Innovarpel 2025

TECHNICAL DAYS

DIGITAL TRANSFORMATION
& INDUSTRIAL CYBERSECURITY
IN THE OIL&GAS INDUSTRY

arpel 60 YEARS

JUNE, 24 & 25
Rio de Janeiro, Brazil

Implementing a cybersecurity program in industrial environments: The strategy to address common challenges and achieve better results

Tonny Matos Siqueira

Cybersecurity Consultant for Automation at Petrobras

Who I am?

Tonny Siqueira

- 20 years at Petrobras
- 17 years of experience in automation and instrumentation maintenance and project execution
- Cybersecurity Consultant for Automation at Petrobras
- Engineer in automation, electronics, electrical and telecommunications

PÚBLICA

Agenda - Common challenges

- Digitalization of Industrial Automation
- Cybersecurity for OT
- Improve (and maintain) your maturity
- Is it enough?

PÚBLICA

Innovarpel 2025

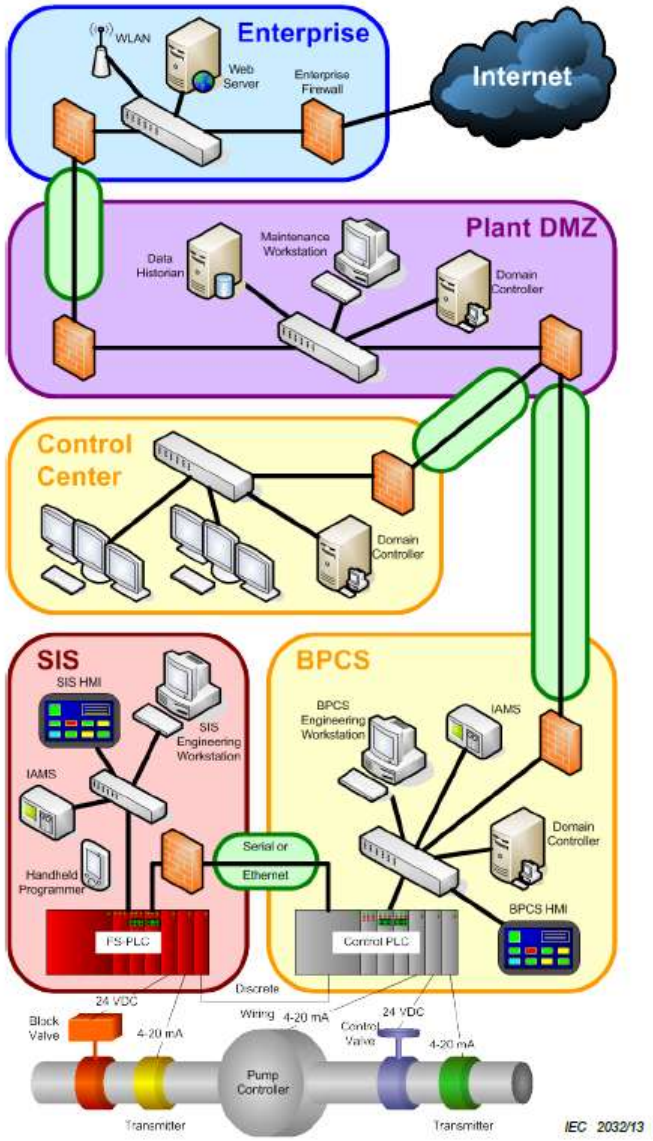
Digitalization of Industrial Automation - OT

