



**National Centre  
of Excellence**  
CYBERSECURITY TECHNOLOGY  
AND ENTREPRENEURSHIP

**DSCI**  
PROMOTING DATA PROTECTION  
A **nasscom** Initiative

**Infopercept**



# ACCELERATING OT SECURITY





© **Copyright 2024**

**All rights reserved**

The information contained herein has been obtained from sources believed to be reliable. It should not be relied upon as a substitute for specific professional advice. Professional advice should always be sought before taking any action based on the information provided. NCoE -DSCI shall have no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof. NCoE- DSCI disclaims all warranties as to the accuracy, completeness or adequacy of such information.

No part of this publication may be reproduced either on paper or electronic media without the prior permission of NCoE-DSCI. Request for permission to reproduce any part of the volume should be sent to NCoE at [ncoe@dsci.in](mailto:ncoe@dsci.in), or mailed to our address

# CONTENTS

---

Executive Summary 05

**01** Introduction 07

- 1.1** Operational Technology (OT) 08
- 1.2** OT Security 08
  - 1.2.1** Components of Modern OT Systems 09
  - 1.2.2** Types of OT Devices 10
- 1.3** Operational Technology Transformation 11
- 1.4** Difference Between IT and OT Cybersecurity 11
- 1.5** Purdue Model 12

**02** Challenges & Opportunities for Innovation 15

- 2.1** Power Sector 16
- 2.2** Oil & Gas Sector 18
- 2.3** Manufacturing and Aviation Sectors 19
- 2.4** Healthcare Sector 20

**03** Research Productization Initiative – IDS for OT Environment 21

- 3.1** Background 22
- 3.2** Product Description 22
- 3.3** How will it Benefit the Indian OT Security/ Global OT Security Space? 23



# CONTENTS

---

**04**

Indian Startup Ecosystem

25

- 4.1** Arishti Info Labs Private Limited 26
- 4.2** GRIDsentry Private Limited 27
- 4.3** Saptang Labs Private Limited 27
- 4.4** Infopercept Consulting Private Limited 28

**05**

Initiatives

29

- 5.1** Leader's Perspective: Setting the Path for Development of OT Security in India 30
- 5.2** Workshop on SCADA/OT Security: Empowering India's Innovation Capability and Research 31
- 5.3** Healthcare Sector Webinar: Challenges and the Future of Healthcare Ecosystem 31
- 5.4** Hands-on Technology Workshop: Understanding and Dissecting Cyber Physical System Protocols 32

**06**

Conclusion

33

# Executive Summary



The National Centre of Excellence for Cyber Security Technology Development and Product Entrepreneurship (NCoE) is a joint initiative of the Data Security Council of India (DSCI) and the Ministry of Electronics and Information Technology (MeitY), Government of India. In collaboration with C-DAC (Centre for Development of Advanced Computing) & Infopercept, NCoE launched the SCADA/OT Security Acceleration Program on November 23, 2022, in New Delhi.

This initiative aimed to drive the development of market-ready products in OT security.

This program stood as a unique effort within the framework of the Triple Helix Model, promoting collaboration between industry, government, and academia. Its core objective was to facilitate the exchange of use cases and co-creation of innovative solutions within the OT security domain. Embracing the principles of the Triple Helix Model, this initiative envisioned a partnership between stakeholders from different arrays of sectors that contributed their expertise and perspectives to address the problems in OT security.

The program was launched by Dr. Sanjay Bahl, DG, CERT-in; Mr. Vinayak Godse, CEO, DSCI; and Dr. S D Sudarsan, Executive Director, C-DAC, Bangalore. This initiative garnered support from MeitY, security leaders, and experts from critical sectors such as Power, Energy, Oil & Gas, Manufacturing, and Aviation.

Throughout the program, various activities like webinars, hands-on technology workshops, and industry-academia interactions were conducted. These activities aimed to enhance visibility within the ecosystem, understand the challenges, and identify potential use cases for the development of commercial technologies and evolve a future strategy for product development to address OT security concerns.

