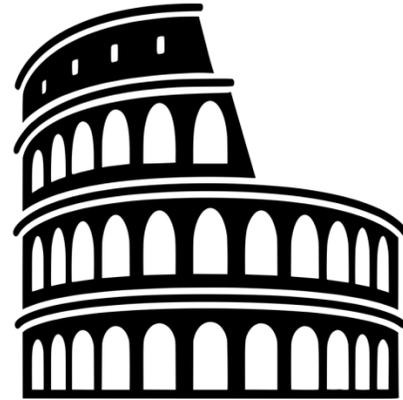
Internal Communication

Teams

F
d
b
c
Sphinx

III - Tools, Gantt Planning & Personal Organization

1 - Tools and programming languages



Ludus



Markdown

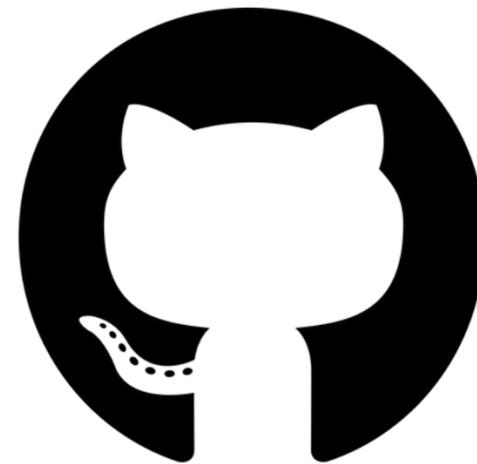
Cyber range
man
depl



Local virtual



Very easy and complete programming language used in most projects



GitHub

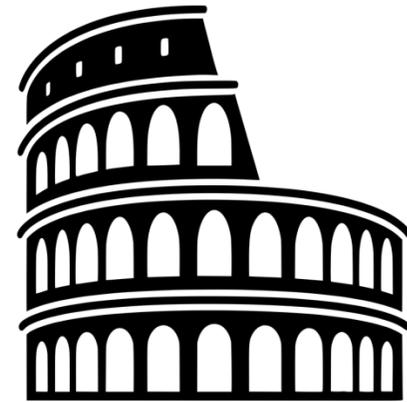
To save, keep track of and share my modifications to projects

F
d
b
c
Sphinx

Teams

III - Tools, Gantt Planning & Personal Organization

1 - Tools and programming languages



Ludus

Cyber range management and deployment



VirtualBox

Local virtual machine management and simulation



Python

Very easy and complete programming language used in most projects



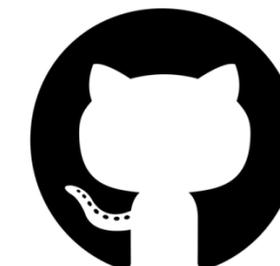
Markdown

Format documentation before converting into Sphinx



Teams

Internal Communication

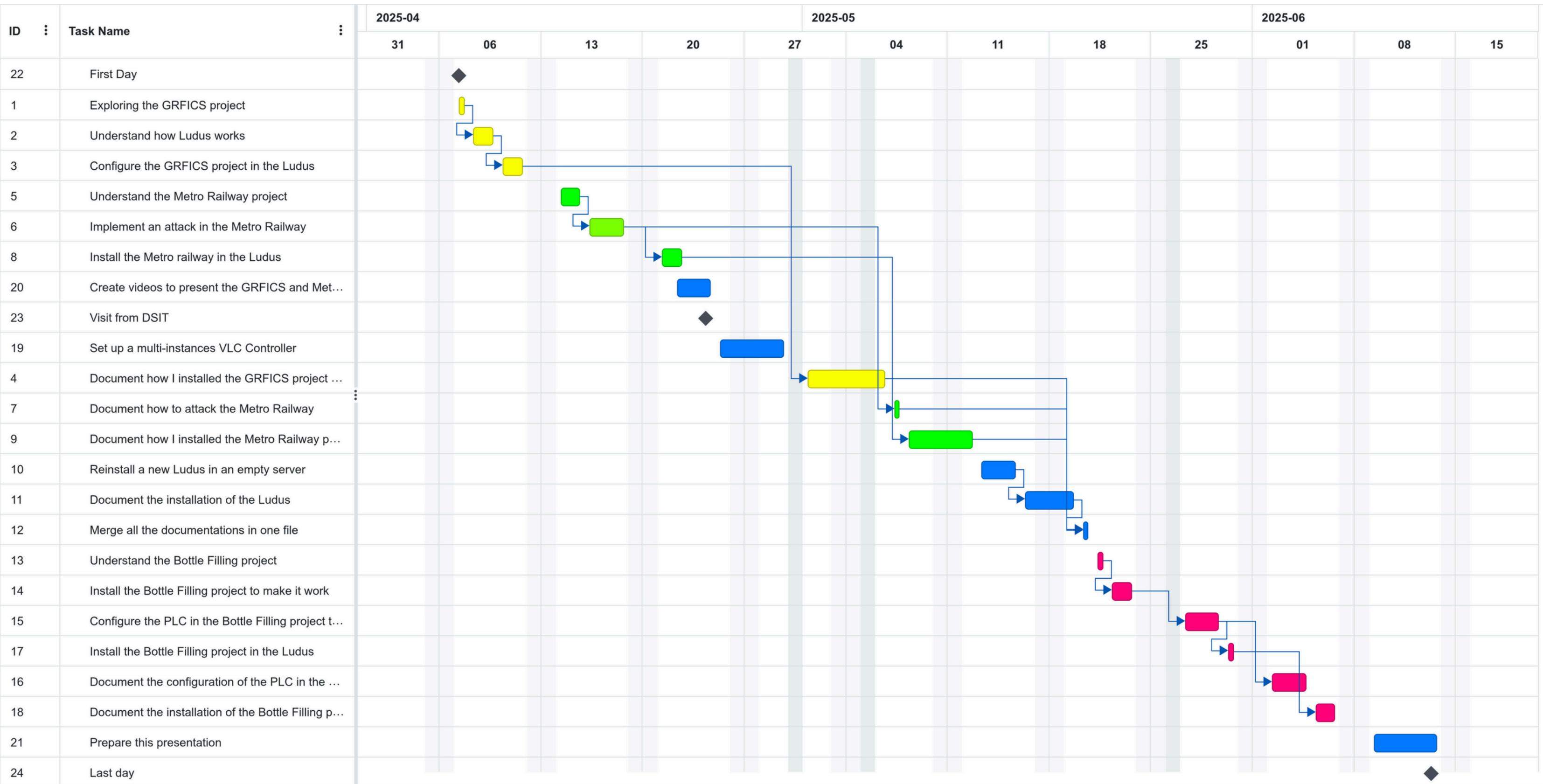


Github

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



III - Tools, Gantt Planning & Personal Organization

- 1 - Tools and programming languages
- 2 - Gantt diagram
- 3 - Personal Organisation

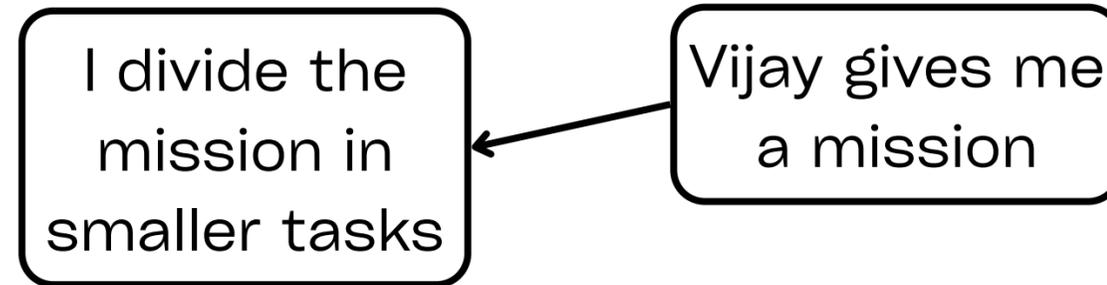
III - Tools, Gantt Planning & Personal Organization

3 - Personal Organisation

Vijay gives me
a mission

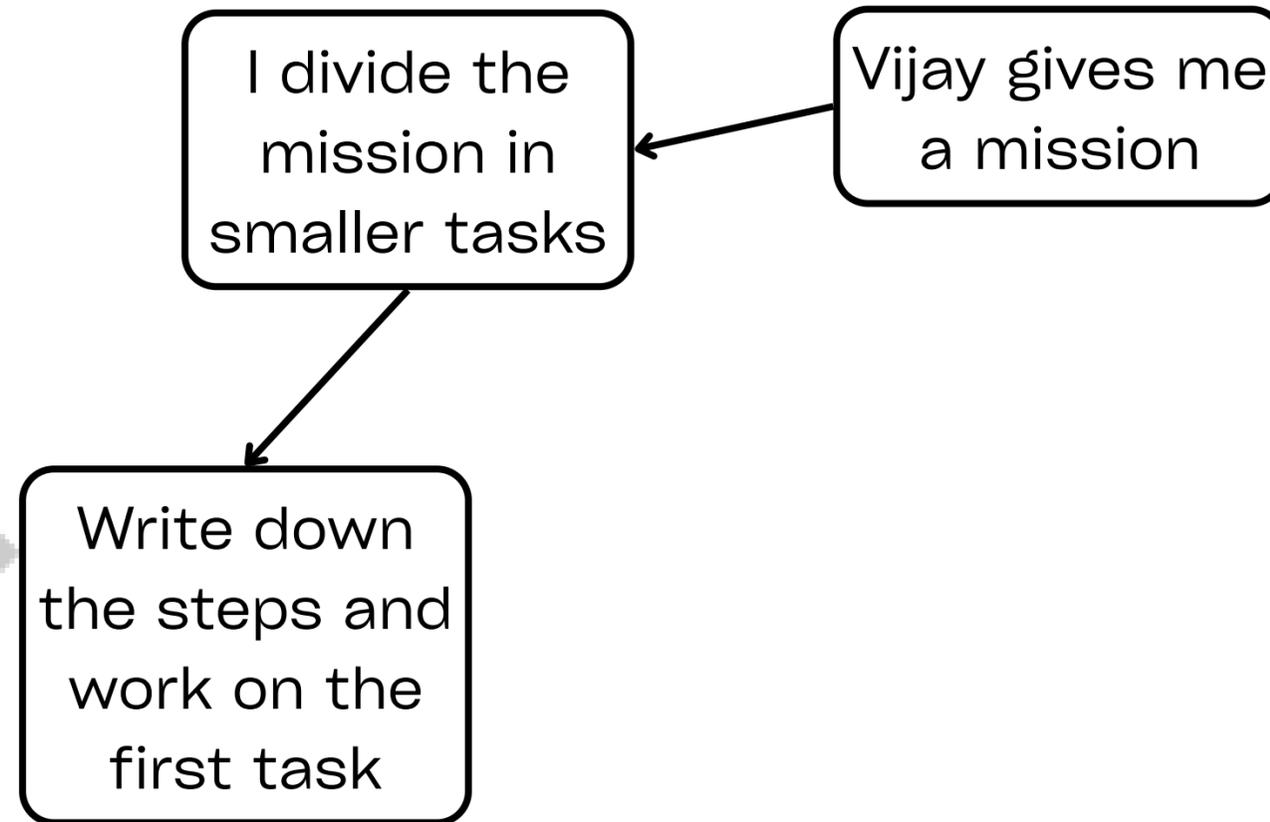
III - Tools, Gantt Planning & Personal Organization

3 - Personal Organisation



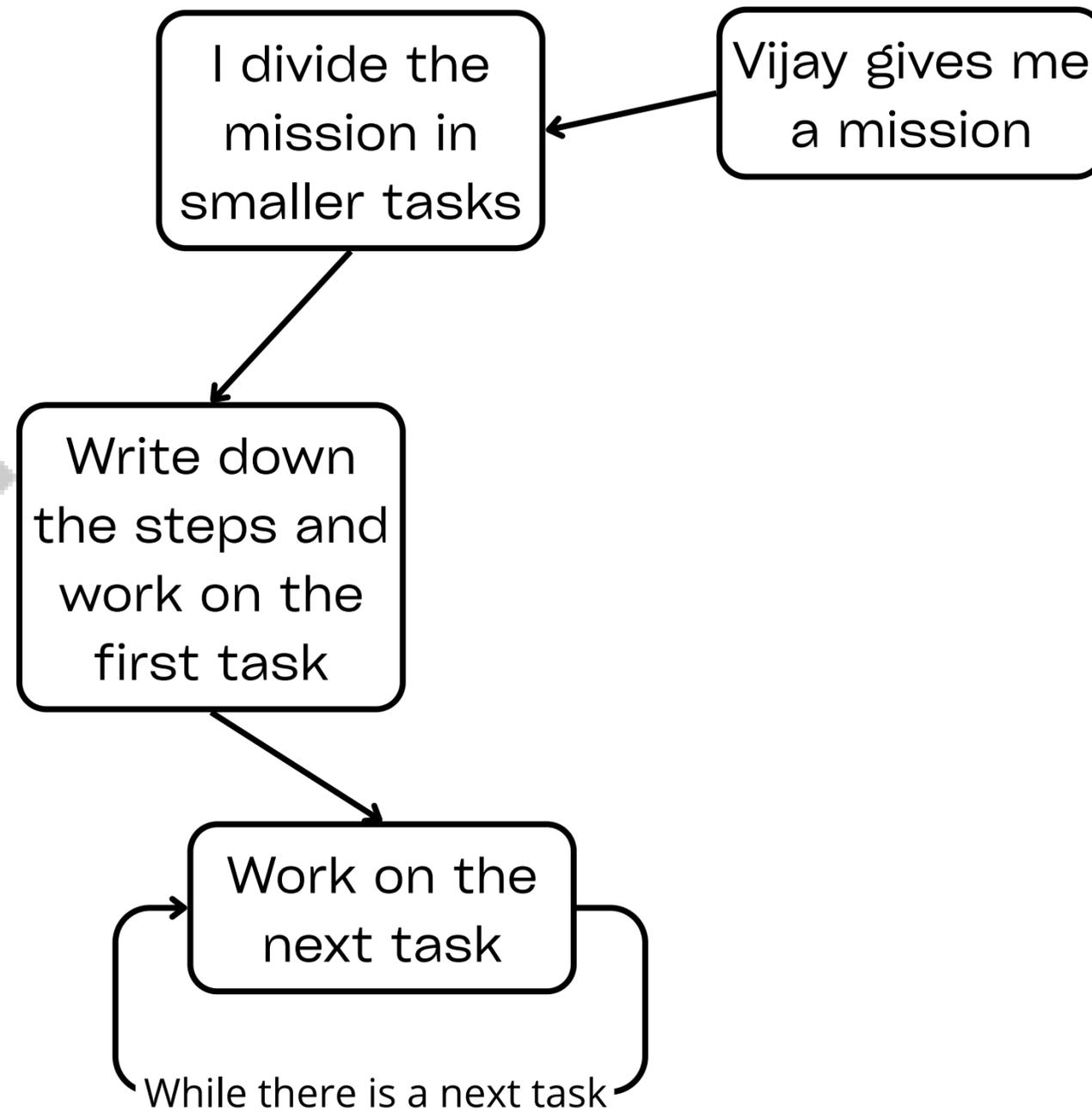
III - Tools, Gantt Planning & Personal Organization

3 - Personal Organisation



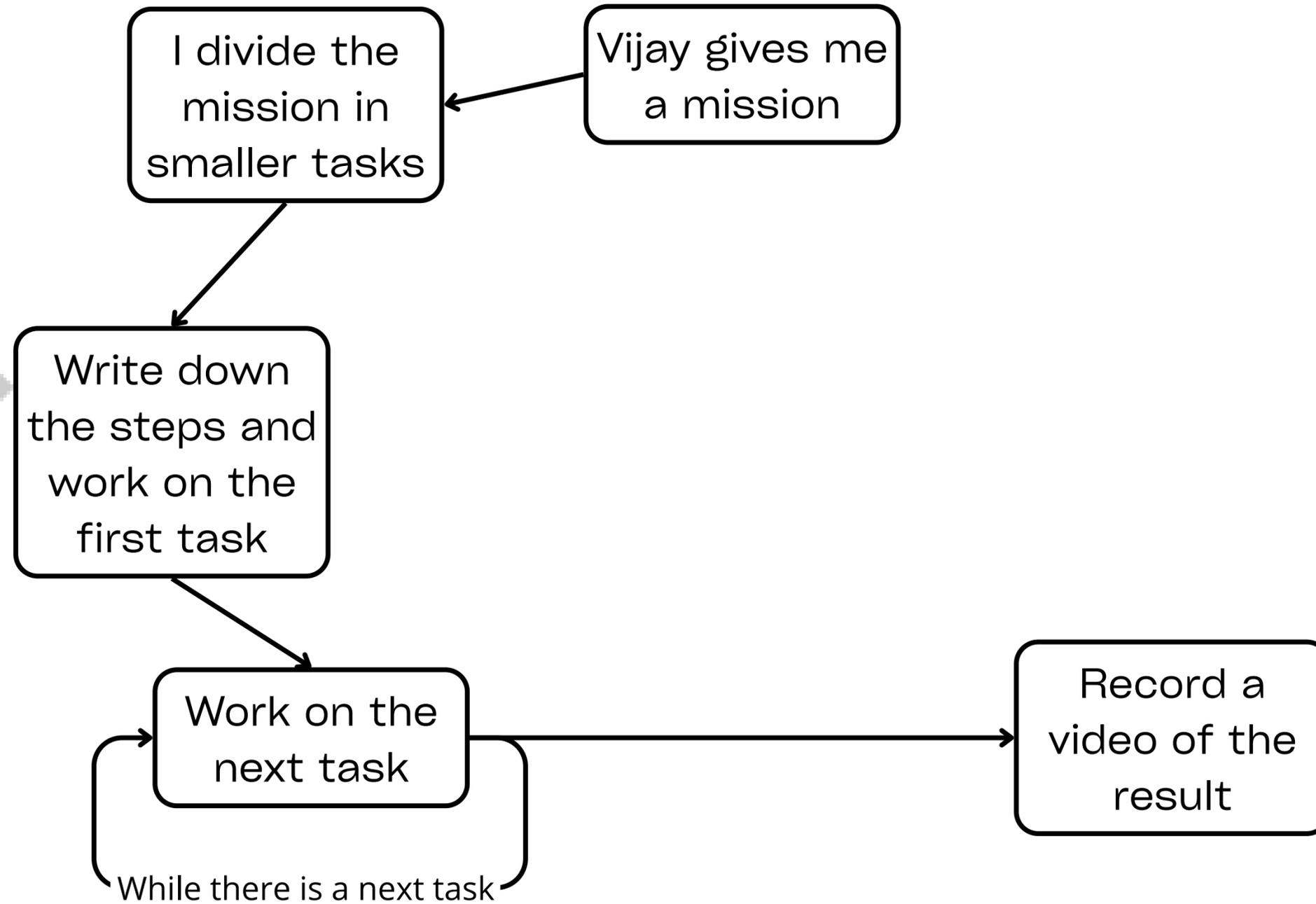
III - Tools, Gantt Planning & Personal Organization