PÚBLICA

Corporate x Industrial

Corporate IT

Industrial OT



PÚBLICA

OT & IT evolution

Foxboro pneumatic controller

First pneumatic controller

1930

Yokogawa Centum

One of the first DCS

1975

World Wide Web

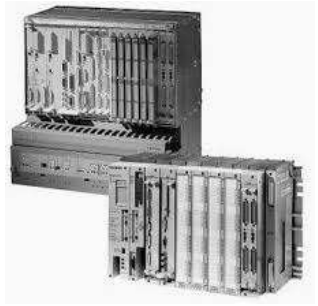
CERN

1990

Modicom 084

First Programmable Logic Controller - PLC

1970



IBM Model 5150

One of the first PCs

1980

PÚBLICA

OT evolution

PÚBLICA

OT evolution

PÚBLICA

IT-OT Integration / Convergence

- **The Good Side** ✓
  - Access to real-time operational data
  - Better decision-making based on data-driven insights
  - Process optimization and efficiency gains
  - Predictive maintenance and reduced downtime
  - Cost reduction through improved operations
  - Enabler for Innovation: Industry 4.0, IIoT, and digital transformation
- **The Bad Side** ✗
  - Increased attack surface with more connected devices and systems
  - Cyber threats from IT can reach OT (viruses, ransomware, malware)
  - IT patching cycles are incompatible with OT stability needs
  - Vulnerable legacy systems and insecure protocols (Modbus TCP, Profinet, etc.)
  - Operational impact – cyber incidents can cause production stoppages or physical damage
  - Potential safety and environmental risks due to cyber attacks

PÚBLICA

Cybersecurity for OT

Cybersecurity for industrial environment

PÚBLICA

What is the industry?

PÚBLICA

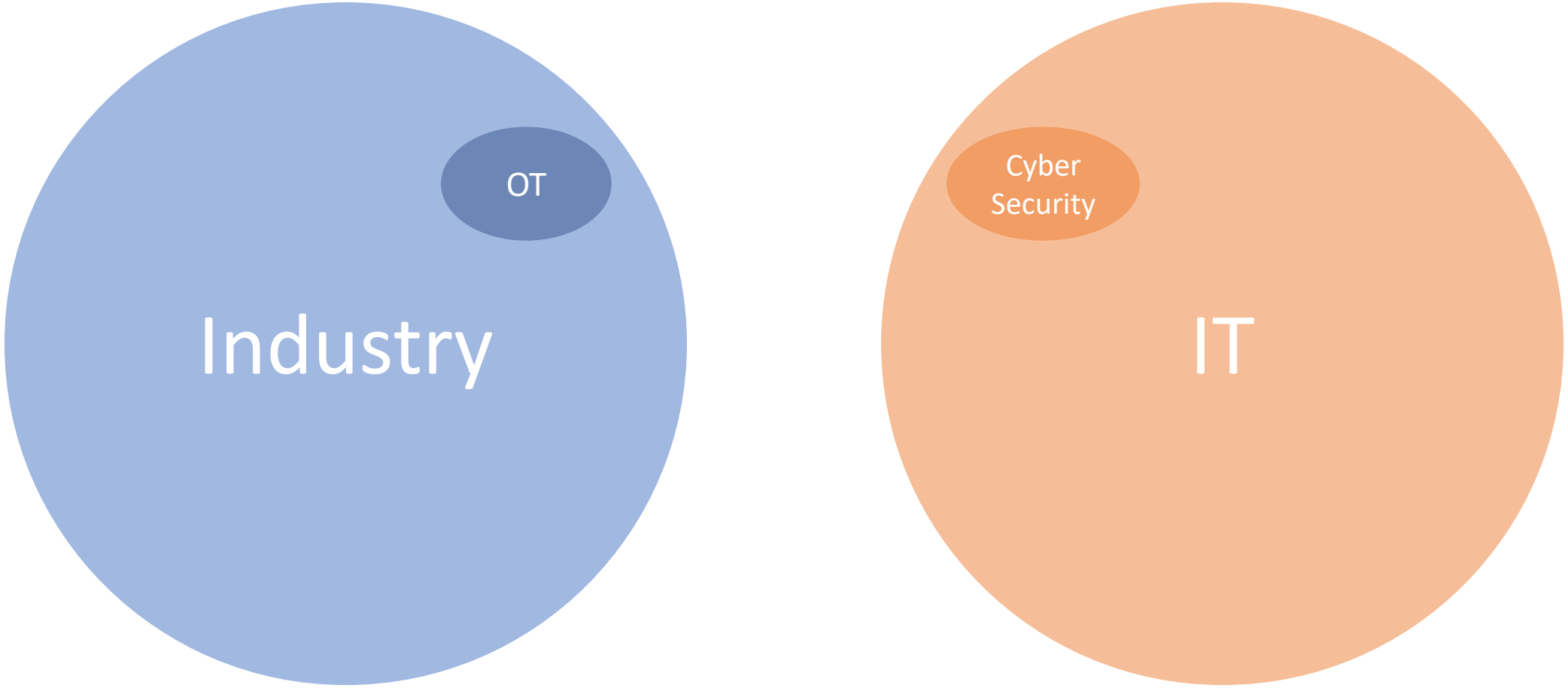
What is in the industry?