A significant achievement of the acceleration program was the technology transfer of the Operational Technology Intrusion Detection System (OT IDS) from SASTRA Deemed University to Infopercept Consulting Pvt. Ltd. This milestone, supported by MeitY, the Government of India, and the collaborative efforts of NCoE, Academia (SASTRA Deemed University), and Industry (Infopercept), successfully translated research efforts funded by MeitY into a stage of commercial technology adoption.





01

Introduction





01

# Introduction

## 1.1 Operation Technology (OT)

Operational technology (OT) involves the use of specialised hardware and software systems in various industries including manufacturing, power, energy, transportation, and other sectors. These systems are used to monitor, control, and manage real-time physical processes, devices, and infrastructure. These systems are specifically designed to automate industrial processes and often communicate using custom protocols and legacy software.

OT systems are distinct from standard IT systems as they primarily focus on the operational aspects of an organisation, ensuring the smooth running of critical processes. In contrary to IT systems, which prioritise processing data and managing information, OT systems prioritise aspects

like system availability, safety, and reliability. They are used in sectors where continuous operation is vital and where an interruption in the process can have detrimental impact on safety, productivity, and the environment.

## 1.2 OT Security

OT security refers to the protective measures and controls implemented to safeguard OT systems. These systems, powered by specialized software designed for automating industrial processes, face the ongoing challenge of potential cybersecurity threats. With the increasing integration of information technology and OT enhancing automation and efficiency in industrial systems, robust OT security has become an essential component of managing critical infrastructure.

Operational technology (OT) involves the use of specialised hardware and software systems in various industries including manufacturing, power, energy, transportation, and other sectors.



## 1.2.1 Components of Modern OT Systems



### **Industrial Control Systems (ICS)**

Industrial Control Systems encompass various systems known as 'factory automation' or 'distributed control systems.' These systems, including Distributed Control Systems (DCS), Supervisory Control and Data Acquisition Systems (SCADA), and Industrial Internet of Things (IIoT), serve as interfaces for managing manufacturing, process control, transportation (rail and maritime), and related functions.



### **Distributed Control Systems (DCS)**

DCS is a subset of ICS designed for managing complex processes in discrete or continuous production environments. It plays a crucial role in controlling and overseeing activities like power generation, manufacturing, and refining within a single geographic location.



### **Supervisory Control and Data Acquisition Systems (SCADA)**

SCADA systems function as comprehensive data networks, capturing inputs and outputs of industrial processes and enabling system monitoring, analysis, and control. They collect data from widely distributed Input/Output (I/O) devices across a large geographic area, often utilized in sectors such as electric transmission, pipelines, and rail operations.



### **Buildings and Physical Access Controls**

OT also extends to systems governing physical facilities, including elevators, HVAC systems, lighting, and related components. Building and access controls encompass security measures like surveillance cameras, swipe card systems, and electronic door locks, employing distinct protocols and approaches separate from industrial systems.

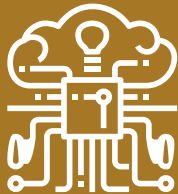
## 1.2.2 Types of OT Devices

Given the diverse array of device types deployed on OT networks, they can be categorized into four main groups:



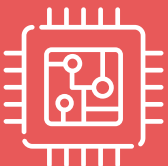
### **Servers, Workstations, and Human-Machine Interfaces (HMI)**

These devices typically run conventional operating systems like Windows or Linux and serve various control and reporting functions, including domain control and critical process application software. Some may also function as historian servers, gathering and transmitting data to enterprise data systems.



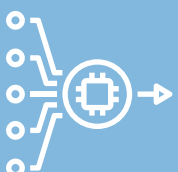
### **Networking Equipment**

OT systems include specialized networking equipment, in addition to traditional IT switches and firewalls. Examples include industrial firewalls designed to control traffic using industrial protocols. These purpose-built devices operate on proprietary embedded operating systems provided by networking equipment manufacturers.



### **Embedded Control Devices**

This category encompasses a wide range of control devices such as Programmable Logic Controllers (PLCs), distributed control systems controllers, remote terminal units, protective relays, and machine controls for manufacturing devices. These devices run proprietary embedded operating systems developed by manufacturers, often customized using commodity components.