3 - Personal Organisation



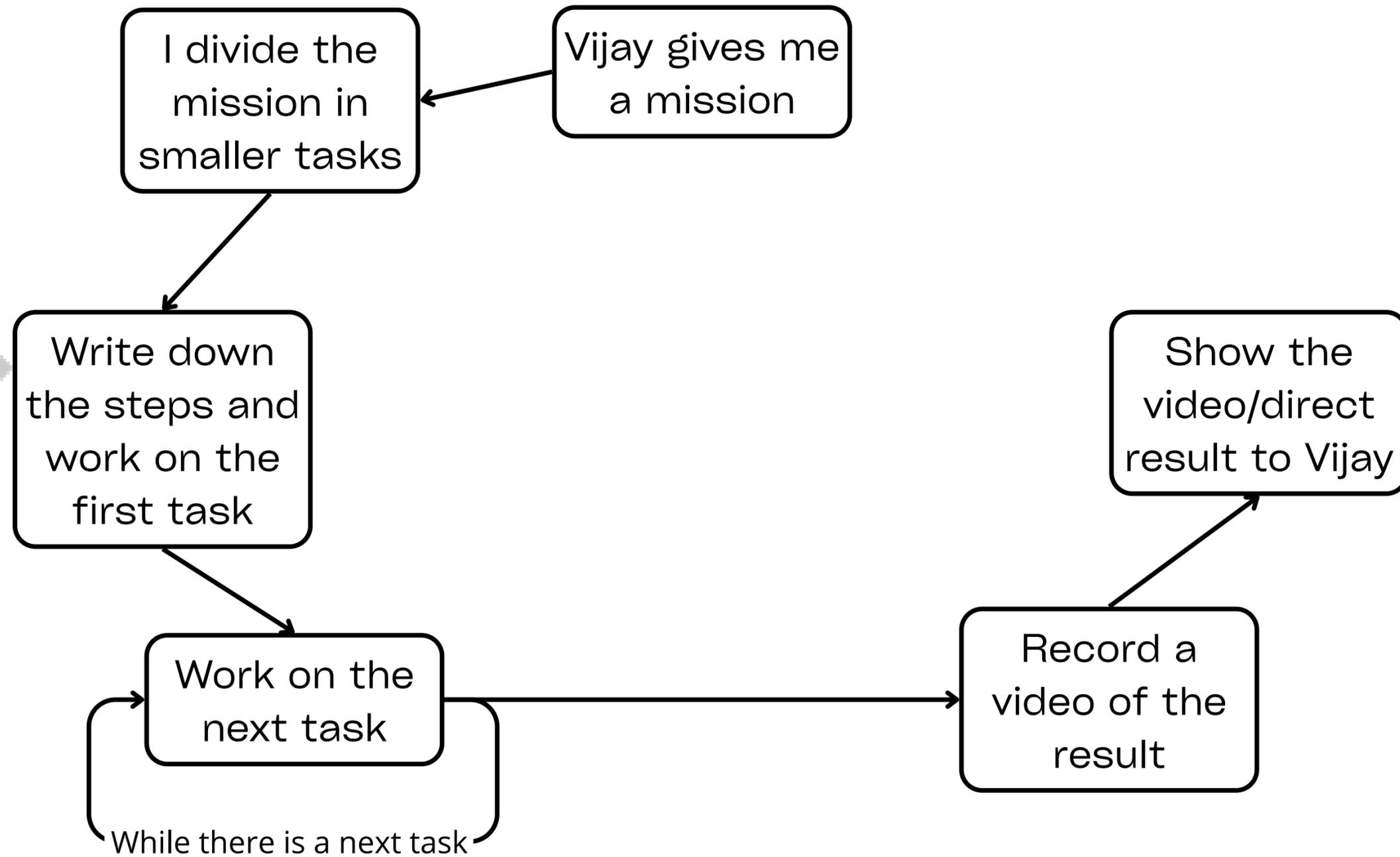
III - Tools, Gantt Planning & Personal Organization

3 - Personal Organisation



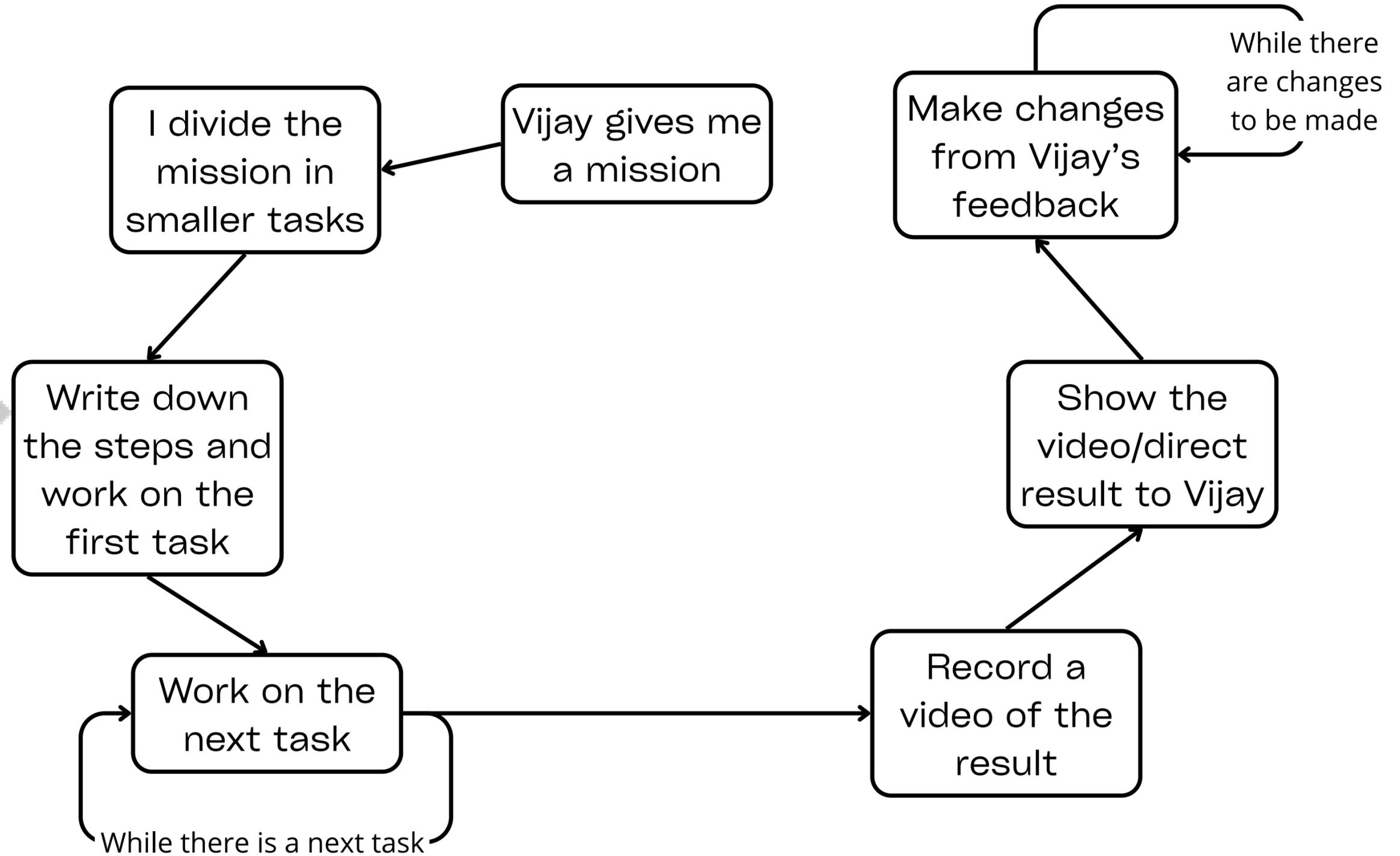
III - Tools, Gantt Planning & Personal Organization

3 - Personal Organisation



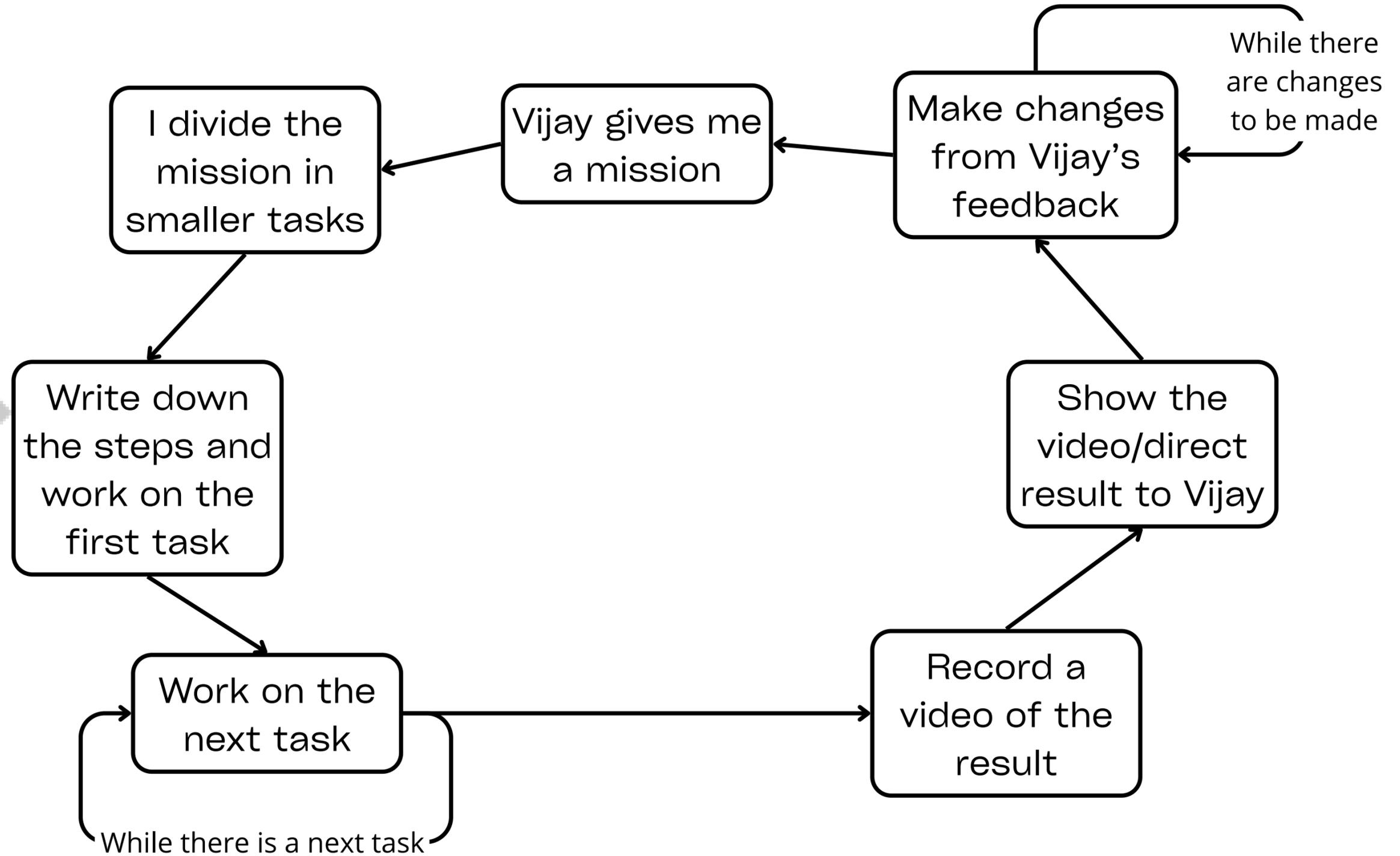
III - Tools, Gantt Planning & Personal Organization

3 - Personal Organisation



III - Tools, Gantt Planning & Personal Organization

3 - Personal Organisation



- 
- 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)



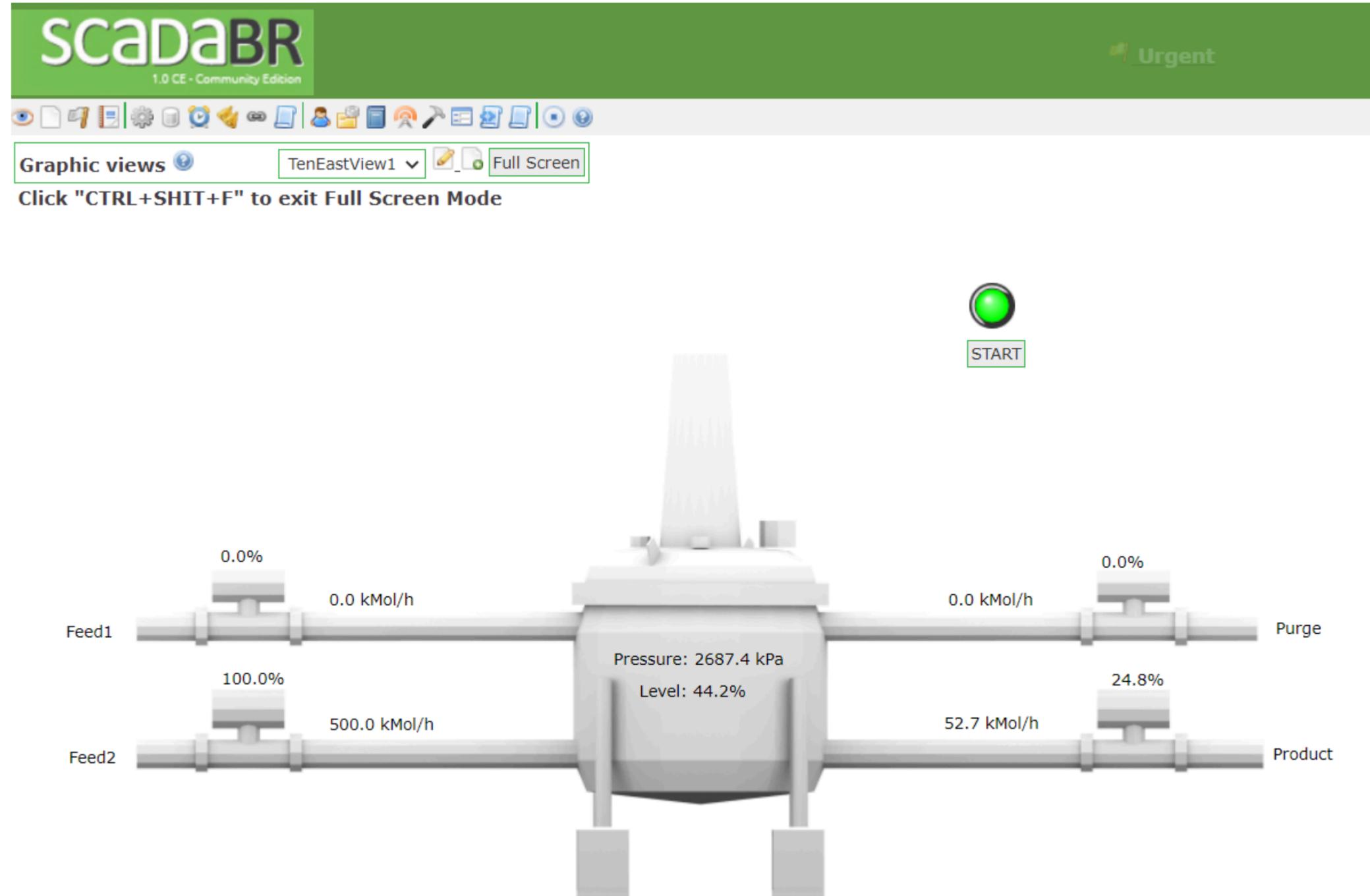
IV - The 3 main projects

1 - GRFICS (Chemical Plant)



IV - The 3 main projects

1 - GRFICS (Chemical Plant)



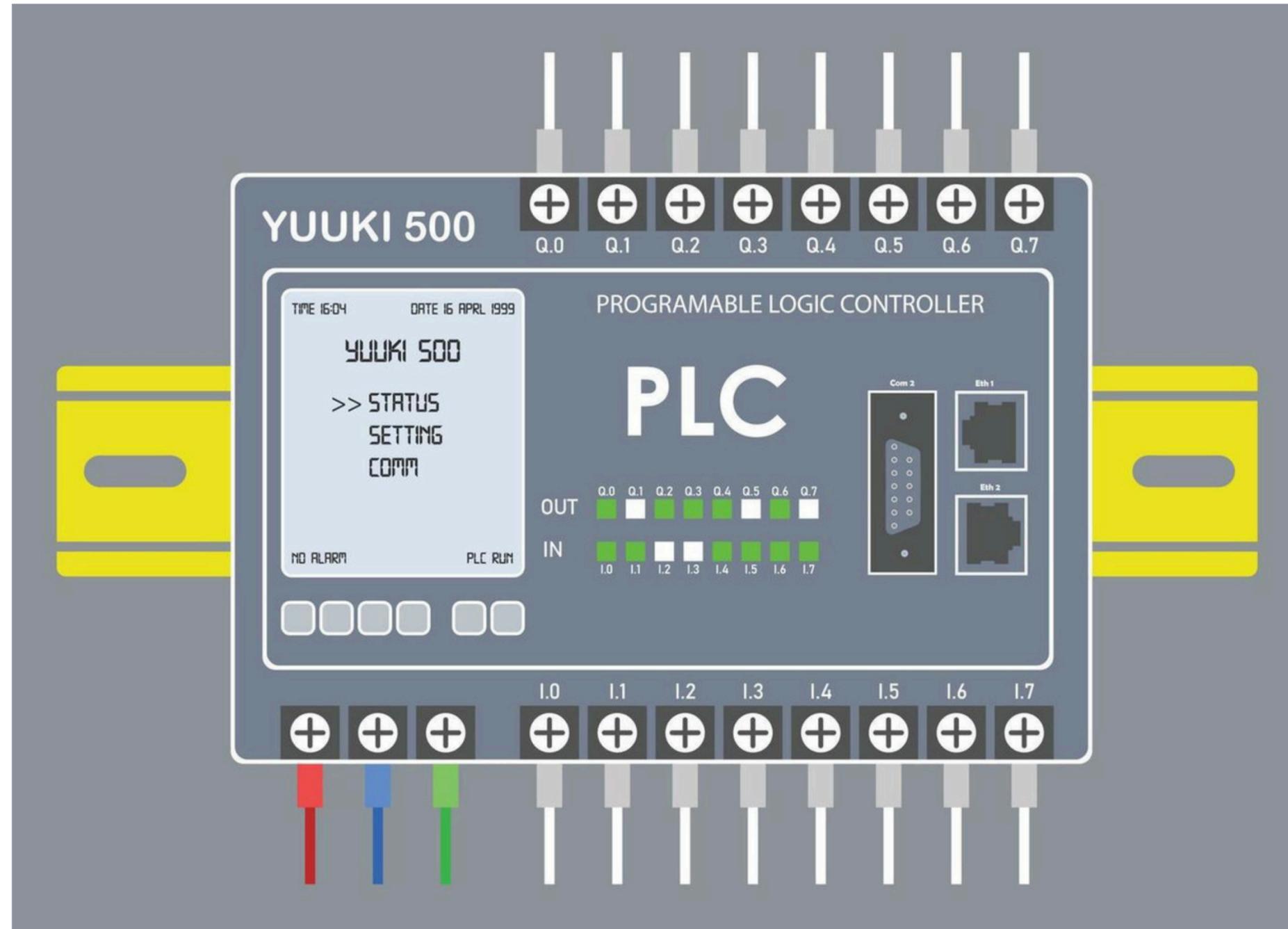
IV - The 3 main projects

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)



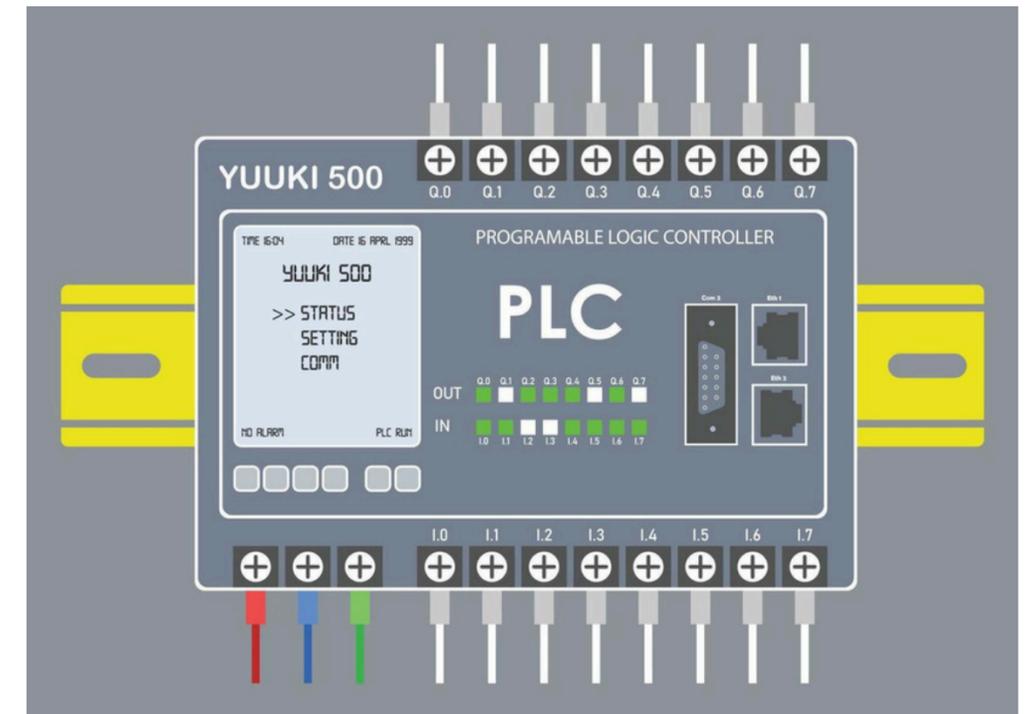
IV - The 3 main projects

1 - GRFICS (Chemical Plant)