Physical – OT

Cyber – IT

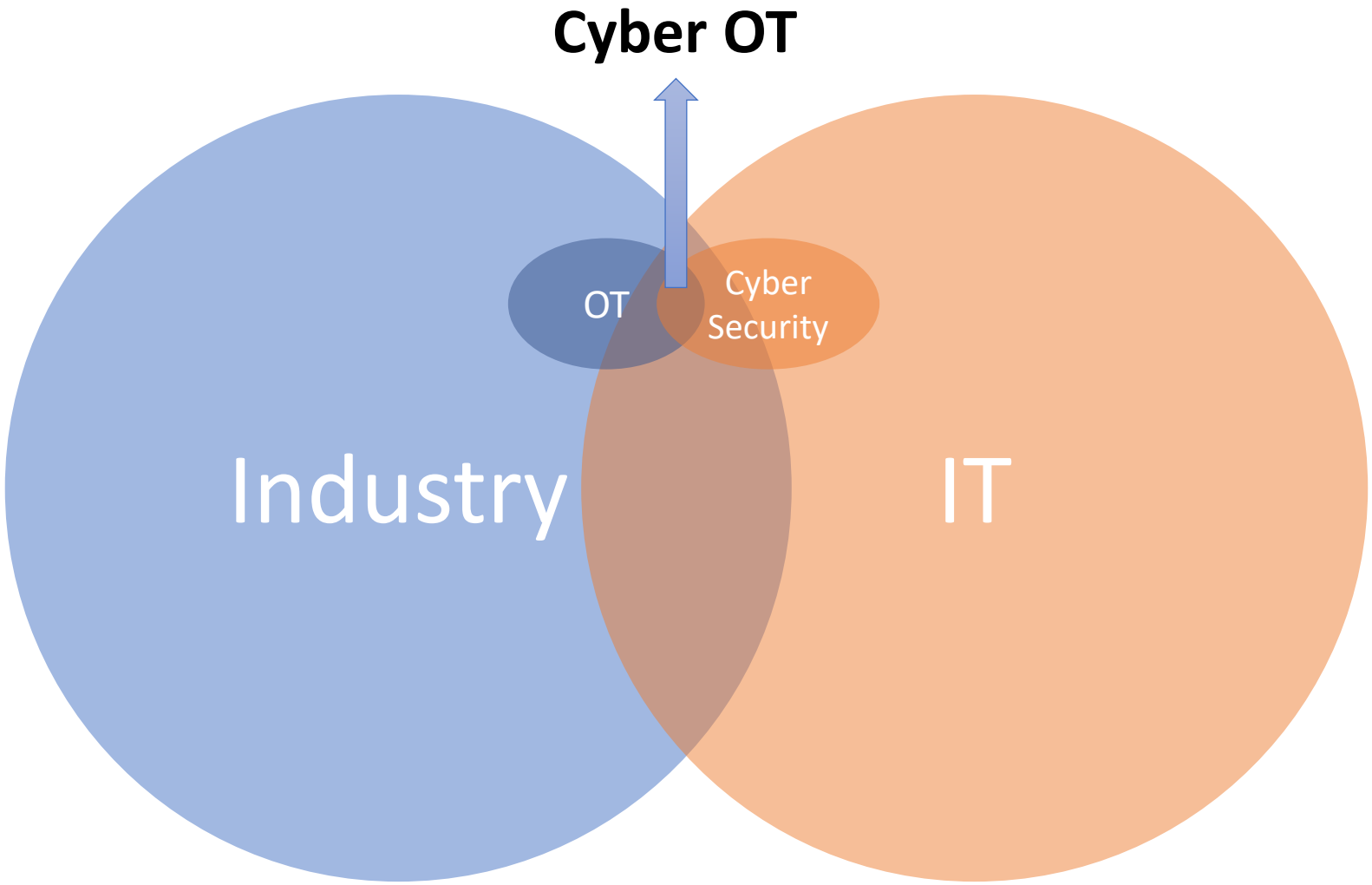
PÚBLICA

Cybersecurity for OT



PÚBLICA

Cybersecurity for OT



PÚBLICA

Geographical Distribution of Petrobras Production Units

- ~ 6,000 employees in Cyber-OT program
- ~ 550 Departments/Divisions
- 30 owned offshore platforms
- 17 chartered offshore platforms
- 10 refineries
- 4 gas processing plants
- 13 thermoelectric power plants