### **Input/Output (I/O) Devices**

I/O devices provide inputs to or outputs from industrial processes. They encompass a vast array of devices, including PLC rack cards, cameras, pressure and temperature sensors, and various other types. Like embedded control devices, I/O devices operate on proprietary manufacturer operating systems, typically built on commodity components with custom elements.

### 1.3 Operational Technology Transformation

Operational Technology (OT) has undergone a significant transformation over time, integrating Information Technology (IT) functionalities into traditional physical systems and replacing or enhancing conventional mechanical control mechanisms. This evolution has been driven by improvements in cost-effectiveness and performance resulting in the emergence of various smart technologies such as smart grids, smart transportation, smart buildings, smart manufacturing, and the Internet of Things (IoT). While these advancements enhance connectivity and the criticality of these systems, they also intensify the need for adaptability, resilience, safety, and security.

The engineering of OT systems continues to advance, offering new capabilities while upholding traditional long-life cycles. The integration of IT functionalities into physical systems can lead to unforeseen behaviours, which necessitate evolving engineering models and analyses. These models now encompass aspects such as safety, security, privacy, and environmental impact interdependencies.

Despite the opportunities technological advancements bring, significant threats loom. There was a widespread misconception that industrial environments were immune to cyber threats. Beliefs included the idea that industrial plants were isolated from the internet, firewalls alone sufficed for protection, hackers remained ignorant of industrial systems, and industrial facilities were unlikely targets. Some even relied solely on plant safety systems for protection, overlooking comprehensive cybersecurity measures.

As digitalization advances, the visibility and surface exposure of OT networks have expanded significantly. This elevated connectivity increases the likelihood of cyber incidents affecting critical infrastructure. OT systems now share vulnerabilities similar to their IT counterparts due to the growing

convergence and connectivity between these two realms.

This convergence introduces unique challenges, particularly in prioritizing cybersecurity efforts effectively. OT and IT environments have distinct knowledge requirements and lifecycles, making it complex to establish risk reduction priorities. Furthermore, a cybersecurity incident in an industrial setting can have tangible impacts beyond the digital realm, potentially causing environmental damage, jeopardizing public health, disrupting essential services, and more.

The integration of OT and IT, the growing demand for connectivity, and the exposure of traditional IT weaknesses in critical facilities present formidable challenges. High-profile cybersecurity incidents have underscored the vulnerability of industrial facilities. State-sponsored groups and criminal organizations have acquired the capability and knowledge to exploit these vulnerabilities, emphasizing the urgent need for comprehensive and adaptive cybersecurity measures.

### 1.4 Difference between IT and OT Cybersecurity

Operational Technology (OT) and Information Technology (IT) represent two distinct realms, each with unique characteristics and cybersecurity priorities. In the IT landscape, the focus revolves around modern, cloud-based devices, emphasizing the C-I-A triad—Confidentiality, Integrity, and Availability. Contrastingly, OT deals with a diverse array of devices, including legacy systems such as Windows XP or Windows 7, embedded devices like PLCs, controllers, and sensors. OT's paramount concern is ensuring the safety of personnel and property, with priorities structured around Safety, Reliability, and Productivity. The table below highlights the nuanced differences between IT and OT cybersecurity, shedding light on their divergent security approaches, protection priorities, responses to distinct threat landscapes, and variations in cybersecurity frameworks.