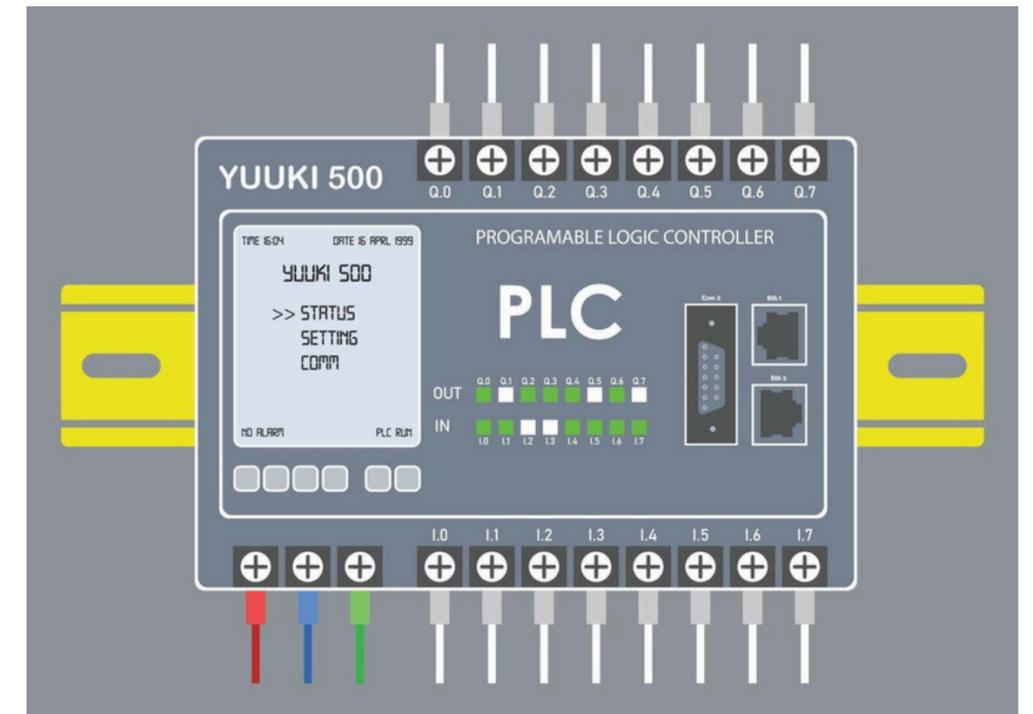
IV - The 3 main projects

1 - GRFICS (Chemical Plant)



IV - The 3 main projects

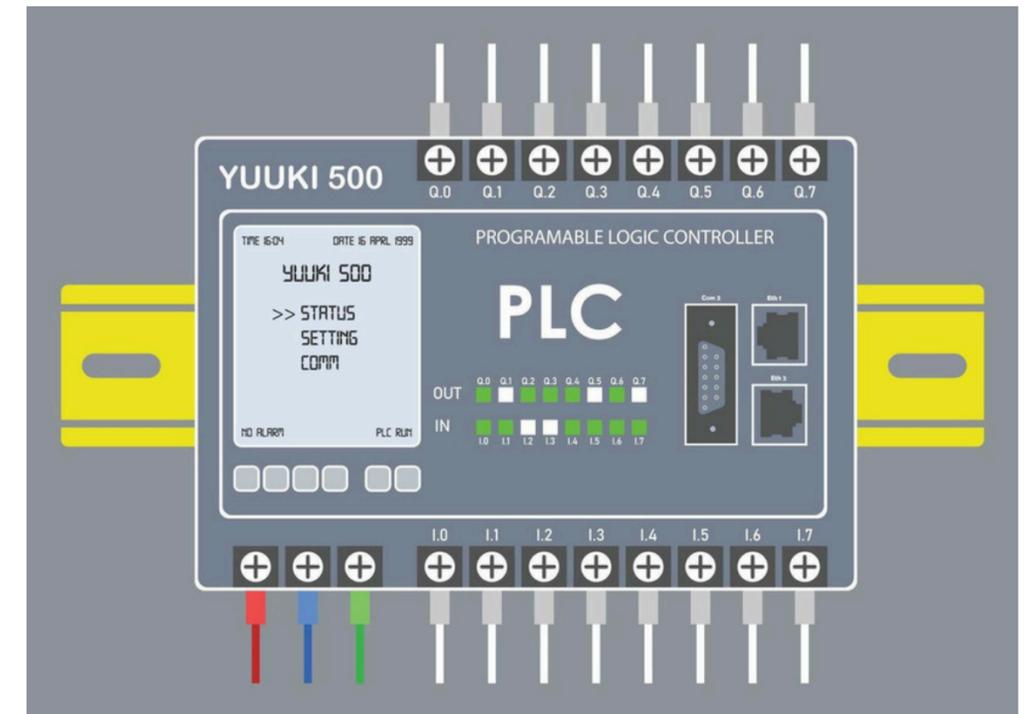
1 - GRFICS (Chemical Plant)



Pressure

IV - The 3 main projects

1 - GRFICS (Chemical Plant)

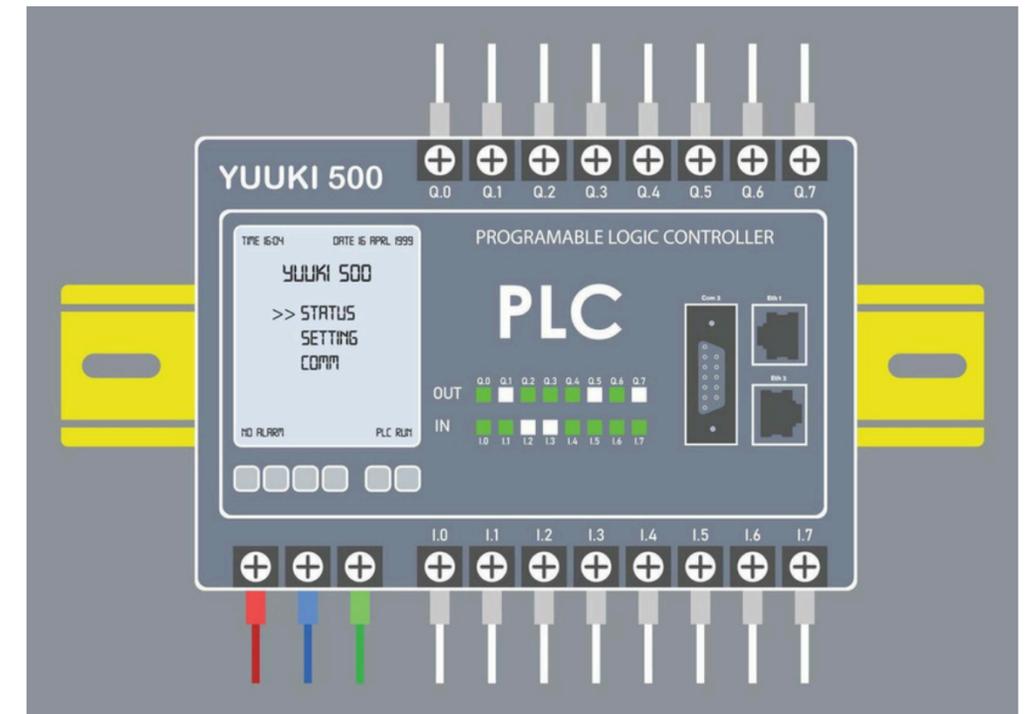


Pressure

Level

IV - The 3 main projects

1 - GRFICS (Chemical Plant)



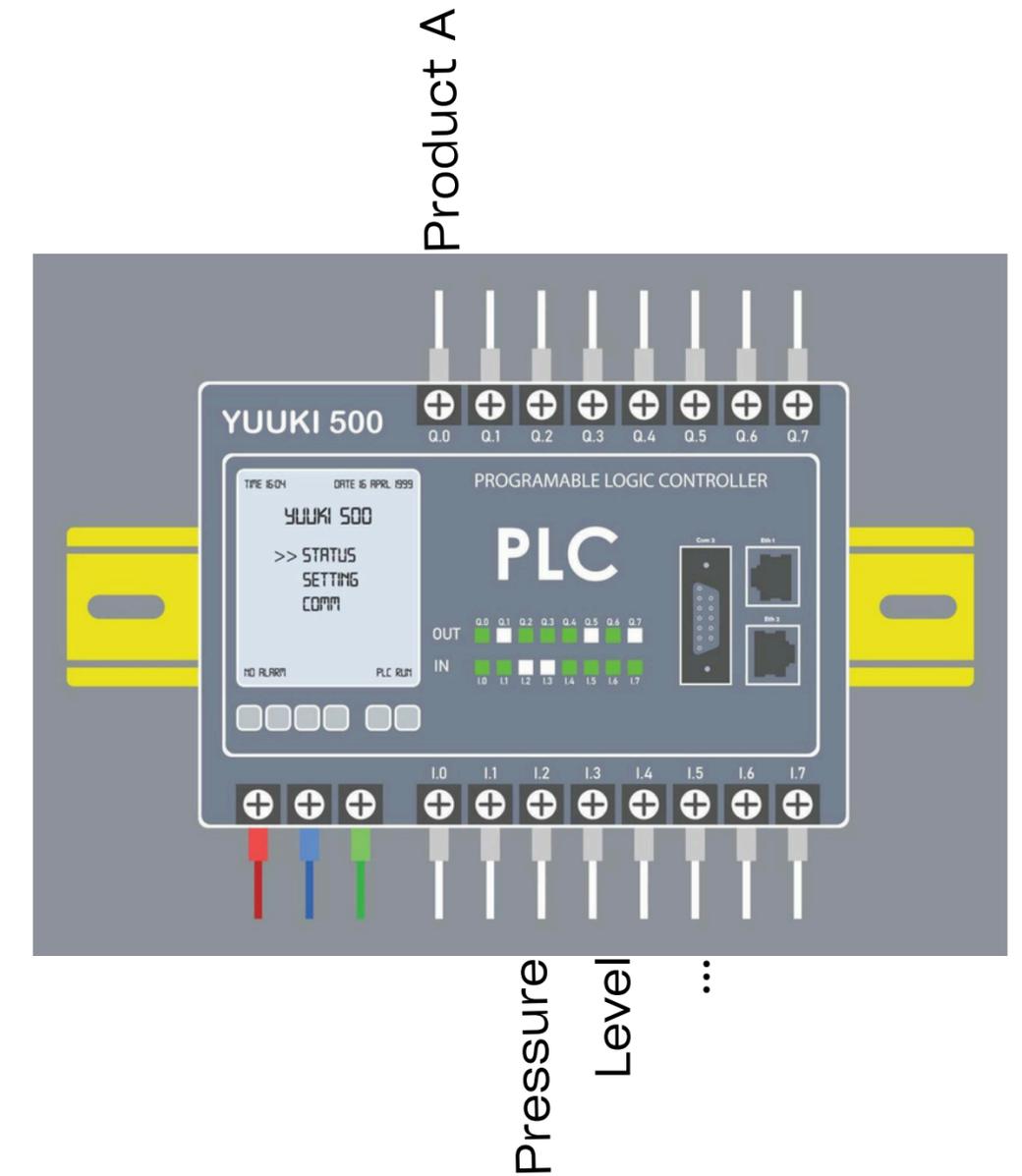
Pressure

Level

...

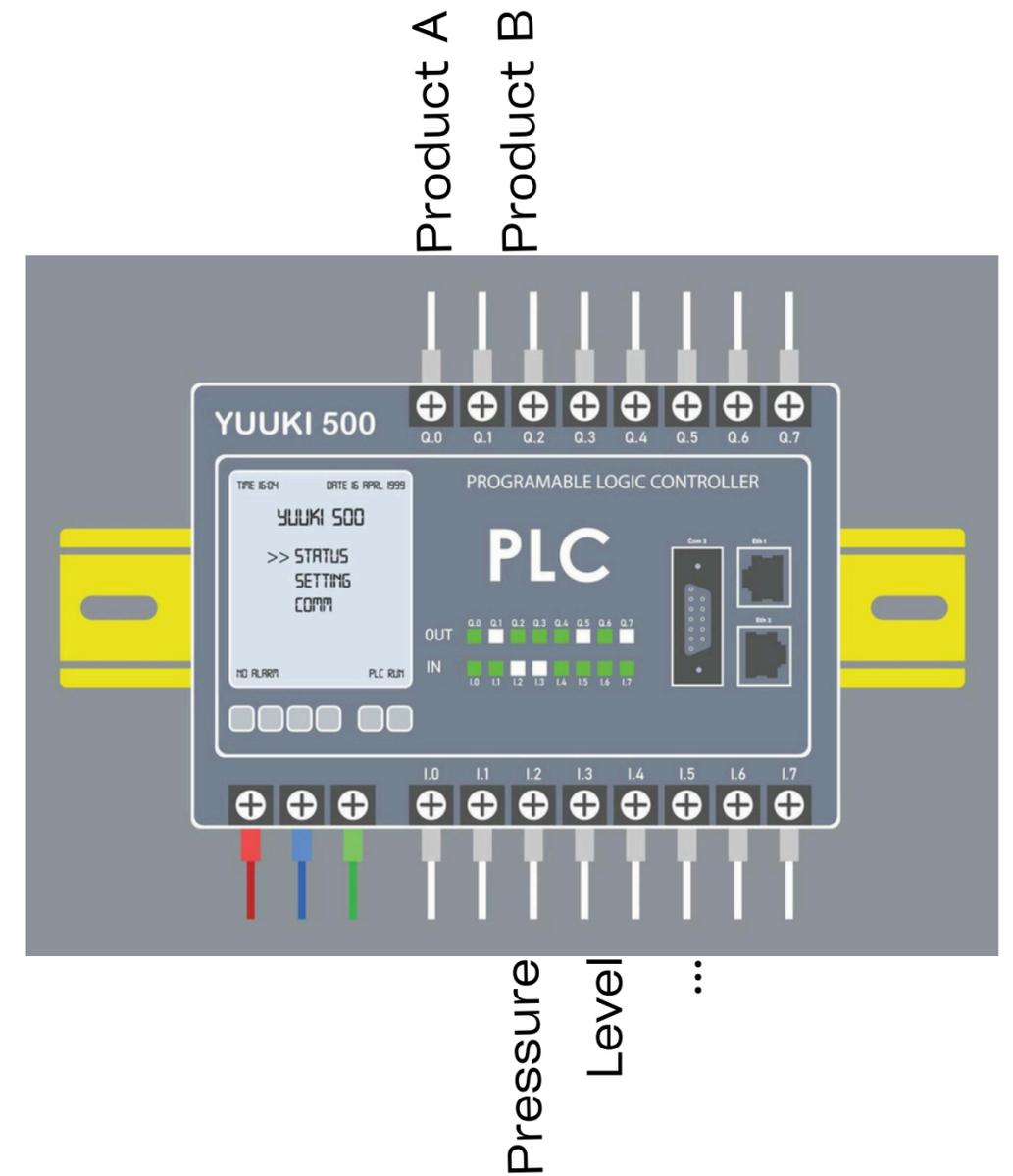
IV - The 3 main projects

1 - GRFICS (Chemical Plant)



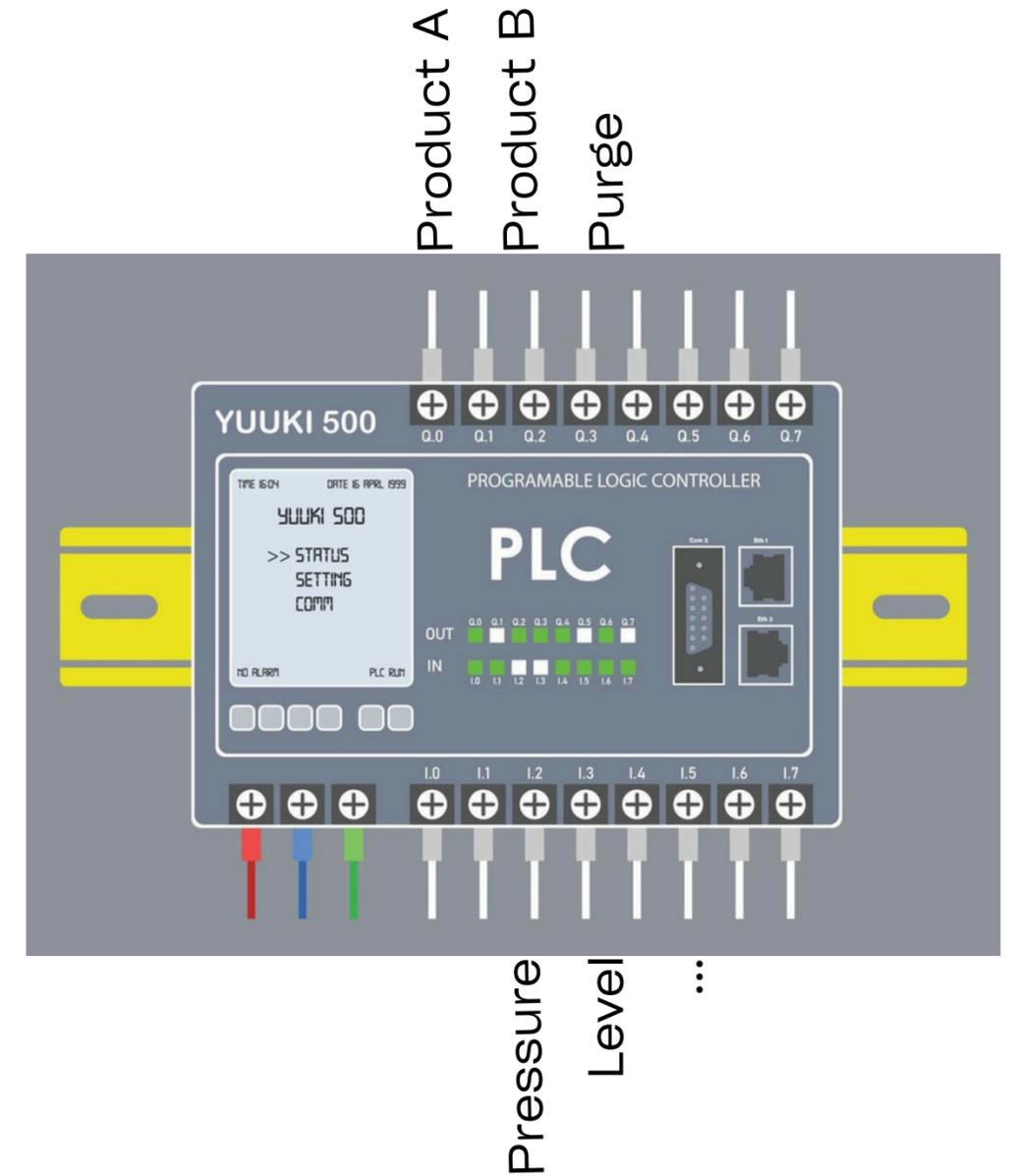
IV - The 3 main projects

1 - GRFICS (Chemical Plant)