PÚBLICA

Improve (and maintain) your maturity

PÚBLICA

Maturity Standards / Frameworks

IT

ISO 27001

CIS Controls

OT

Industrial communication networks
Network and system security

IEC 62443

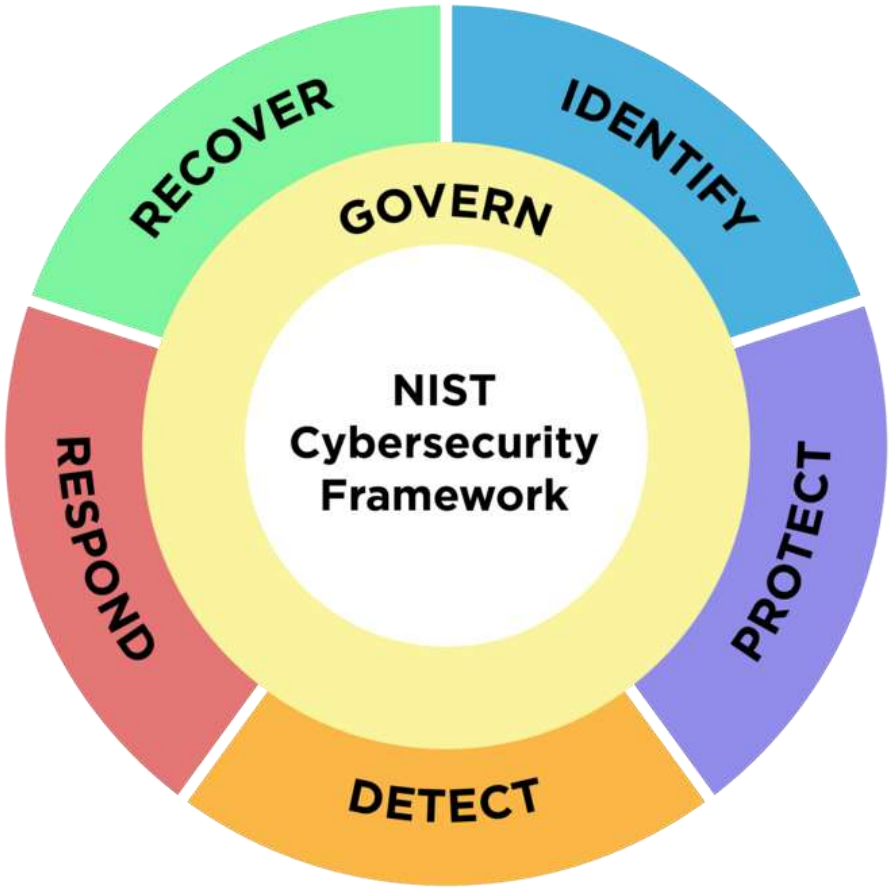
C2M2
Cybersecurity Capability Maturity Model