Aspect	IT Cybersecurity	OT Cybersecurity
<b>Devices</b>	Modern, updated, OS-based, or cloud-based devices in the IT stack.	Diverse devices, including old Windows versions (e.g., Windows XP or Windows 7), embedded devices (PLCs, controllers, relays, sensors), industrial networking equipment, etc.
<b>Security Approach</b>	Traditional IT security processes and technology.	Requires a specialized approach due to unique devices and operational requirements.
<b>Protection Priorities</b>	Guided by the C-I-A triad: Confidentiality, Integrity, and Availability.	Prioritizes Safety, Reliability, and Productivity, with a focus on protecting people, property, and process control systems.
<b>Risk Management</b>	Adheres to the C-I-A triad and focuses on data security and confidentiality.	Adopts the Safety-Reliability-Productivity (SRP) model, emphasizing safety, operational reliability, and productivity.
<b>Safety Priority</b>	Emphasizes data security and confidentiality.	Prioritizes the safe operation of facilities, protecting life and property from potential catastrophic harm.
<b>Productivity Priority</b>	Addresses concerns over slowed or disrupted operations due to cyberattacks.	Acknowledges the risk of operational disruptions impacting production and business continuity.
<b>Reliability Priority</b>	Critical for system reliability in the face of cyber threats.	Significant emphasis on system reliability, as disruptions can lead to substantial financial losses and operational challenges.
<b>Frequency of Attacks</b>	More exposed to the internet, faces attacks at a higher frequency.	Less exposed to the internet, faces attacks at a lower frequency, but potential consequences are severe.
<b>Security Patching</b>	Frequent patching in response to regular updates and vulnerabilities.	Patching is less frequent in OT environments, with a focus on stability and avoiding disruptions to critical operations.

## 1.5 Purdue Model

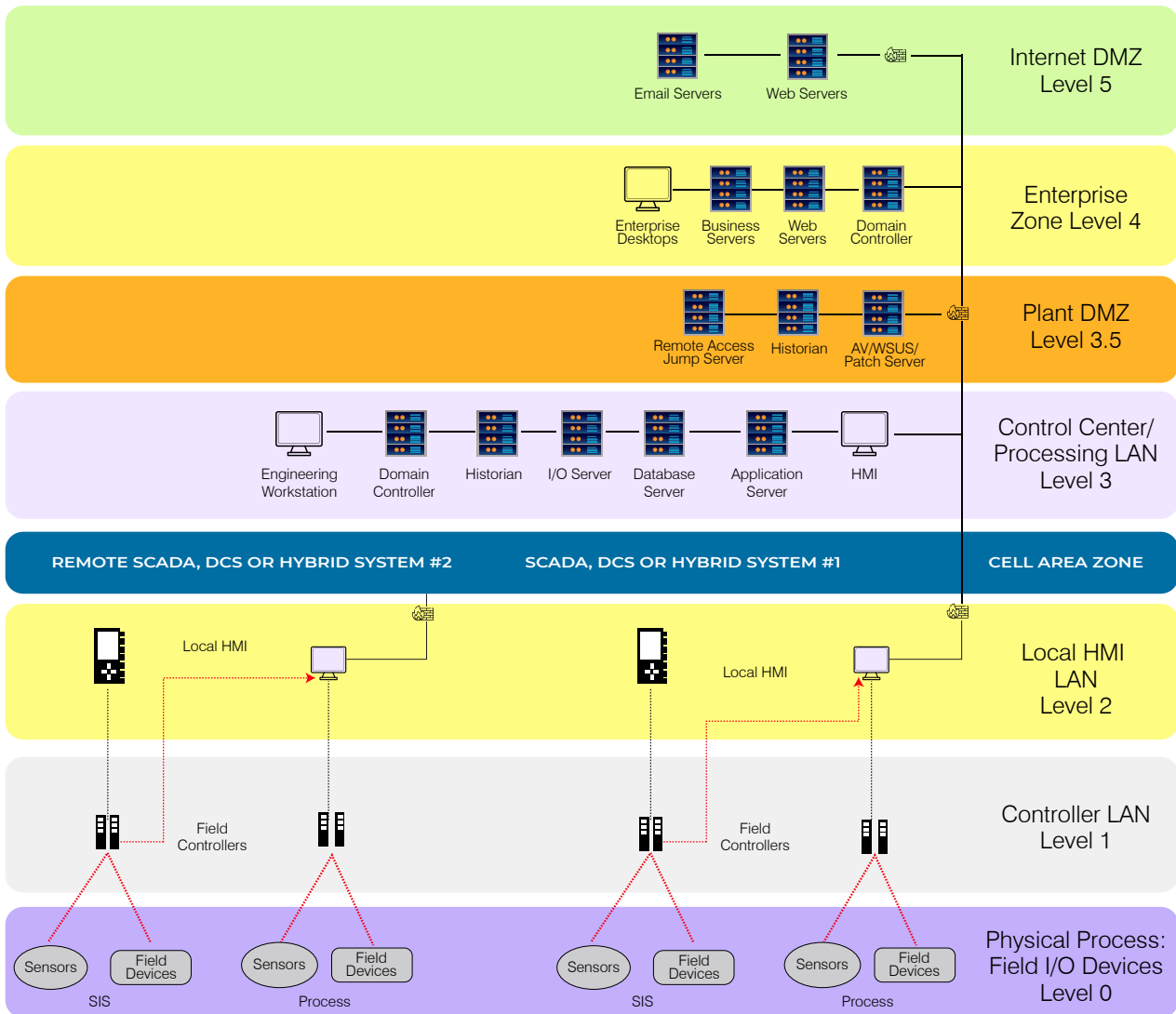
The Purdue model serves as a structural framework for securing Industrial Control Systems (ICS) by focusing on the segmentation of physical processes, sensors, supervisory controls, operations, and logistics. As an integral part of the Purdue Enterprise Reference Architecture