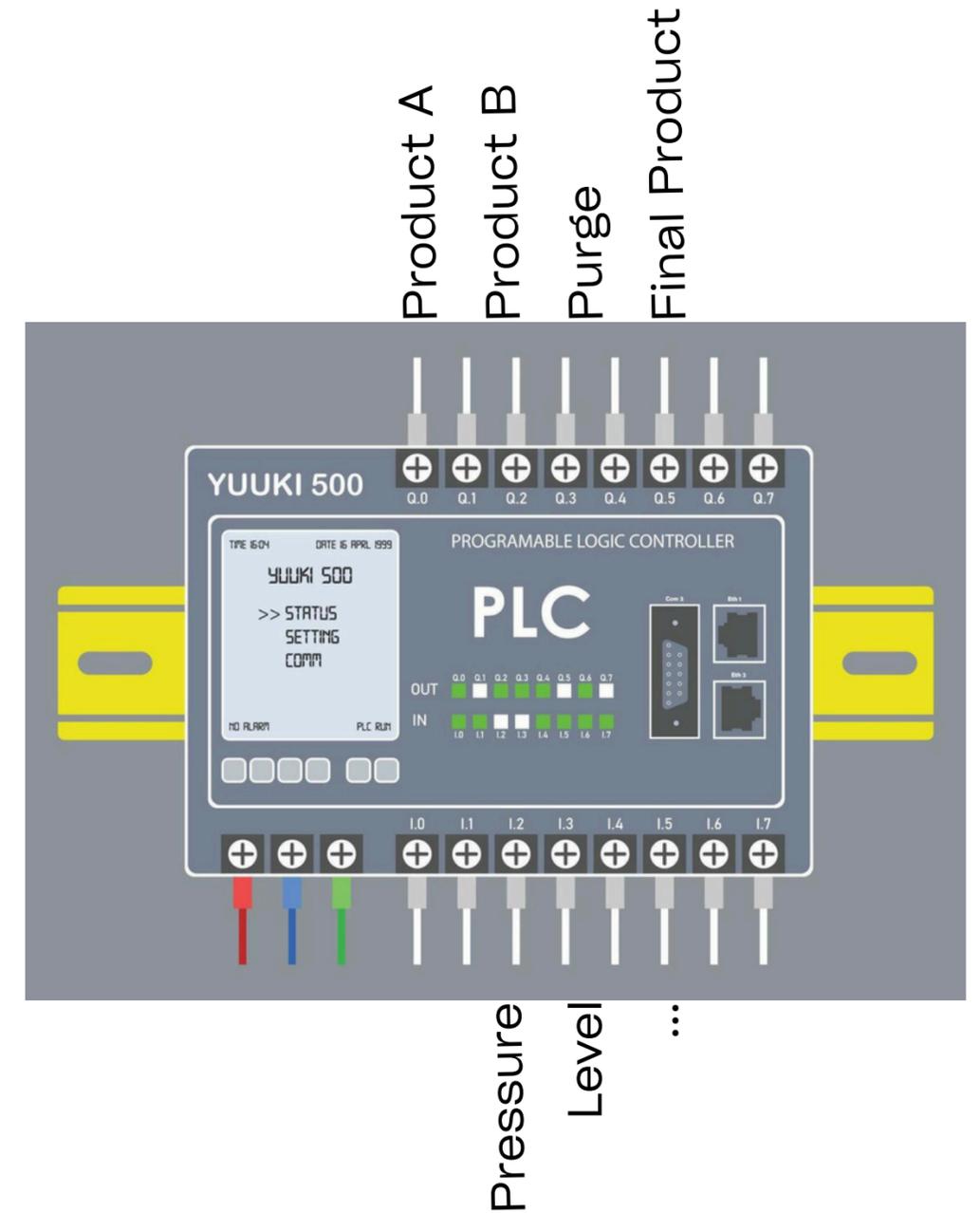
IV - The 3 main projects

1 - GRFICS (Chemical Plant)



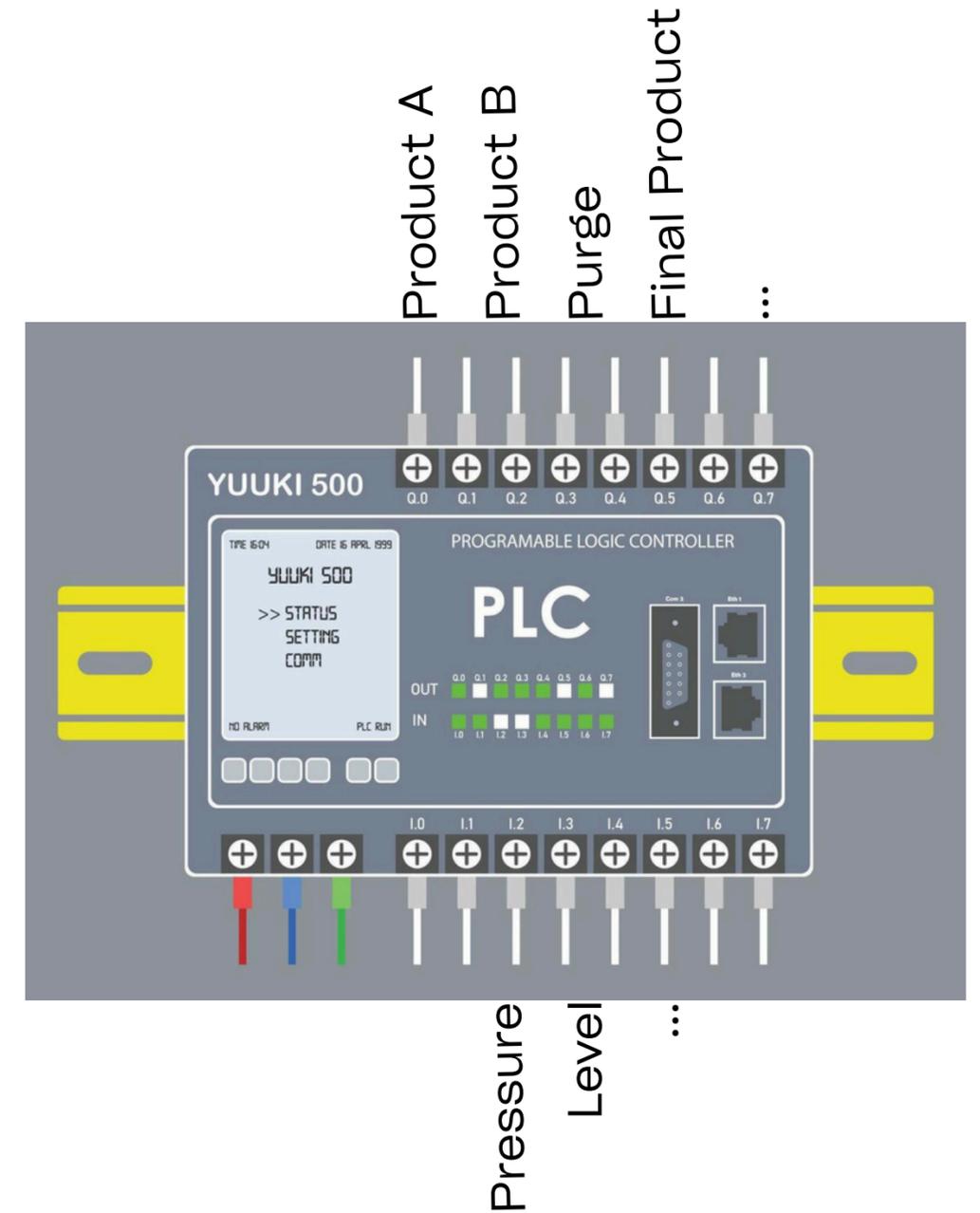
IV - The 3 main projects

1 - GRFICS (Chemical Plant)



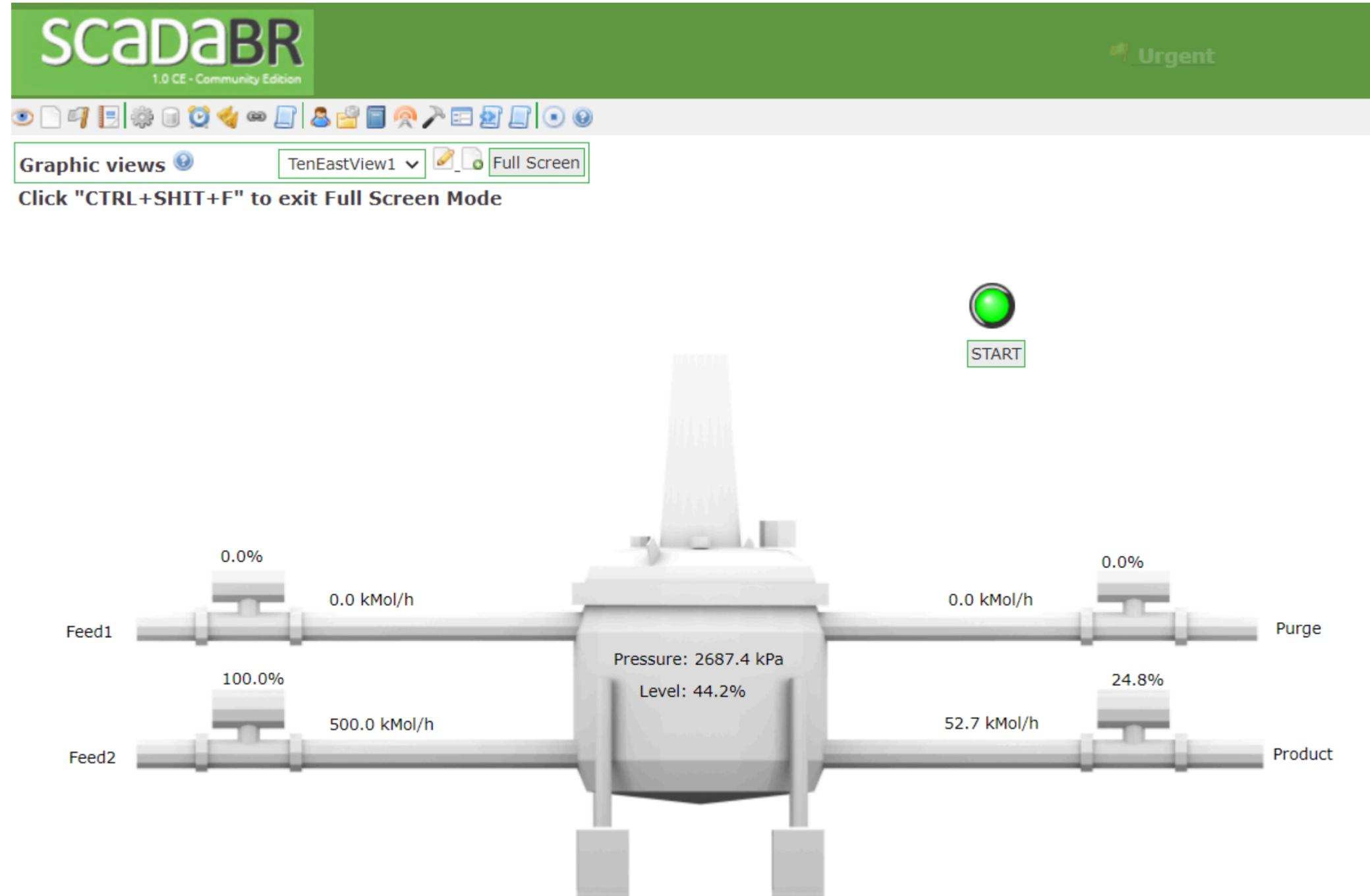
IV - The 3 main projects

1 - GRFICS (Chemical Plant)



IV - The 3 main projects

1 - GRFICS (Chemical Plant)



IV - The 3 main projects

1 - GRFICS (Chemical Plant)

My work:



IV - The 3 main projects

1 - GRFICS (Chemical Plant)

My work:

- Understand the project



IV - The 3 main projects

1 - GRFICS (Chemical Plant)

My work:

- Understand the project
- Install it



IV - The 3 main projects

1 - GRFICS (Chemical Plant)

My work:

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



IV - The 3 main projects

1 - GRFICS (Chemical Plant)

My work:

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

IV - The 3 main projects

1 - GRFICS (Chemical Plant)

My work:

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

IV - The 3 main projects

1 - GRFICS (Chemical Plant)

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)

Fortiphyl / GRFICSv2

Code Issues 8 Pull requests Discussions Actions Projects Security Insights

GRFICSv2 Public Watch 29 Fork 100 Star 510

master 2 Branches 0 Tags

Go to file Add file Code

djformby Merge pull request #11 from Thus0/patch-simulation 7e77a6c · 2 years ago 94 Commits

figures	add screenshots of sim and hmi	5 years ago
hmi_vm	fix formatting	5 years ago
pfsense_vm	Updated Documentation	5 years ago
plc_vm	Add execution permissions to building scripts in PLC's Docke...	4 years ago
simulation_vm	Merge pull request #11 from Thus0/patch-simulation	2 years ago
workstation_vm	add comment about gateway	5 years ago
LICENSE	Create License	5 years ago
README.md	Boot order for the VMs	4 years ago

README GPL-3.0 license

GRFICSv2

Version 2 of the Graphical Realism Framework for Industrial Control Simulation (GRFICS)

Overview

This version of GRFICS is organized as 5 VirtualBox VMs (a 3D simulation, a soft PLC, an HMI, a pfsense firewall, and a workstation) communicating with each other on host-only virtual networks. For a more detailed explanation of the entire framework and some background information on ICS networks, please refer to the workshop paper located at <https://www.usenix.org/conference/ase18/presentation/formby>

A video series walking through VM setup and example attacks is available on the Fortiphyl YouTube channel at <https://www.youtube.com/playlist?list=PL2RSrzaDx0R670yPIYPqM51guk3bQjFG5>

A commercial version of GRFICS with more scenarios, advanced features, and streamlined usability is being offered by

About

Version 2 of the Graphical Realism Framework for Industrial Control Simulation (GRFICS)

cybersecurity hmi industrial-automation ics-security plc-programming

Readme GPL-3.0 license Activity Custom properties 510 stars 29 watching 100 forks Report repository

Releases

No releases published

Packages

No packages published

Contributors

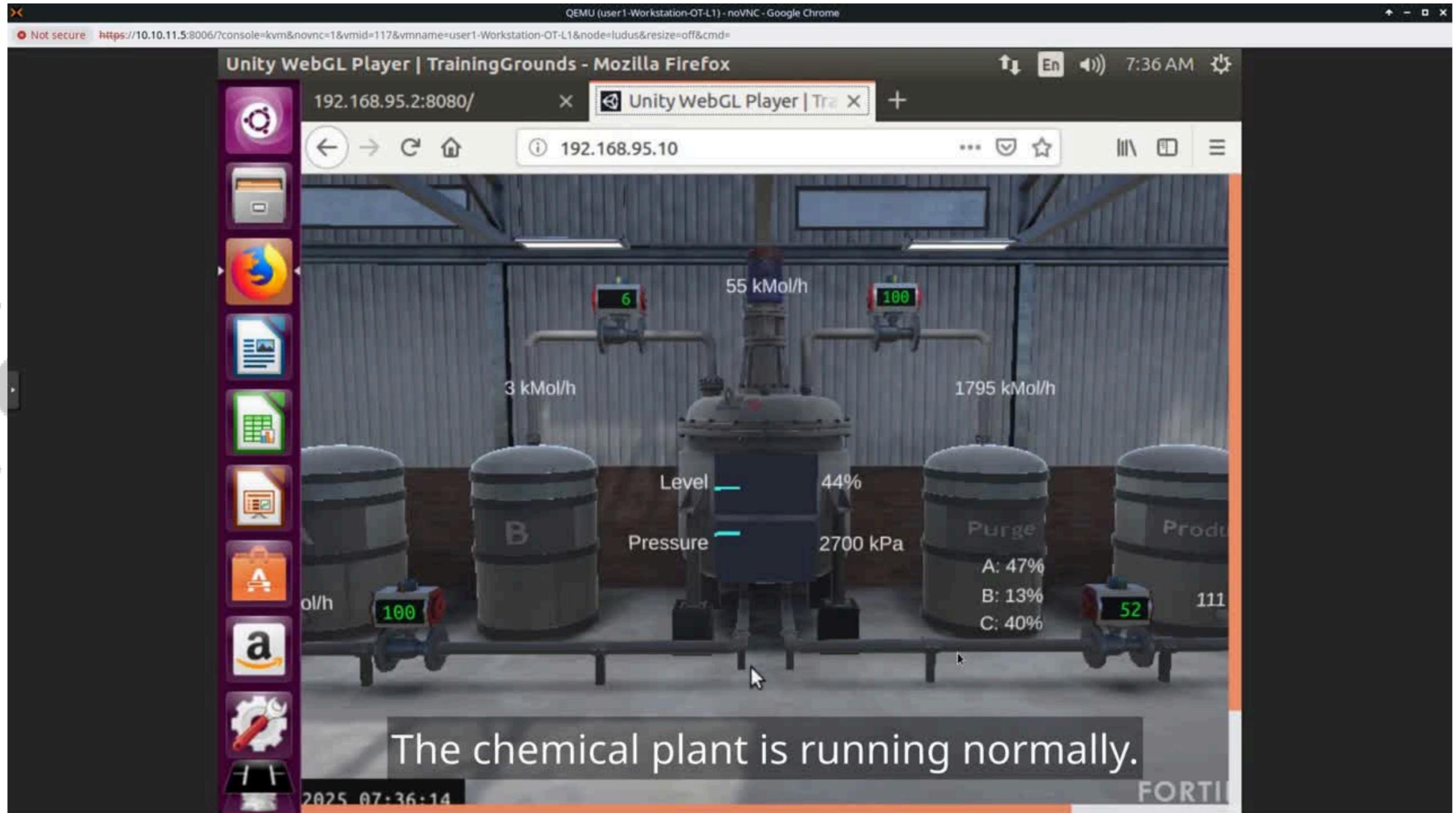
6

Languages

C++	54.3%	C	19.6%	Shell	10.3%
Yacc	10.3%	LLVM	2.3%	JavaScript	0.9%
Other	2.3%				

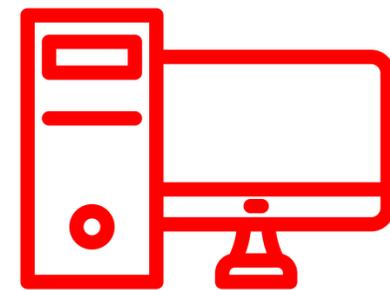
IV - The 3 main projects

1 - GRFICS (Chemical Plant)

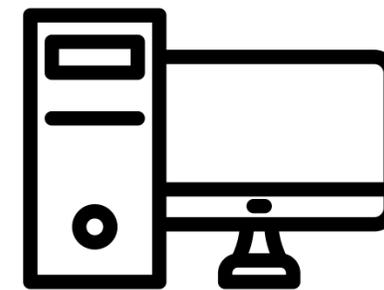


IV - The 3 main projects

1 - GRFICS (Chemical Plant)