Guide to Operational Technology (OT) Security

CIS Critical Security Controls v8.1 Industrial Control Systems (ICS) Guide

PÚBLICA

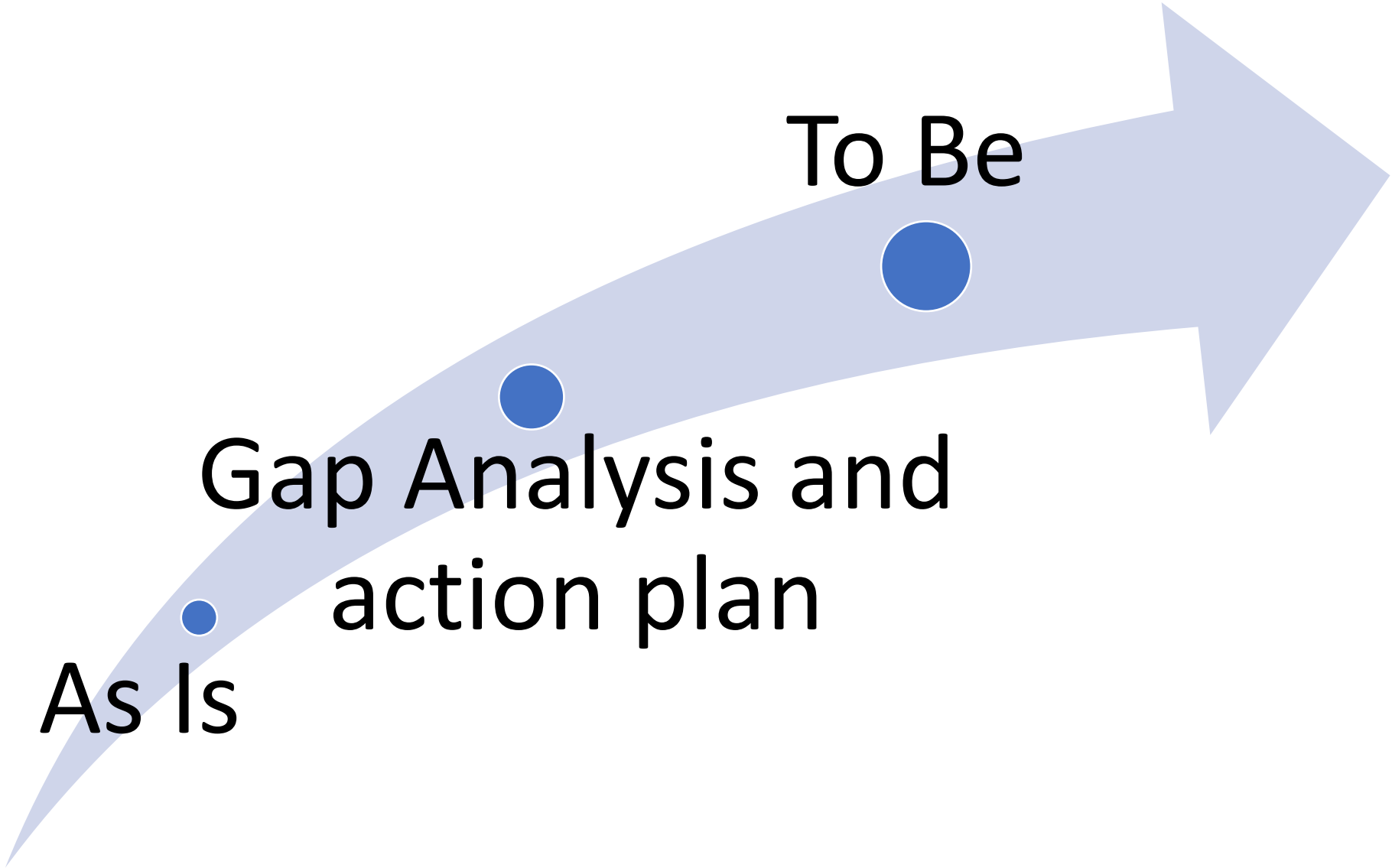
Maturity Standards / Frameworks



NIST CSF v2.0

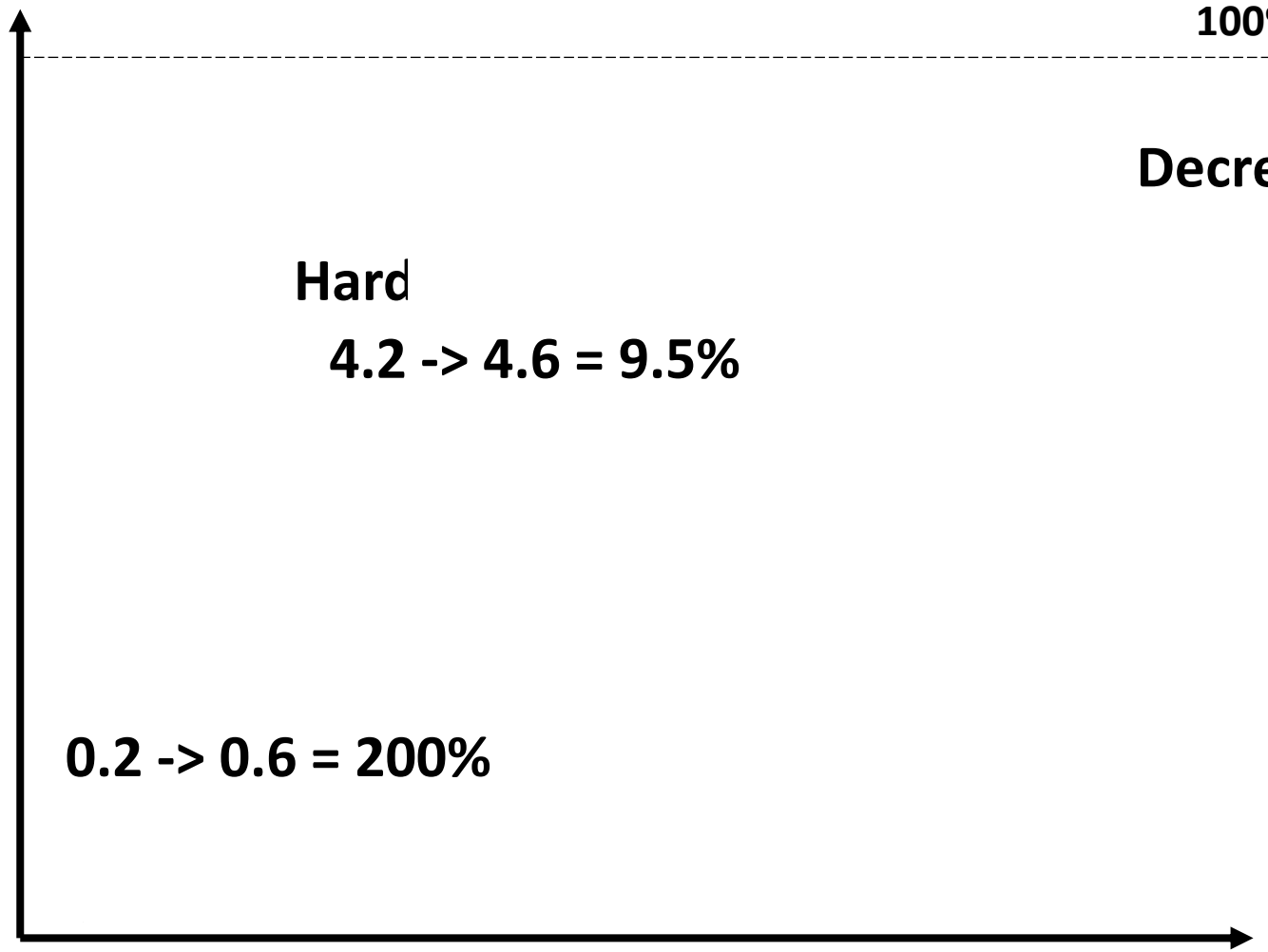
PÚBLICA

Gap Analysis



PÚBLICA

Maturity Evolution



PÚBLICA

Improve (and maintain) your maturity

- Improve
  - C-Level sponsorship
  - Choose a framework
  - GAP analysis (AS-IS -> TO-BE)
  - Develop an action plan
  - Include all areas involved
    - OT
    - IT
    - Cybersecurity
    - HSE
    - Others?
  - Include in Performance Appraisal
  - Monitor periodically
  - Start again!
- Maintain
  - Recognize the factors of degradation
  - Identify the controls for these degradation factors
  - Determine monitoring methods
  - Create a monitoring system
  - Establish objectives
  - Implement processes to sustain
  - Monitor periodically