(PERA), this model was specifically devised as a reference model for data flows within computer-integrated manufacturing (CIM) scenarios, where plant processes are fully automated. Functioning as the standard for constructing ICS network architecture, the Purdue model facilitates Operational Technology (OT) security by strategically separating the layers of the network to

maintain a hierarchical flow of data. This model delineates the interconnections among the typical elements of an ICS architecture, categorizing them into six zones that encompass both Information Technology (IT) and OT systems. When correctly implemented, the Purdue model

establishes an “air gap” between ICS/OT and IT systems, effectively isolating them. This isolation enables organizations to enforce robust access controls without impeding business operations, making it a foundational element for safeguarding ICS against malware and other security threats.

Fig 1: Basic Purdue Architecture – power sector



Commencing from the topmost level and descending in a hierarchical order:

**LEVEL  
4/5**

**Enterprise Zone**

This zone serves as the apex, housing the conventional IT network where pivotal business functions unfold. Here, enterprise resource planning (ERP) systems orchestrate manufacturing operations, overseeing production schedules, material utilization, shipping, and inventory levels. Disruptions within this zone can have severe consequences, leading to extended downtime, economic damage, critical infrastructure failure, or potential revenue loss.

### **Demilitarized Zone (DMZ)**

**LEVEL  
3.5**

Situated below the Enterprise Zone, the DMZ incorporates essential security systems like firewalls and proxies. It plays a crucial role in preventing lateral threat movement between IT and OT. As automation prompts increased bidirectional data flows between OT and IT, this convergence layer provides a competitive advantage but introduces cyber risks if a flat network approach is adopted.

### **Operations Systems Zone**

**LEVEL  
3**

Moving down the hierarchy, this zone houses customized OT devices responsible for managing production workflows on the shop floor. It includes Manufacturing Operations Management (MOM) systems, Manufacturing Execution Systems (MES), and Data Historians. Disruptions in this zone, akin to Levels 4 and 5, can result in economic damage, critical infrastructure failure, safety risks, or revenue loss.

### **Control Systems Zone**

**LEVEL  
2**

The next level accommodates systems supervising, monitoring, and controlling physical processes. It encompasses Supervisory Control and Data Acquisition (SCADA) software, Distributed Control Systems (DCS), and Human-Machine Interfaces (HMIs). These systems are pivotal for basic controls and monitoring.

### **Intelligent Devices Zone**

**LEVEL  
1**

Descending further, this zone comprises instruments sending commands to devices at Level 0. Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs) play essential roles in monitoring and adjusting automated or human-input processes.

### **Physical Process Zone**

**LEVEL  
0**

At the base of the hierarchy, Level 0 involves sensors, actuators, and machinery directly engaged in physical processes. Modern sensors in this zone often communicate directly with monitoring software in the cloud via cellular networks, showcasing the integration of physical processes with advanced technologies.





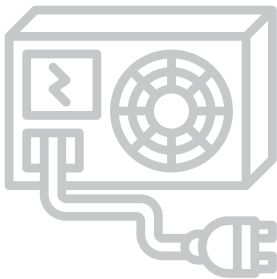
02

Challenges &  
Opportunities for  
Innovation

02

# Challenges & Opportunities for Innovation

Multiple deliberations organized by NCoE brought to light the key challenges faced by industries in implementing the OT security. These sector-specific challenges offer valuable insights for entrepreneurs and researchers entering the OT security ecosystem. Below are a few identified challenges and highlights of use cases that serve as strategic entry points for those looking to make meaningful contributions to this dynamic and critical field.