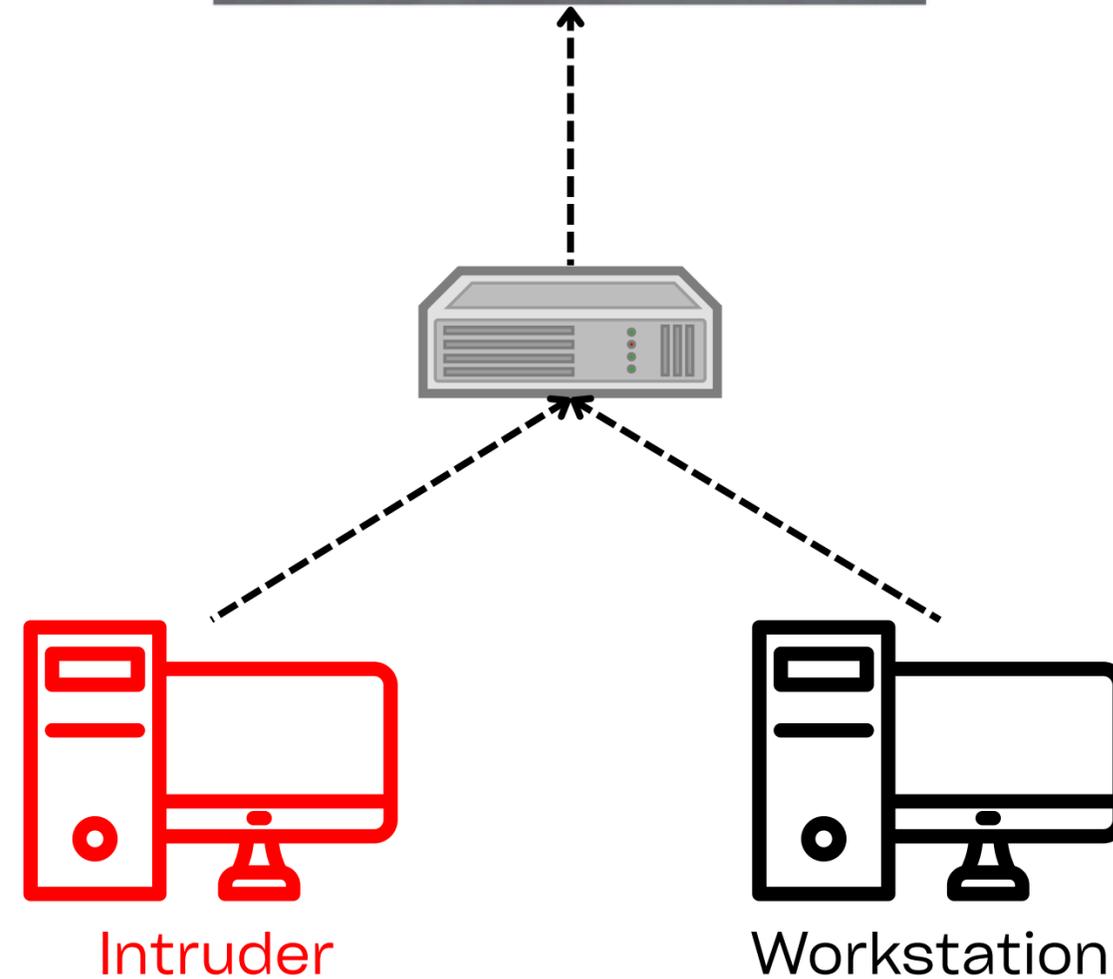
Intruder



Workstation

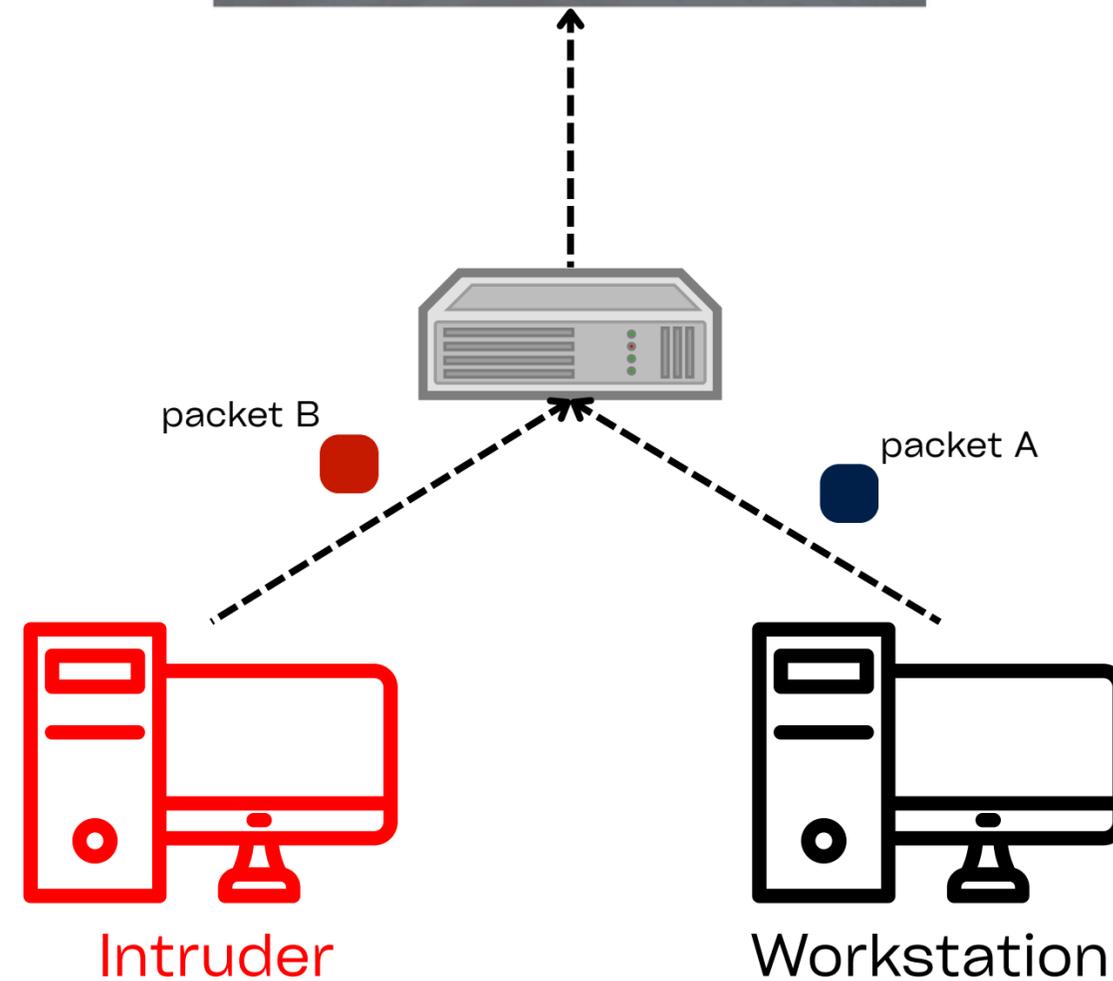
IV - The 3 main projects

1 - GRFICS (Chemical Plant)



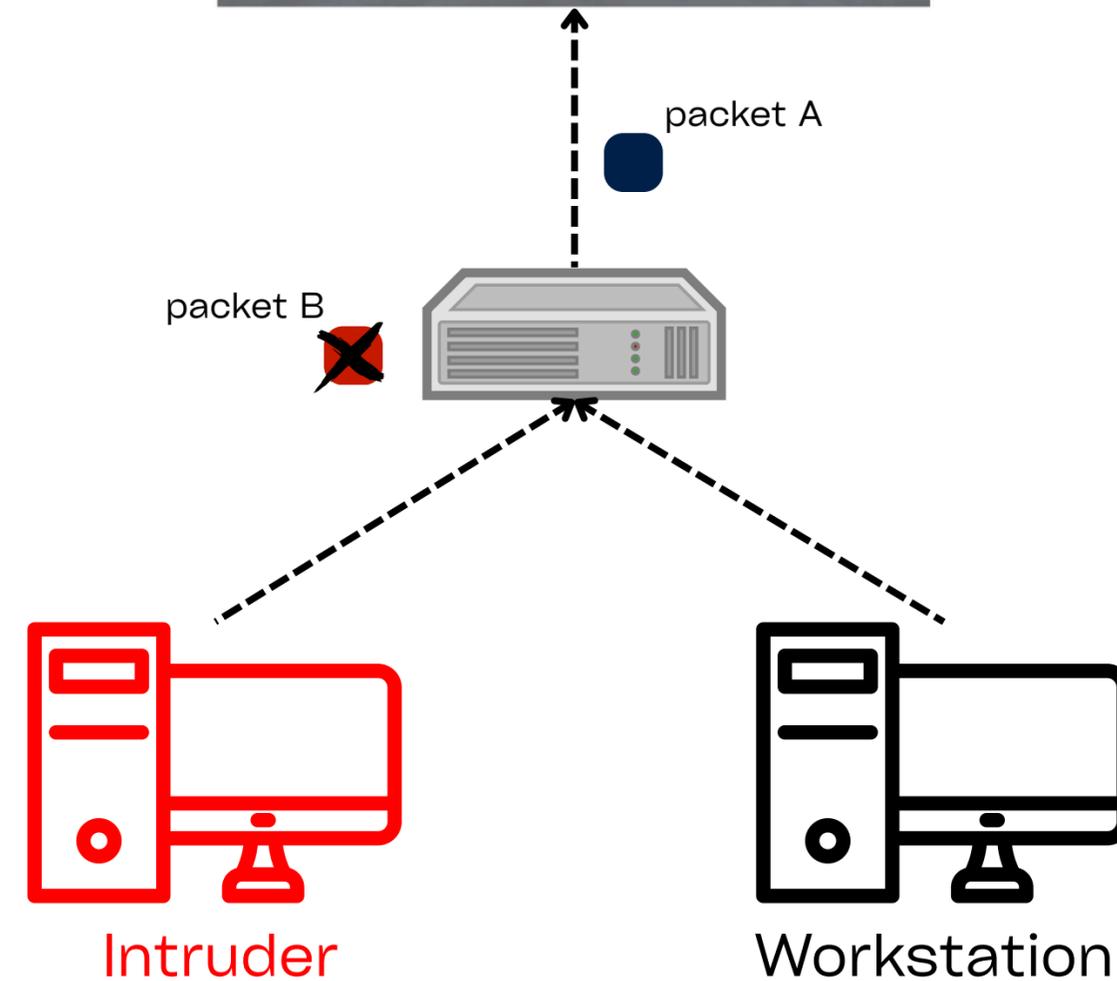
IV - The 3 main projects

1 - GRFICS (Chemical Plant)



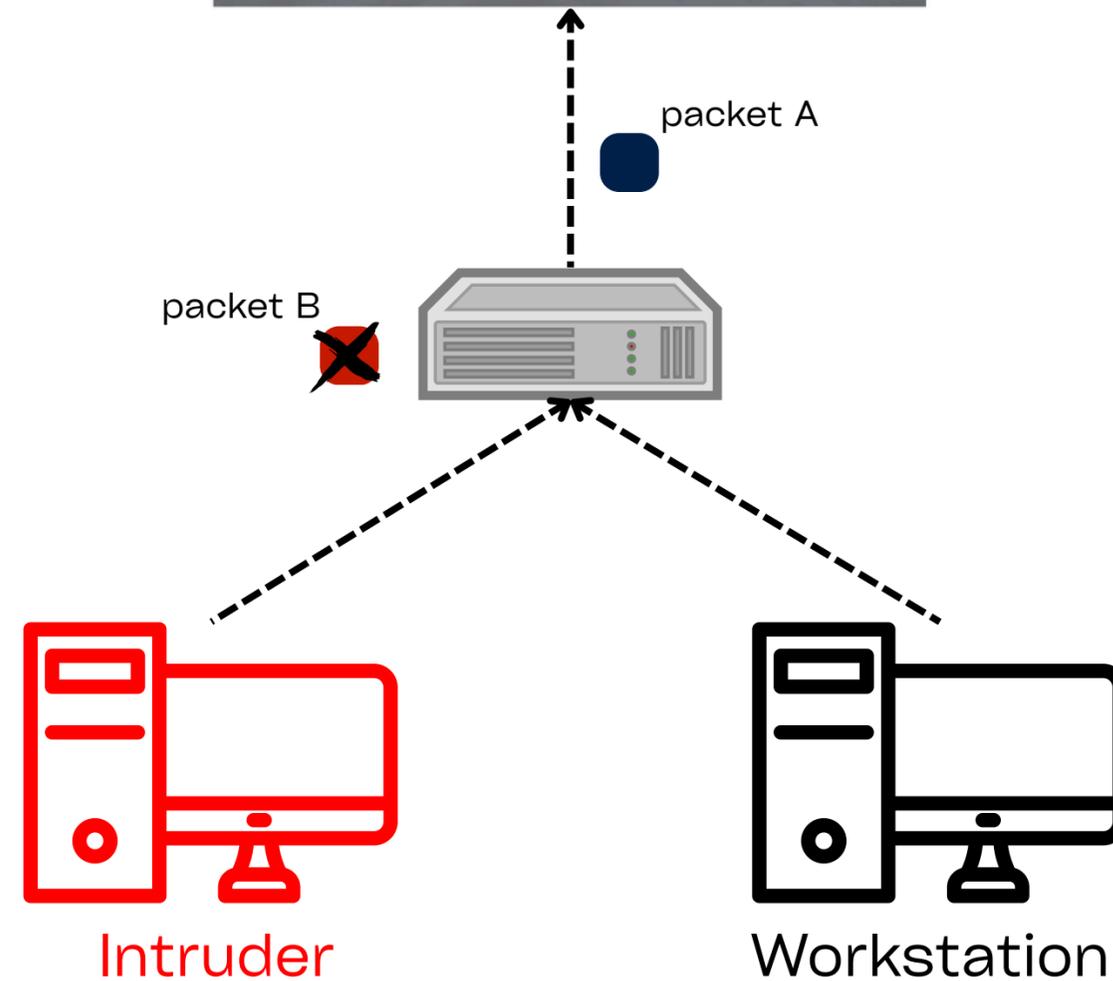
IV - The 3 main projects

1 - GRFICS (Chemical Plant)



IV - The 3 main projects

1 - GRFICS (Chemical Plant)



IV - The 3 main projects

1 - GRFICS (Chemical Plant)

Benefits





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

Benefits

Already installed, so no direct benefit for the CIH



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

Benefits

Already installed, so no direct benefit for the CIH

I understood what the CIH was working on



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

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

RealWorld Metro System Emulator

Date & Time: Jul 25 2023 10:46:53

Trains Control

East-West Line Code: EW

Train: weline - 0

Train: weline - 1

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

Train: ccline - 1

Train: ccline - 2

Train Speed Reset

Train Emergency Stop

Auto collision avoidance

Legend

- Train Sensor
- Train Station
- Railway Cross Signal
 - Green: Pass [off]
 - Red: Block [on]

Sensor-Signal-PLCs[PLC-00, PLC-01, PLC-02]
Last update Time: 08:00:00
Connection State: offline

Station-PLCs[PLC-03, PLC-04, PLC-05]
Last update Time: 08:00:00
Connection State: offline

Train-PLCs[PLC-06, PLC-07]
Last update Time: 08:00:00
Connection State: offline

Test mode: True

IV - The 3 main projects

2 - Cardiff Metro Emulator

railway SCADA HMI

East-West Line Code: EW
Circle Line Code: CC/CE
North-South Line Code: NS

PLC Monitor Panels [Signal system]

PLC Name: PLC-00[Masterslot-0] PLC IPAddr: 127.0.0.1 : 502 Connection: Connected	PLC Name: PLC-01[Slaveslot-1] PLC IPAddr: 127.0.0.1 : 502 Connection: Connected	PLC Name: PLC-02[Slaveslot-2] PLC IPAddr: 127.0.0.1 : 502 Connection: Connected
wes00 R_%H 0.0 %Q 0.0 OFF Swe00	wes14 R_%H 0.0 %Q 0.0 OFF Sns00	Scc04 R_%H 0.0 %Q 0.0 OFF Scc03
wes01 R_%H 0.1 %Q 0.1 OFF Swe01	wes15 R_%H 0.1 %Q 0.1 OFF Sns01	Scc05 R_%H 0.1 %Q 0.1 OFF Scc04
wes02 R_%H 0.2 %Q 0.2 OFF Swe02	wes16 R_%H 0.2 %Q 0.2 OFF Sns02	Scc06 R_%H 0.2 %Q 0.2 OFF Scc05
wes03 R_%H 0.3 %Q 0.3 OFF Swe03	wes17 R_%H 0.3 %Q 0.3 OFF Sns03	Scc07 R_%H 0.3 %Q 0.3 OFF Scc06
wes04 R_%H 0.4 %Q 0.4 OFF Swe04	wes18 R_%H 0.4 %Q 0.4 OFF Sns04	Scc08 R_%H 0.4 %Q 0.4 OFF Scc07
wes05 R_%H 0.5 %Q 0.5 OFF Swe05	wes19 R_%H 0.5 %Q 0.5 OFF Sns05	Scc09 R_%H 0.5 %Q 0.5 OFF Scc08
wes06 R_%H 0.6 %Q 0.6 OFF Swe06	wes20 R_%H 0.6 %Q 0.6 OFF Sns06	Scc10 R_%H 0.6 %Q 0.6 OFF Scc09
wes07 R_%H 0.7 %Q 0.7 OFF Swe07	wes21 R_%H 0.7 %Q 0.7 OFF Sns07	Scc11 R_%H 0.7 %Q 0.7 OFF Scc10
wes08 R_%H 0.8 %Q 0.8 OFF Swe08	wes22 R_%H 0.8 %Q 0.8 OFF Sns08	Scc12 R_%H 0.8 %Q 0.8 OFF Scc11
wes09 R_%H 0.9 %Q 0.9 OFF Swe09	wes23 R_%H 0.9 %Q 0.9 OFF Sns09	
wes10 R_%H 0.10 %Q 0.10 OFF Swe10	wes24 R_%H 0.10 %Q 0.10 OFF Sns10	
wes11 R_%H 0.11 %Q 0.11 OFF Swe11	wes25 R_%H 0.11 %Q 0.11 OFF Sns11	
wes12 R_%H 0.12 %Q 0.12 OFF Swe12	wes26 R_%H 0.12 %Q 0.12 OFF Sns12	
wes13 R_%H 0.13 %Q 0.13 OFF Swe13	wes27 R_%H 0.13 %Q 0.13 OFF Sns13	
wes14 R_%H 0.14 %Q 0.14 OFF Swe14	wes28 R_%H 0.14 %Q 0.14 OFF Sns14	
wes15 R_%H 0.15 %Q 0.15 OFF Swe15	wes29 R_%H 0.15 %Q 0.15 OFF Sns15	

PLC Monitor Panels [Station]

PLC Name: PLC-03[Masterslot-0] PLC IPAddr: 127.0.0.1 : 503 Connection: Connected	PLC Name: PLC-04[Slaveslot-1] PLC IPAddr: 127.0.0.1 : 503 Connection: Connected	PLC Name: PLC-05[Slaveslot-2] PLC IPAddr: 127.0.0.1 : 503 Connection: Connected
west00 R_%H 0.0 %Q 0.0 OFF STwe00	west08 R_%H 0.0 %Q 0.0 OFF STwe08	ccst00 R_%H 0.0 %Q 0.0 OFF STcc00
west01 R_%H 0.1 %Q 0.1 OFF STwe01	west09 R_%H 0.1 %Q 0.1 OFF STwe09	ccst01 R_%H 0.1 %Q 0.1 OFF STcc01
west02 R_%H 0.2 %Q 0.2 OFF STwe02	west10 R_%H 0.2 %Q 0.2 OFF STwe10	ccst02 R_%H 0.2 %Q 0.2 OFF STcc02
west03 R_%H 0.3 %Q 0.3 OFF STwe03	west11 R_%H 0.3 %Q 0.3 OFF STwe11	ccst03 R_%H 0.3 %Q 0.3 OFF STcc03
west04 R_%H 0.4 %Q 0.4 OFF STwe04	west12 R_%H 0.4 %Q 0.4 OFF STwe12	ccst04 R_%H 0.4 %Q 0.4 OFF STcc04
west05 R_%H 0.5 %Q 0.5 OFF STwe05	west13 R_%H 0.5 %Q 0.5 OFF STwe13	ccst05 R_%H 0.5 %Q 0.5 OFF STcc05
west06 R_%H 0.6 %Q 0.6 OFF STwe06	west14 R_%H 0.6 %Q 0.6 OFF STwe14	
west07 R_%H 0.7 %Q 0.7 OFF STwe07	west15 R_%H 0.7 %Q 0.7 OFF STwe15	
	west16 R_%H 0.8 %Q 0.8 OFF STwe16	
	west17 R_%H 0.9 %Q 0.9 OFF STwe17	
	west18 R_%H 0.10 %Q 0.10 OFF STwe18	
	west19 R_%H 0.11 %Q 0.11 OFF STwe19	
	west20 R_%H 0.12 %Q 0.12 OFF STwe20	
	west21 R_%H 0.13 %Q 0.13 OFF STwe21	
	west22 R_%H 0.14 %Q 0.14 OFF STwe22	
	west23 R_%H 0.15 %Q 0.15 OFF STwe23	