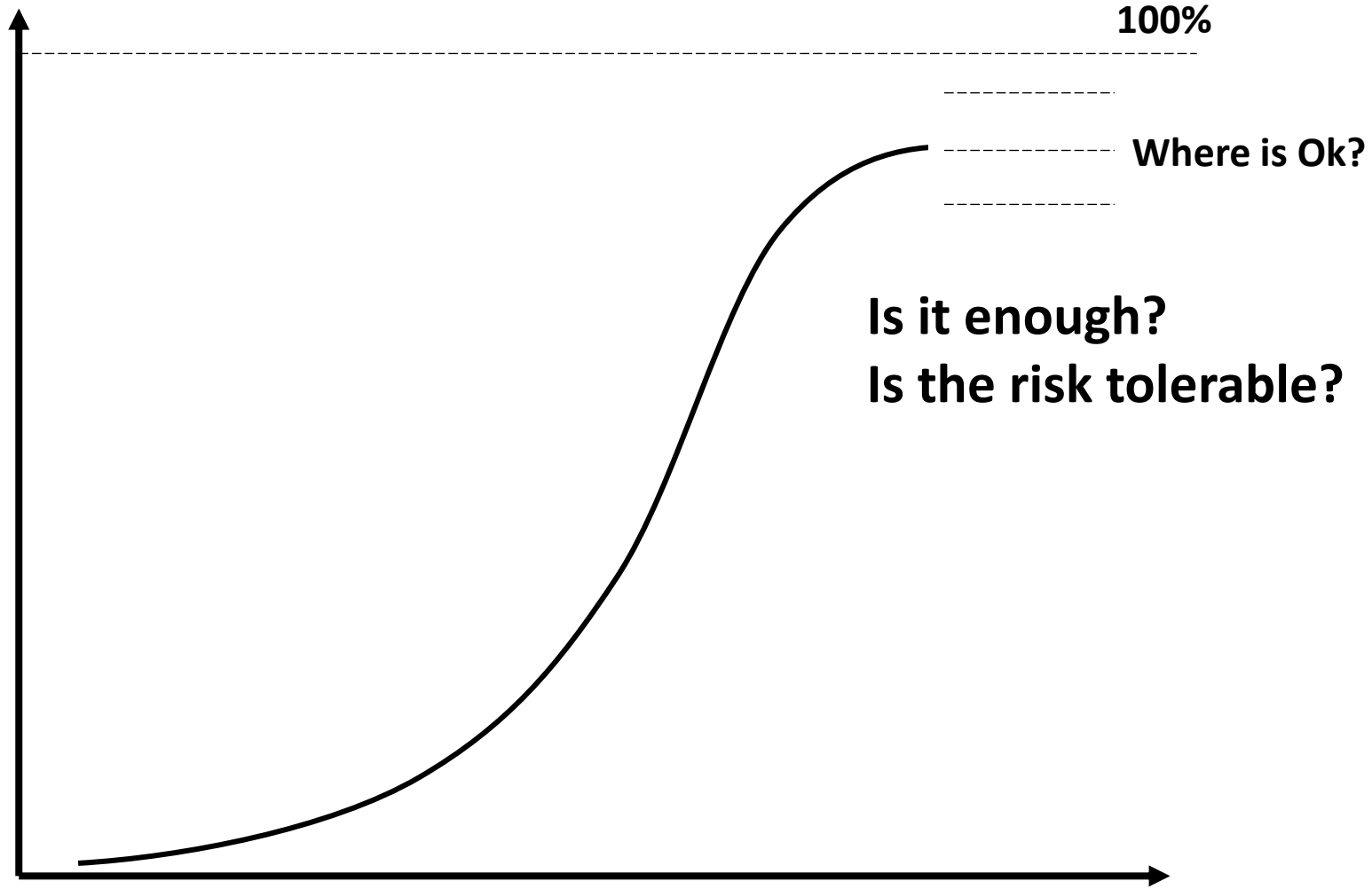
PÚBLICA

Innovarpel 2025

Is it enough?

PÚBLICA

Maturity Evolution



PÚBLICA

Strategies for Risk Analysis in Industrial Environments

- A framework does not determine the ideal maturity
- A risk analysis calibrates the target maturity level
- Deciding on the ideal maturity is done through Risk Analysis
- Methods for Industrial Cyber Risk Analysis:
  - IEC 62443-3-2
  - NIST SP 800-30
  - ISO/IEC 27005
  - FAIR - Factor Analysis of Information Risk
- Practical risk analysis methods:
  - Qualitative
  - Semi-quantitative
  - Quantitative

PÚBLICA

Thank you!

Tonny Matos Siqueira

tmsiqueira@petrobras.com.br