## 2.1. Power Sector

The implementation of operational technology brings various security concerns ranging from encryption issues to the absence of standardized frameworks, necessitate innovative solutions. Here, we will explore the challenges encountered in securing OT within the power sector, followed by potential use cases to address these identified needs.

### A. Challenges

- a. Encryption of OT data will help improve security, but it brings in challenges with latency and interoperability of devices from different vendors as protocols may differ.
- b. Although there is a proper framework/ guidelines or policy for OT security in some sectors, but the same is yet to be introduced in other sectors. Once the same is available, it will be comparably easy for different organizations to establish consistent security measures and effectively respond to security incidents.



- c. Relying solely on perimeter-based security measures possess a challenge for organizations as it may not provide adequate protection against internal threats or attacks that originate from within the network perimeter.
- d. Identifying vulnerabilities and access points for potential intrusions is also a challenge as it requires good identification of the Electronic Security Perimeter (ESP) and continuous monitoring & analysis of network traffic, security logs, as well as regular vulnerability assessments and penetration testing.
- e. Mapping business processes to critical and non-critical areas is challenging as it requires a deep understanding of the business operations, potential impact of security incidents, and effective prioritization of security controls and resources.
- f. Knowing the underlying ICT asset of Critical Information Infrastructure is of prime importance, but use of legacy OT systems with primitive network infrastructure is posing a challenge in integration of Asset Discovery tools.
- g. With present requirement of agile, lean organization and the advent of concept of Work from Home, there is the challenge of securing OT infrastructure in case of allowing users remote access to OT systems.

## B. Potential Use Cases:

- a. Tools and methodologies to identify and classify critical information infrastructure (CII) that need to be protected.
- b. Technology to map appropriate security standards (e.g., 62443, 20243) with the requirement of specific sectors to make informed decisions.
- c. Certification services/ labs to certify suppliers as compliant with the ISA IEC 62443 standards as CEA mandated the certification.
- d. Developing Deception technique and tools for smooth integration into OT architecture.
- e. Developing use case for implementation of Zero-Trust solutions for east-west and North-south traffic in OT.
- f. Developing effective solutions for detecting and isolating compromised systems.
- g. Developing training modules on the list of the topics provided in the CEA guidelines to train the workforce.
- h. Hardening solutions for legacy systems to improve security posture of older, potentially vulnerable systems that cannot be easily replaced or updated.
- i. Developing indigenous SCADA/OT systems with customizability and cost-effectiveness. Also reduces dependency on foreign technologies and potential supply chain vulnerabilities.
- j. Technology to identify vulnerabilities in embedded devices which are in-built in OT devices and communicating them to relevant parties.
- k. Testing solutions to identify malware and malicious code before deployment of any software/hardware in power sector industries which was mandated by CEA in 2020.
- l. Tools for intrusion detection at the sensor and actuator level to detect APTs.





## 2.2. Oil & Gas Sector

As a critical industry sector, Oil & Gas sector grapples with distinctive challenges in securing the operational technology landscape. Here, we will explore the challenges encountered in securing OT within the O&G sector, followed by potential use cases to address these identified challenges.

### A. Challenges

- a. Low visibility into the systems, which can make it difficult to detect security breaches or vulnerabilities.
- b. Integrating the new technology with the existing legacy systems is challenging because of which the technology adoption is slow.
- c. Obsolete and vulnerable systems can be another challenge, as some systems may be outdated and lack the necessary security features to protect against evolving cyber threats.
- d. There is also a dependency on OT OEMs, as they play a significant role in maintaining and securing their products, which can make it difficult for organizations to implement their own security measures.
- e. Vulnerability assessment and remediation can be difficult in OT systems, as in most cases it requires plant shutdown for these activities and there may be very limited options for testing before patching vulnerabilities.
- f. A comprehensive asset inventory is crucial for OT security, as it allows organizations to track and monitor their systems for any abnormalities or security breaches.
- g. The lack of OT specific threat intelligence services can be a challenge.