st mode: False

IV - The 3 main projects

2 - Cardiff Metro Emulator

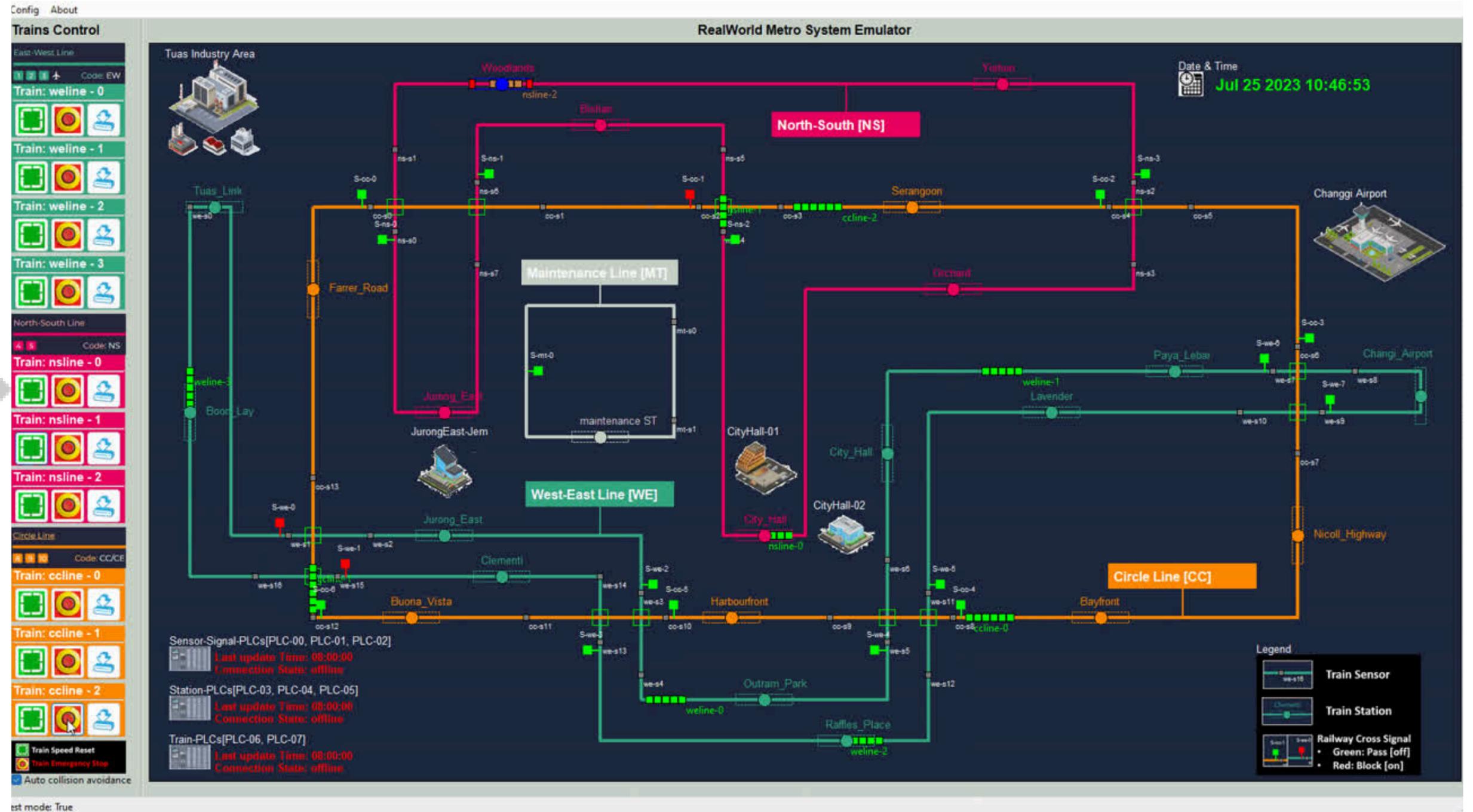
The screenshot displays the Cardiff Metro Emulator interface, which is organized into several key sections:

- Train Status Grid:** A 3x4 grid of panels for different train lines (weline, neline, celine). Each panel includes a speed gauge, a 'Power' indicator (ON/OFF), and digital readouts for Current (A) and Voltage (V).
 - weline (Green):** weline-0 (82 Km/h, 195 A, 717 V), weline-1 (84 Km/h, 196 A, 730 V), weline-2 (0 Km/h, 0 A, 791 V), weline-3 (58 Km/h, 179 A, 705 V).
 - neline (Pink):** neline-0 (98 Km/h, 150 A, 702 V), neline-1 (91 Km/h, 174 A, 723 V), neline-2 (99 Km/h, 156 A, 710 V).
 - celine (Orange):** celine-0 (85 Km/h, 179 A, 716 V), celine-1 (74 Km/h, 178 A, 702 V), celine-2 (91 Km/h, 199 A, 714 V).
- Trains Information Table:** A table listing 12 trains with their IDs, railway IDs, speeds, currents, DC voltages, and power states.

Train-ID	Railway-ID	Speed(km/h)	Current(A)	DC-Voltage(V)	Power-State
1	weline-0	82 km/h	195 A	702 V	ON
2	weline-1	84 km/h	174 A	720 V	ON
3	weline-2	0 km/h	0 A	794 V	OFF
4	weline-3	58 km/h	151 A	708 V	ON
5	neline-0	97 km/h	150 A	701 V	ON
6	neline-1	91 km/h	156 A	701 V	ON
7	neline-2	98 km/h	164 A	700 V	ON
8	celine-0	83 km/h	176 A	722 V	ON
9	celine-1	84 km/h	168 A	722 V	ON
10	celine-2	79 km/h	174 A	716 V	ON
11					
12					
- PLC Monitor Panels [Trains]:** Two panels showing PLC status for 'Master' and 'Slave' units. Each panel lists various digital outputs (e.g., R_SH01 to R_SH10) and their current states (ON/OFF).
- Control Panel:** Located at the bottom right, featuring a 'Trains Collision Auto-Avoidance' toggle set to 'Enable'.

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



IV - The 3 main projects

2 - Cardiff Metro Emulator

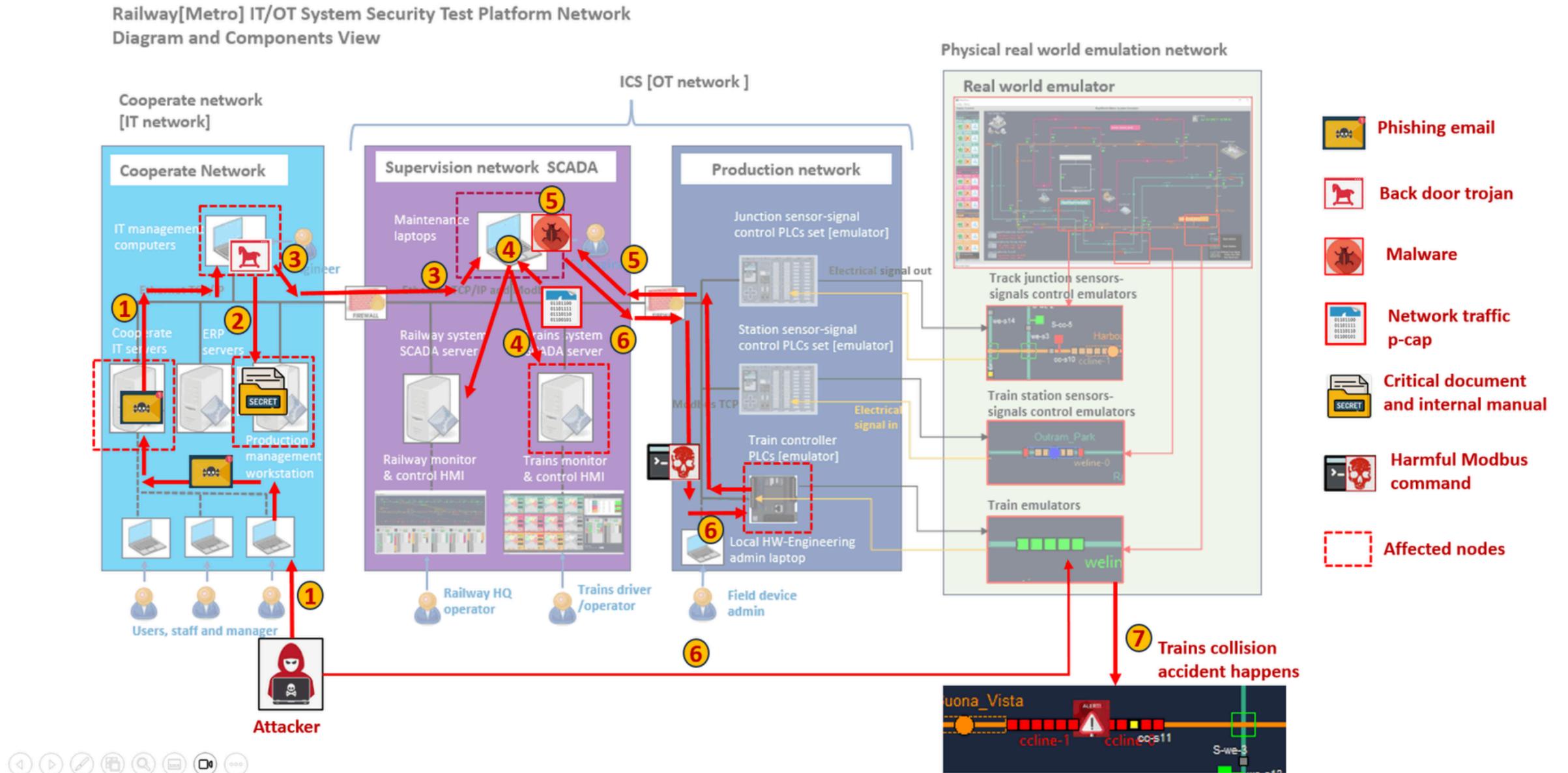
My work:

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

IV - The 3 main projects

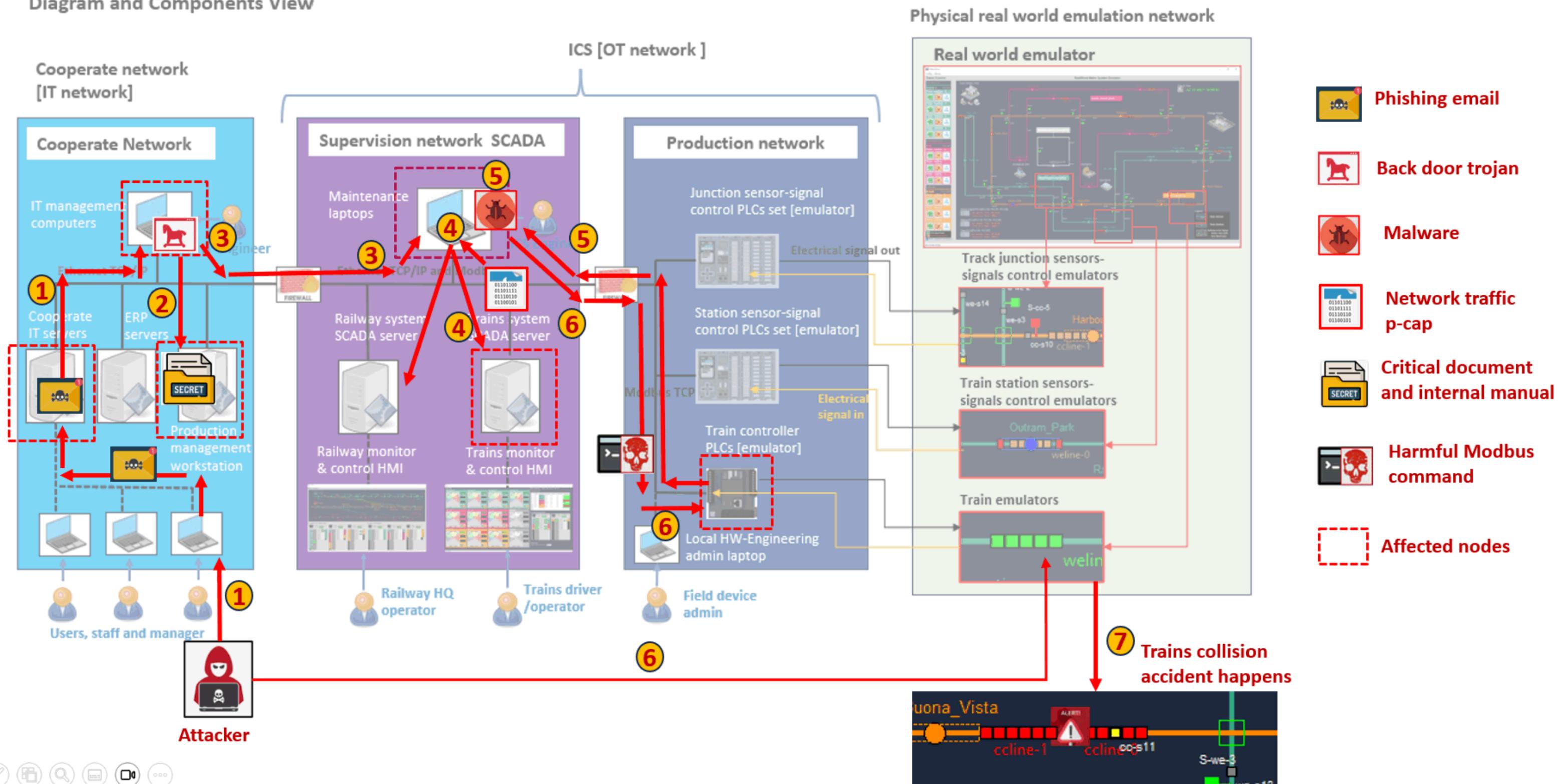
2 - Cardiff Metro Emulator

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



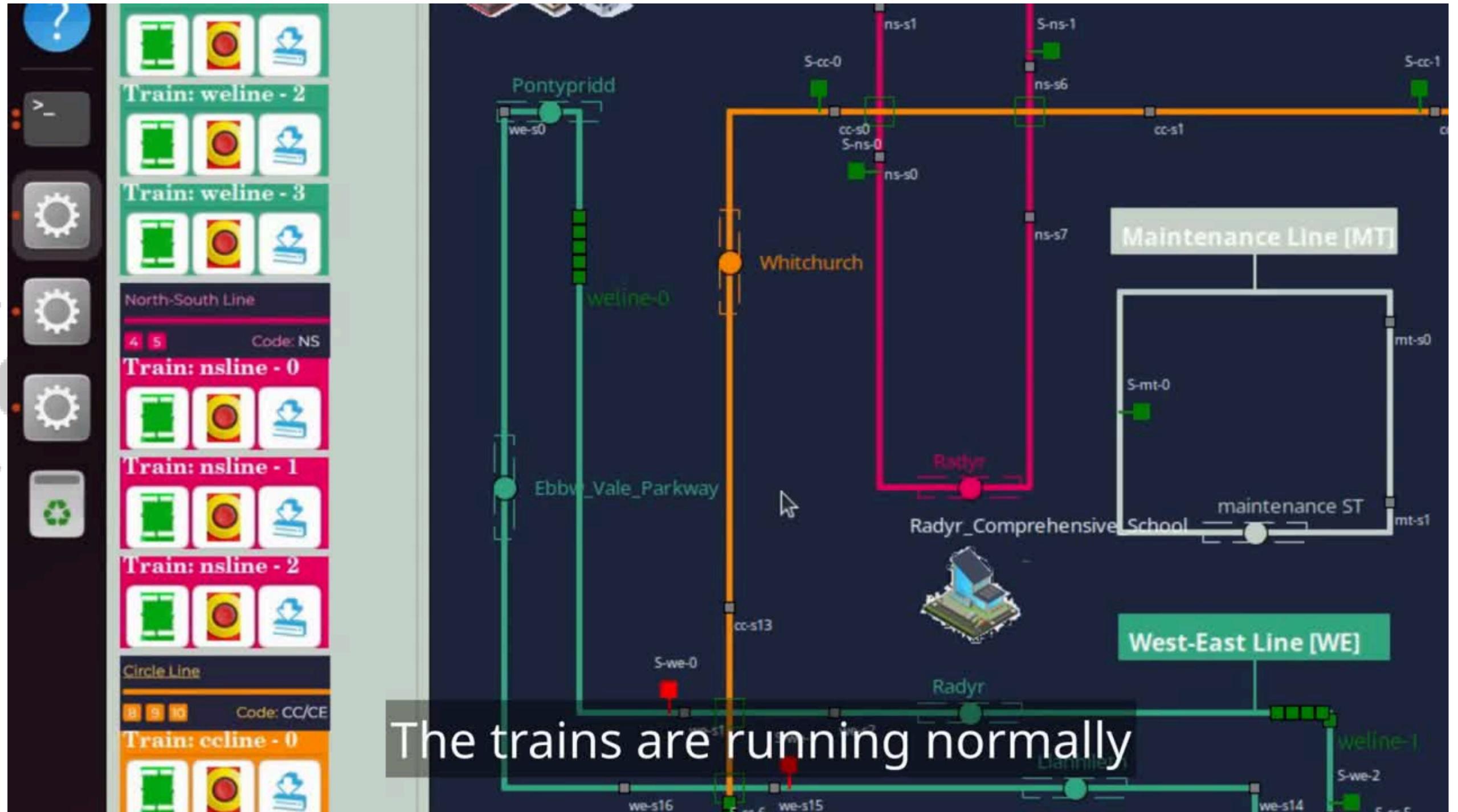
Attack Scenario 1: False command injection attack via phishing email and Backdoor Trojan

Railway[Metro] IT/OT System Security Test Platform Network Diagram and Components View



IV - The 3 main projects

2 - Cardiff Metro Emulator



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



IV - The 3 main projects

3 - Bottle Filling Plant

2 main problems:

IV - The 3 main projects

3 - Bottle Filling Plant

2 main problems:

- The PLC should be programmed using ladder logic

IV - The 3 main projects

3 - Bottle Filling Plant

2 main problems:

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

IV - The 3 main projects
3 - Bottle Filling Plant

SIEMENS

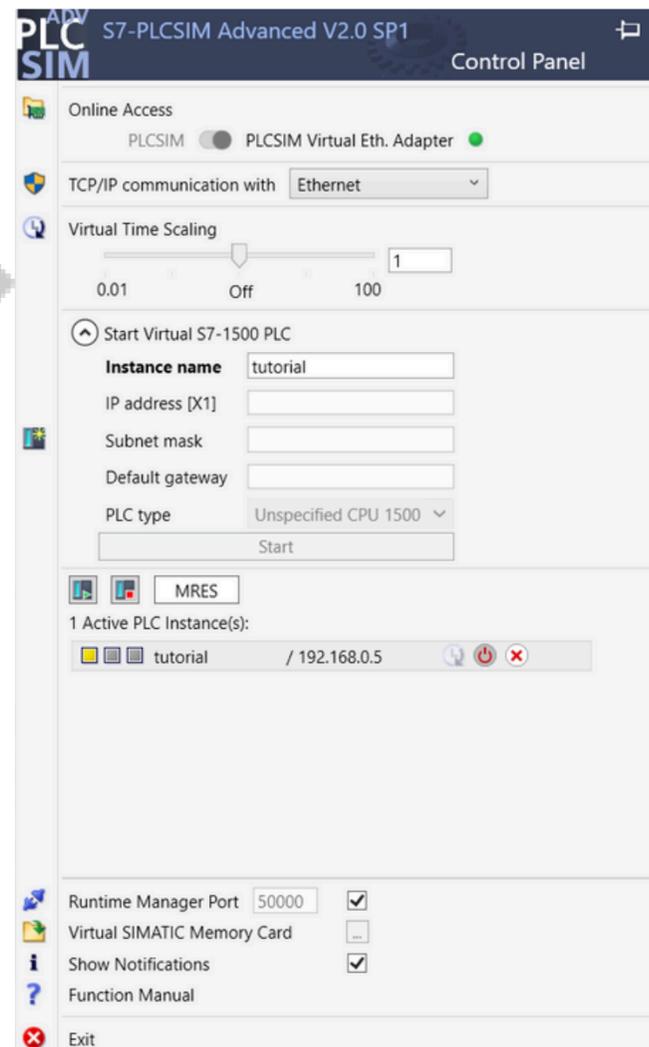


IV - The 3 main projects

3 - Bottle Filling Plant

SIEMENS

PLC Simulator



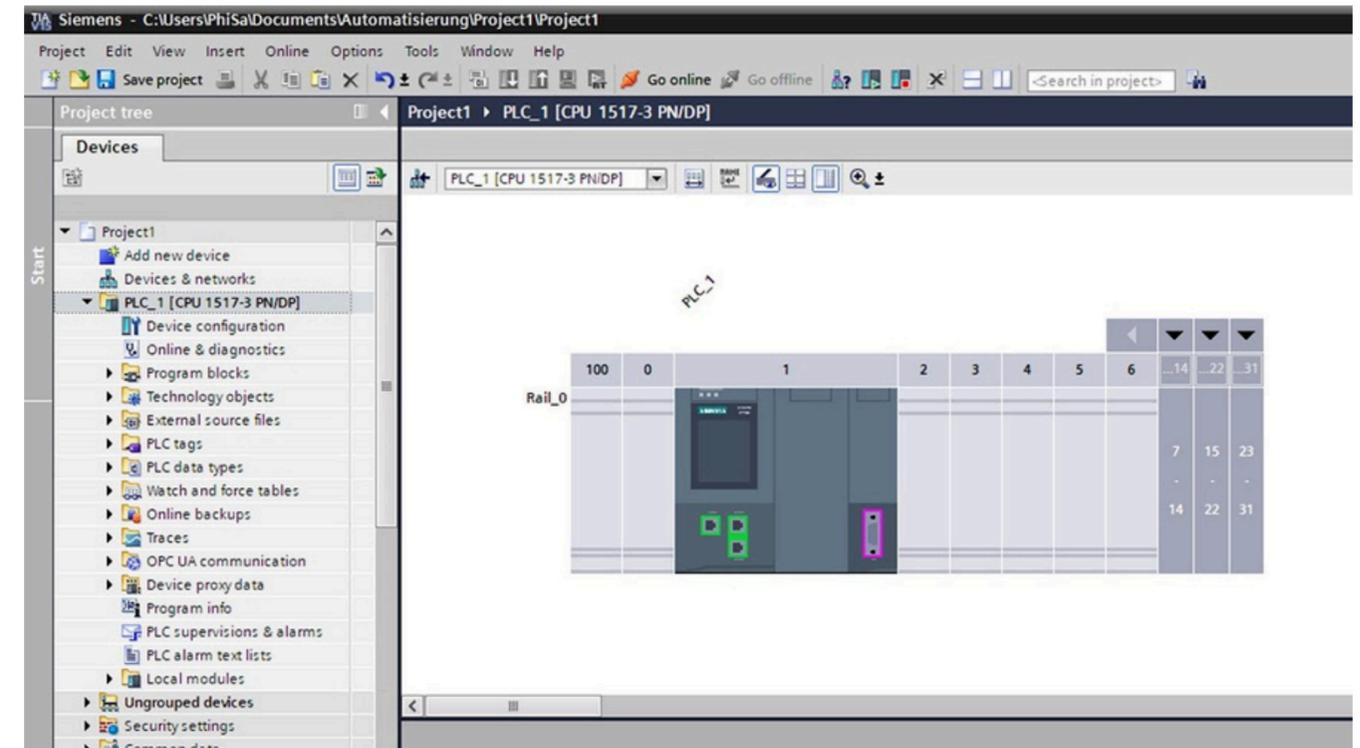
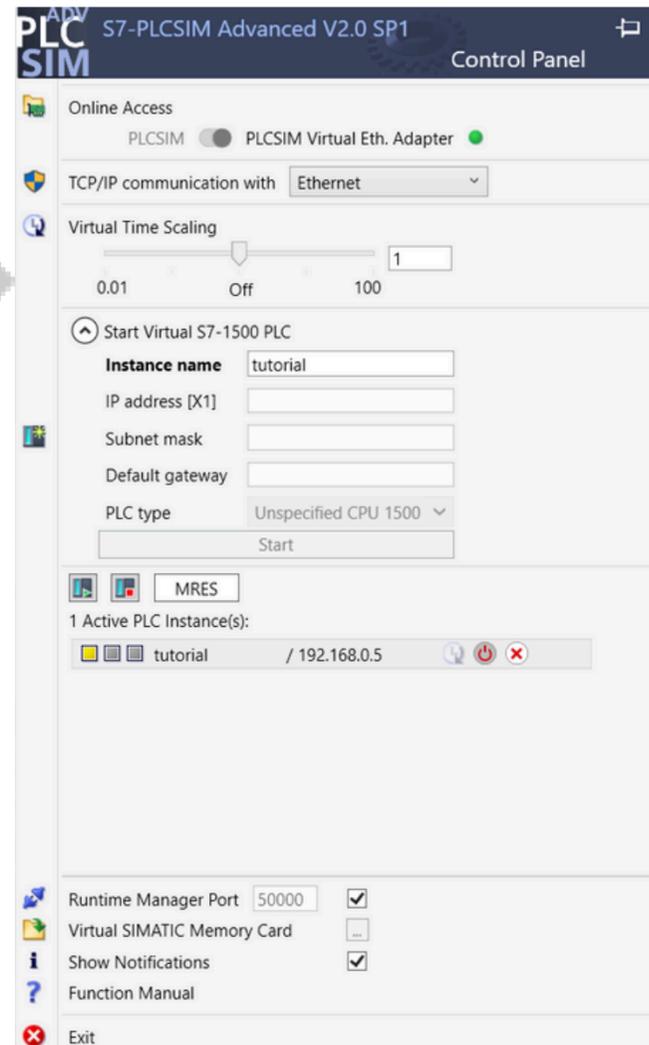
IV - The 3 main projects

3 - Bottle Filling Plant

SIEMENS

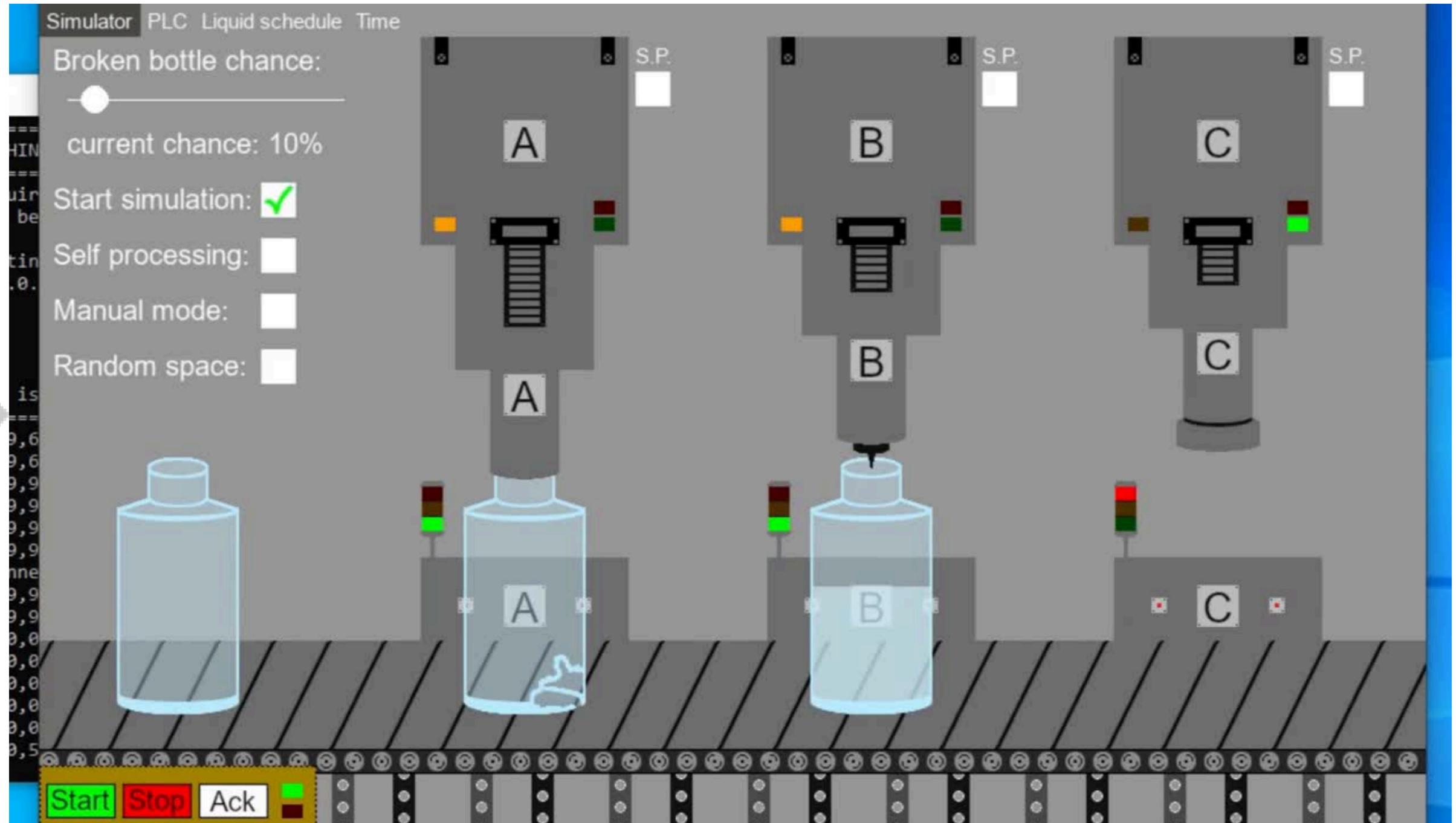
PLC Simulator

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

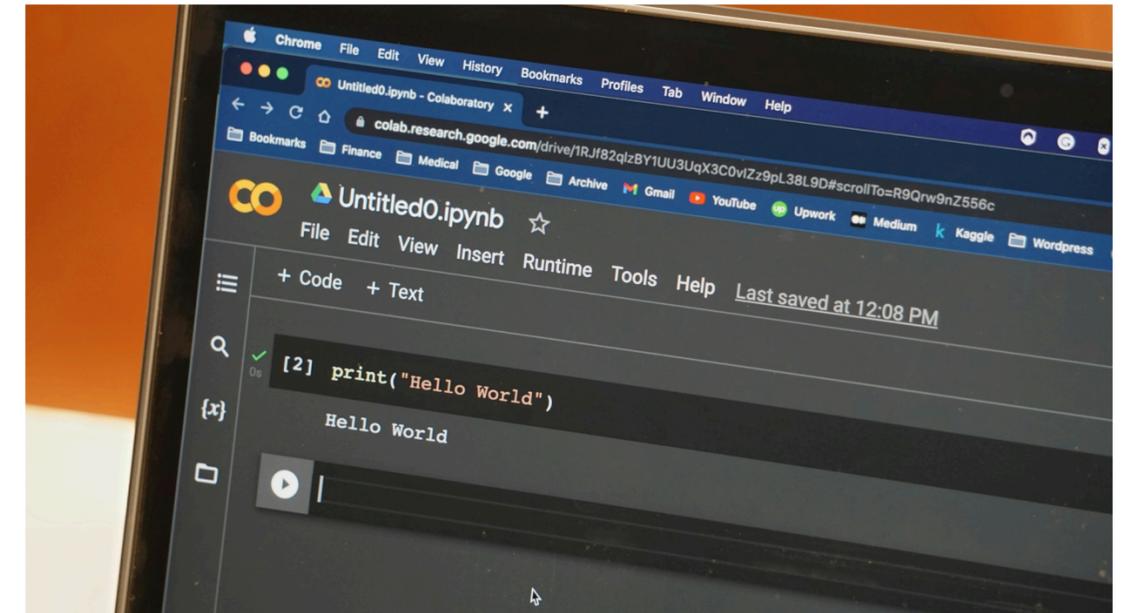
Python = 170 lines

Ladder logic = 7 days of 8 hours

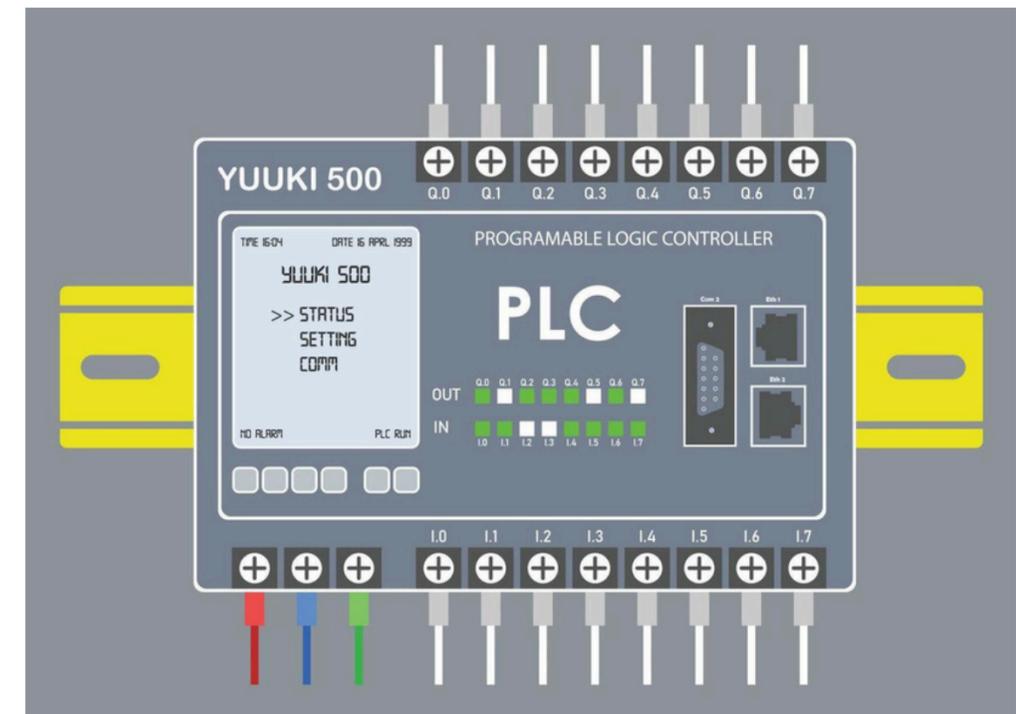
IV - The 3 main projects

3 - Bottle Filling Plant

Python = 170 lines



Ladder logic = 7 days of 8 hours



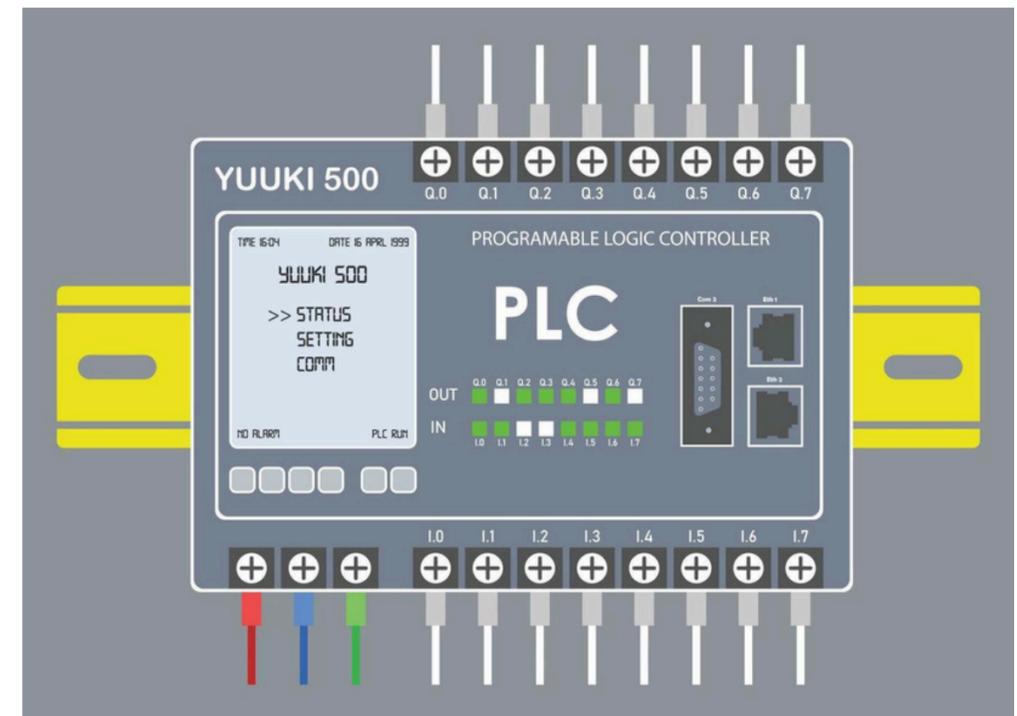
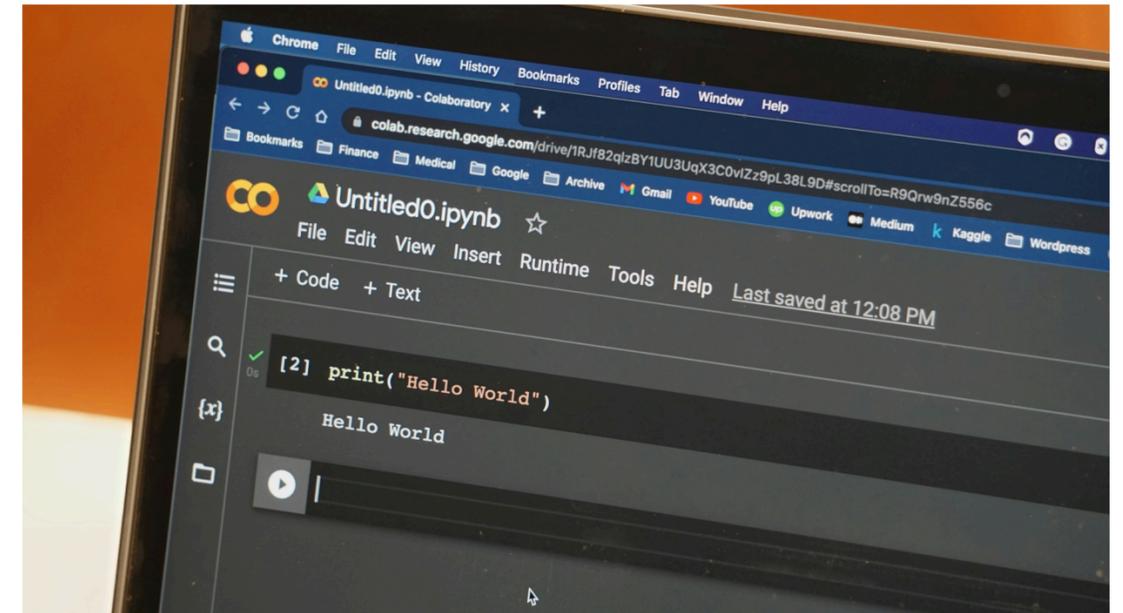
IV - The 3 main projects