### B. Potential Use Cases:

- a. Development of digital twins of OT systems to create virtual replicas for active cyber security assessments, simulations, and exercises.
- b. Technology for compensatory controls for the vulnerable systems, as to monitor and manage compensatory controls to ensure their effectiveness and identify any weaknesses or gaps in security.
- c. Secure remote access tools such as Virtual Desktop Infrastructure (VDI) to enable secure access to OT systems from remote locations.
- d. Protection against ransomware attacks by implementing innovative data backup solution with ransomware protection.
- e. Development of forensic expertise in OT to investigate and respond to security incidents and breaches.
- f. Implementation of passive asset inventory tools to keep track of all assets and devices on the OT network.

- g. Secure patch management solutions to keep OT systems up to date with the latest security patches and updates.
- h. Development of secure communication protocols for IoT devices involved in OT systems that are not within the perimeter of the security zone.
- i. Establishment of an OT SOC (Security Operations Centre) to provide round-the-clock monitoring and incident response for OT networks.
- j. Development of secure methods or solutions for integrating OT data with IT systems to enable data-driven decision making.



### 2.3. Manufacturing and Aviation sectors

Identifying vulnerabilities, securing legacy systems, and adapting to evolving digital environments further compound the security landscape of manufacturing and aviation sectors. The subsequent pointers outline challenges and the potential use cases pertaining to OT security in these industries.

#### A. Challenges

- a. The lack of visibility into OT networks and protocols poses a significant challenge as it limits the ability to detect and respond to potential cyber threats and operational issues effectively.
- b. Configuration errors in OT systems poses vulnerabilities that can be exploited by attackers to gain unauthorized access.
- c. The effective management of remote devices is challenging as they may be in inaccessible areas, making it difficult to monitor and maintain their security.
- d. Absence of proper logging and monitoring pose challenge in identifying and responding to security incidents promptly.
- e. Lack of two-factor authentication for vendor access and movement increases the risk of unauthorized access.
- f. Lack of established procedures and frameworks for effectively responding to and recovering from cyber-attacks.

#### B. Potential Use Cases:

- a. Develop a comprehensive framework for organizations to establish a structured approach for managing OT security, mitigating risks, and enhancing resilience.
- b. Implement data diodes to provide one-way communication channels, isolating OT systems from external networks and ensuring sensitive information remains secure.
- c. Implement advanced technology solutions to effectively manage the expanding attack surface in OT systems as the number of connected devices increases.

- d. Observability-based security tools to analyse the behaviour of devices and systems, detect anomalies and mitigate attacks.
- e. Passive monitoring tools to identify vulnerabilities from live systems feed.
- f. Remediation playbooks for various common OT attack vectors.



## 2.4 Healthcare sector

Healthcare sector, being diverse and critical in nature as it encompasses multiple stakeholders entails security risks from multiple facets. So securing OT in healthcare becomes a matter of lives, introducing unique challenges that requires comprehensive solutions.

### A. Challenges

- a. The lack of interoperability for the secure exchange of data between different healthcare systems.
- b. Inadequate visibility into the networks poses a challenge for managing medical devices leading to potential security gaps.
- c. Insufficient network segmentations, coupled with insecure communication protocols leads to unauthorized access and data interception.
- d. The absence of a single international standard akin to ISO 27001 for healthcare systems creates challenges in achieving consistent cybersecurity compliance across diverse regulatory frameworks.

### B. Potential Use Cases:

- a. Develop a comprehensive platform that enables real-time monitoring, identification, and management of all connected medical devices, ensuring a secure and well-monitored healthcare environment.
- b. Develop a framework to assign reputational scores to healthcare data, enabling dynamic classification and integration with segmentation solutions. This ensures adaptive access controls





03

Research  
Productization  
Initiative – IDS for  
OT Environment



03

# Research Productization Initiative – IDS for OT Environment

## 3.1. Background

With the aim of fostering innovation and research productization, NCoE, through its SCADA/OT Security Acceleration Program initiative, facilitated collaboration between Dr. Shankar Sriram from SASTRA Deemed University and Infopercept Consulting to commercialize the JARA – the open-source IDS for cyber-physical systems developed by Prof. Sriram as an overall end-deliverable product for the project funded by the Ministry of Electronics and Information Technology (MeitY), Govt. of India.