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

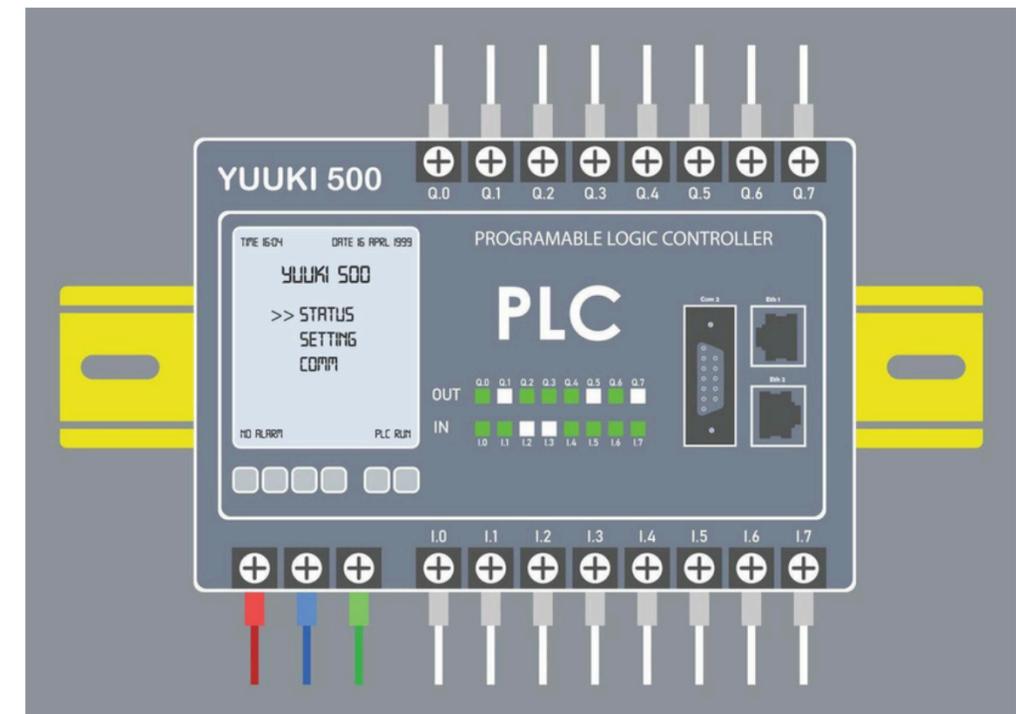
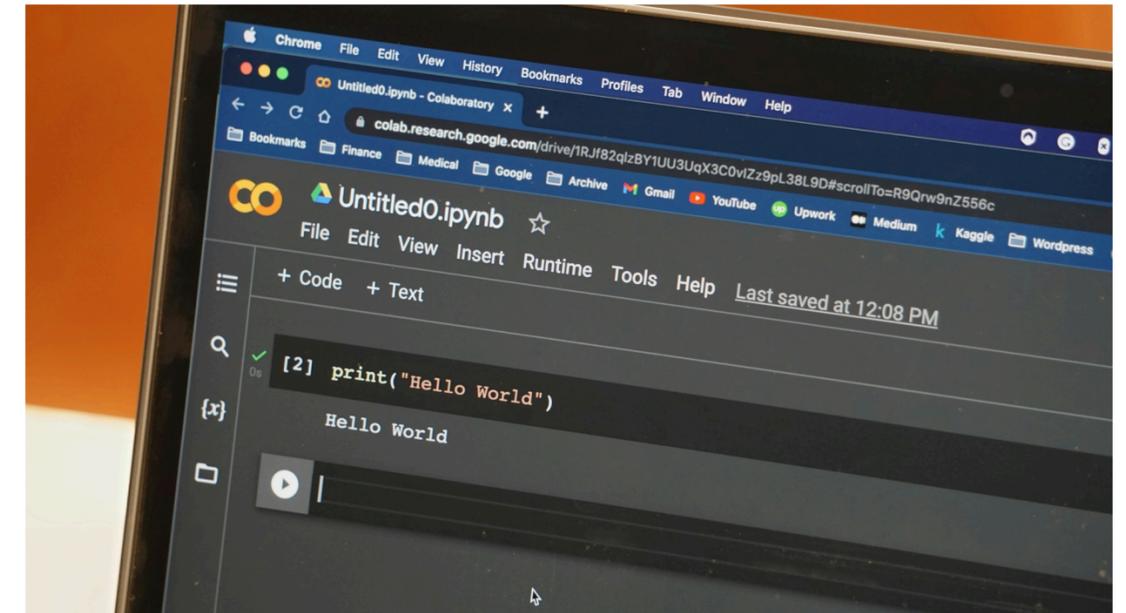
Python = 170 lines

Written programming language

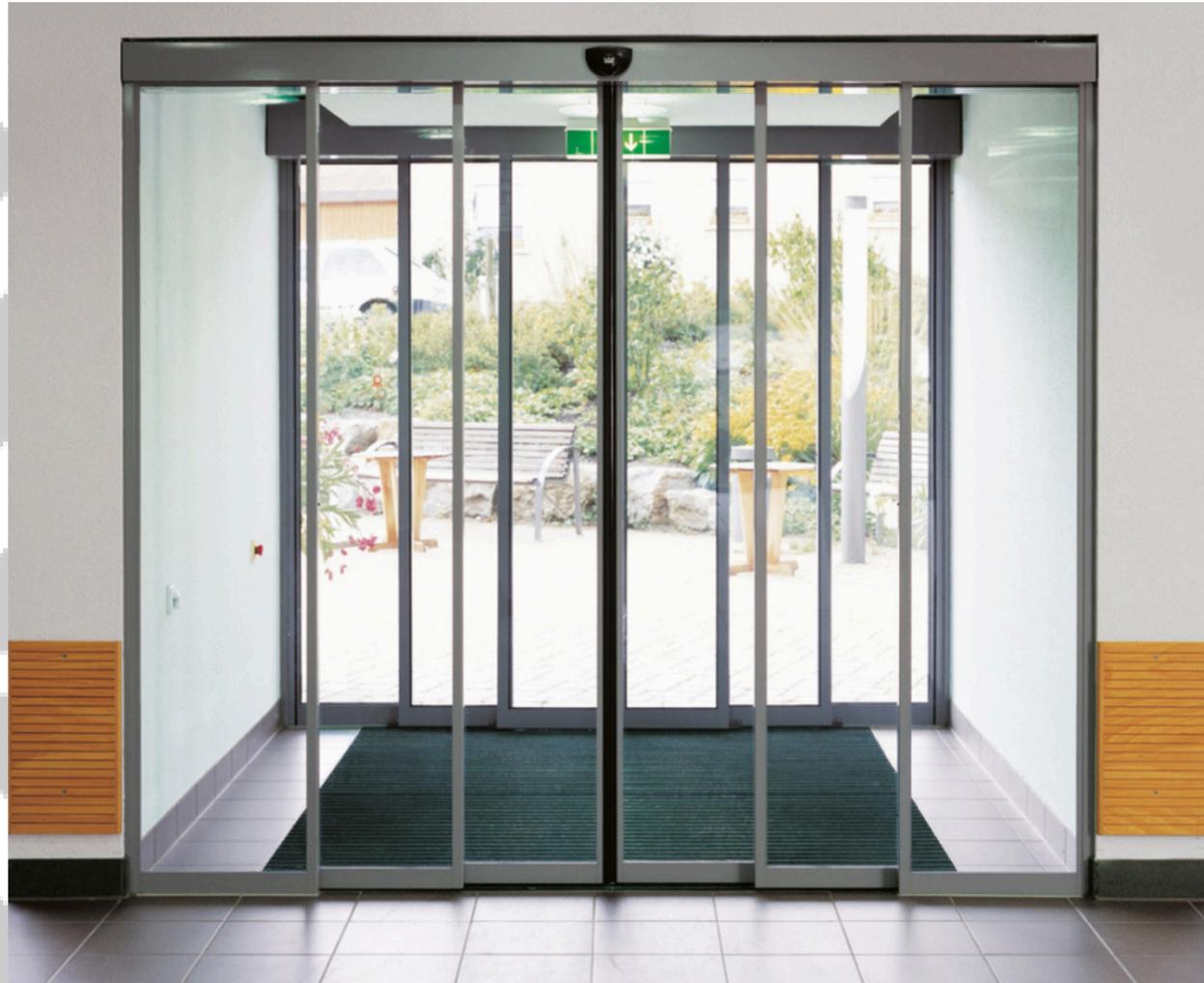
Ladder logic = 7 days of 8 hours

Visual programming language

Mainly conditions



IV - The 3 main projects 3 - Bottle Filling Plant

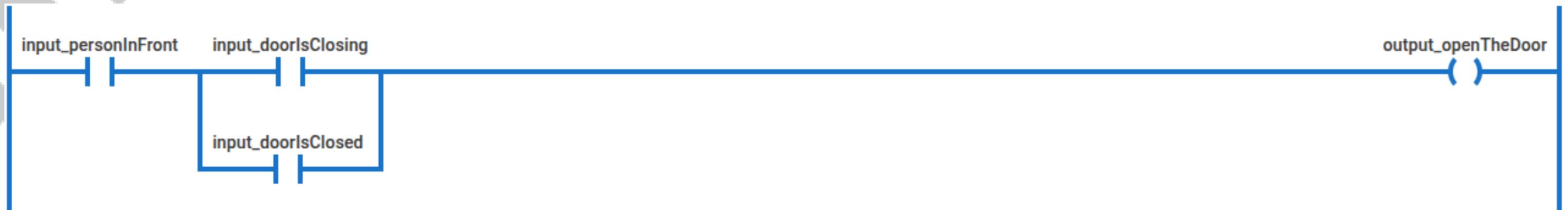


IV - The 3 main projects

3 - Bottle Filling Plant

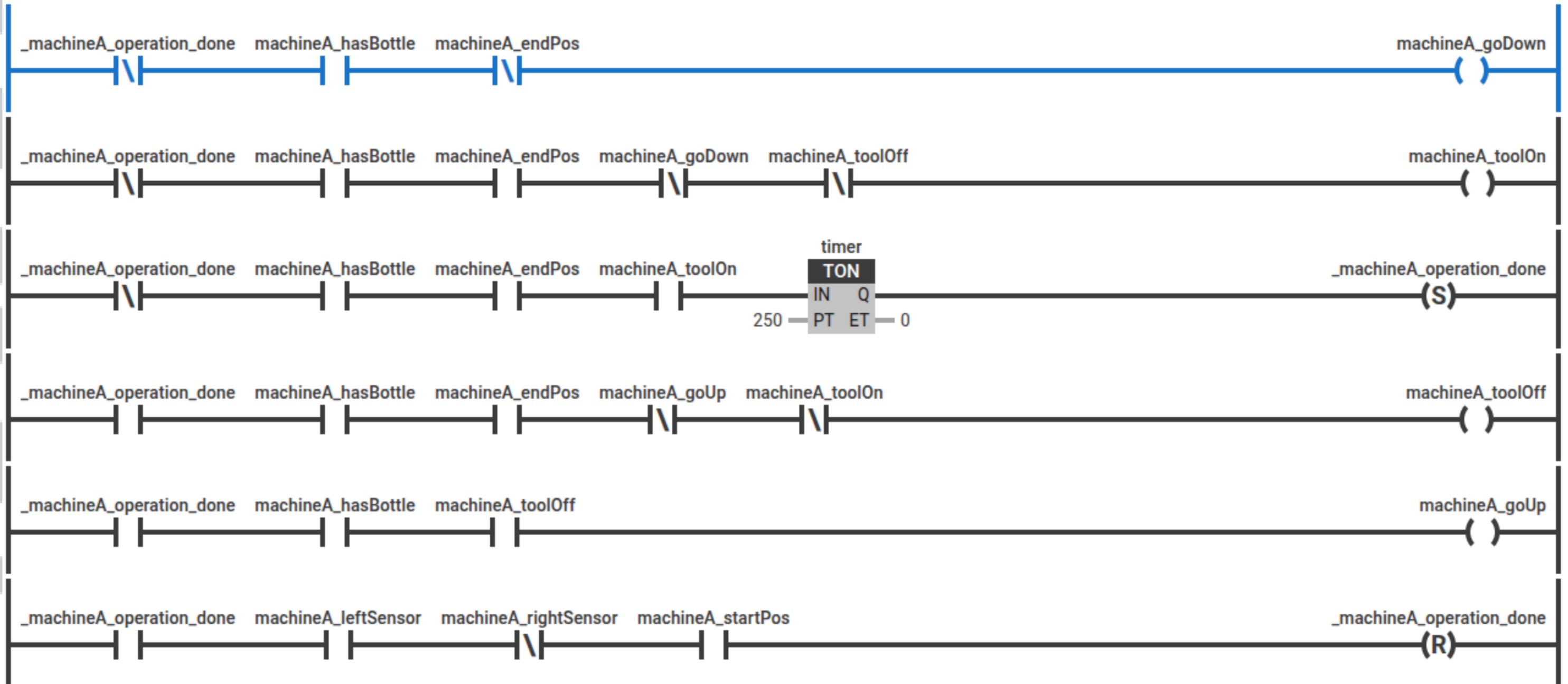


=

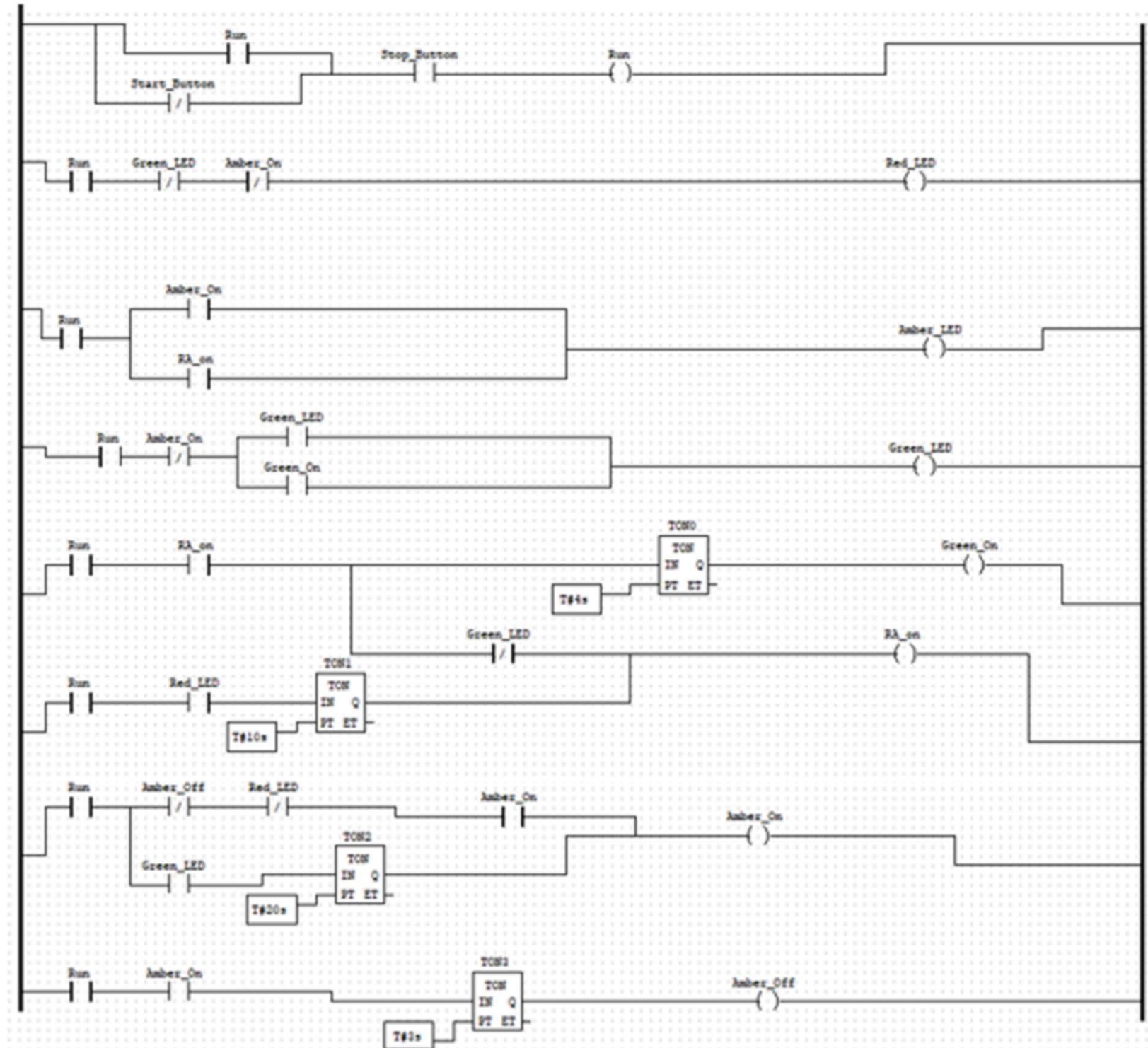


IV - The 3 main projects

3 - Bottle Filling Plant

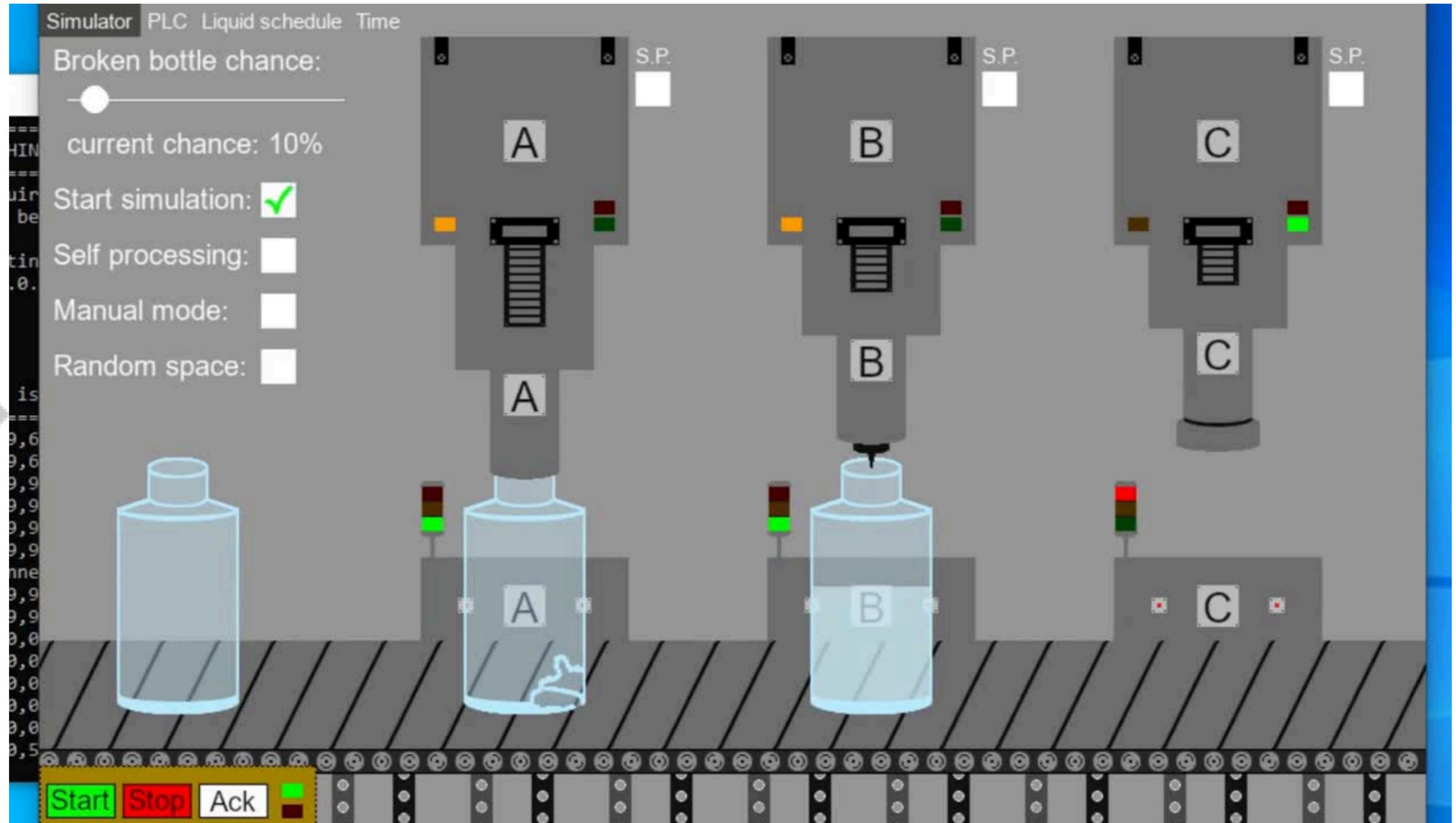


IV - The 3 main projects



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



V - Current VS Initial situation, Technical & Human Assessment

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

1 simulation

No documentation

No videos for presentations

After

3 simulations

Documentation on:

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

Videos for:

- Chemical Plant
- Cardiff Metro Emulator
- Bottle Filling Plant

V - Current VS Initial situation, Technical & Human Assessment

Before

1 simulation

No documentation

No videos for presentations

No way to control the screen wall

After

3 simulations

Documentation on:

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

Videos for:

- Chemical Plant
- Cardiff Metro Emulator
- Bottle Filling Plant

A simple webpage to control all the screens

V - Current VS Initial situation, Technical & Human Assessment

Before

1 simulation

No documentation

No videos for presentations

No way to control the screen wall

No easy and educative way to approach cybersecurity

After

3 simulations

Documentation on:

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

Videos for:

- Chemical Plant
- Cardiff Metro Emulator
- Bottle Filling Plant

A simple webpage to control all the screens

8 scenarios in the Backdoors&Breaches game

V - Current VS Initial situation, Technical & Human Assessment



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



V - Current VS Initial situation, Technical & Human Assessment

Discovered people and a new culture

V - Current VS Initial situation, Technical & Human Assessment

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

Internship at the Cyber Innovation Hub

Cybersecurity in Operational Technologies

Final words



Hyb Arloesedd Seiber
Cyber Innovation Hub