The IDS technology functionally utilizes threat intelligence for signature-based threat detection and machine learning models for identifying unseen exploits, thereby raising alerts for zero-day intrusion attempts.

Building upon this foundational capability, Infopercept enhanced the IDS ecosystem to increase its global market acceptance, refining its go-to-market strategy and execution. The company successfully developed a global OT security product from India, catering to both the domestic market and the global market.

NCoE played a crucial role in facilitating and deliberating on the commercial equation,

enabling the technology transfer. These deliberations successfully led the JARA-IDS R&D project funded by MeitY, towards adoption and its transformation into commercial technology.

## 3.2. Product Description

The focal point of this technology transfer is the OT IDS sensor, an integral component of Invinsense OT security services offered by Infopercept Consulting. This sensor monitors the network traffic and system activities within Operational Technology (OT) environments, with a focus on detecting anomalies, intrusions, and potential security threats. It is designed

The **“Make in India”** approach in OT security ensures that solutions are tailored to the unique challenges of the Indian critical infrastructure, thereby enhancing reliability and security.



to understand and analyze the industrial communication protocols commonly used in OT environments, such as Modbus, DNP3, OPC, and others.

The sensor employs anomaly detection techniques to identify deviations from normal network behavior. This can include a typical traffic pattern, unusual device behaviors, or configuration changes. It uses predefined signatures and rules to detect known threats, including malware and attack patterns commonly seen in OT environments. When the sensor detects a potential security threat or anomaly, it generates alerts and notifications, allowing security teams to respond promptly to potential incidents.

### 3.3. How will it Benefit the Indian OT Security/ Global OT Security Space?

The technology transfer holds significant implications for both Indian OT security and the global OT security landscape. By leveraging the indigenous development of the OT IDS technology, India can strengthen its cybersecurity capabilities, particularly in critical sectors such as power, energy, manufacturing, automobiles, pharmaceuticals, and transportation. The “Make in India” approach in OT security ensures that solutions are tailored to the unique challenges of the Indian critical infrastructure, thereby enhancing reliability and security. Globally, this technology transfer contributes to diversifying the sources of OT security solutions and promotes trust in products proven effective in India on a global scale. It represents a collaborative stride towards creating a secure and resilient OT ecosystem worldwide.









04

# Indian Startup Ecosystem





04

# Indian Startup Ecosystem

As a recognized National Centre of Excellence in Cybersecurity Technology Development and Entrepreneurship, our primary mission is to drive innovation and facilitate the development of security capabilities within the country. In alignment with this goal, NCoE has successfully accelerated a diverse array of start-ups. These start-ups, carefully selected and nurtured within our ecosystem are at the forefront of developing indigenous products aimed at addressing some of the challenges within the OT security landscape. By providing these emerging startups with a dedicated platform and unique opportunities, NCoE is actively contributing to the growth of a robust ecosystem, empowering these start-ups to make impactful strides in the realm of OT security.

## 4.1. Arishti Info Labs Private Limited



About: Arishti Info Labs founded in 2020 is led by Hardik Tarpara, who is an experienced professional with four years of experience in IoT Development and Security. The

company is dedicated to safeguarding the industrial civilization from cybersecurity threats and risks. The name 'Arishti' is derived from Sanskrit signifying security or safety. They have assembled a team of certified experts on ICS (Industrial Control System), SCADA (Supervisory Control and Data Acquisition), OT (Operational Technology) and cybersecurity. At Arishti, their mission is to instill trust in the industrial society by addressing mission-critical and cybersecurity issues. Arishti is widely recognised as the trusted ICS and SCADA

In India, more than 6 lakh manufacturing industries exist, out of which **70K+ utilize OT** network-based technologies, the adoption of Dorje is expected to increase due to growing adoption of IIoT.

security partners, dedicated to ensuring the integrity of operational data. The company has successfully deployed its solution for CPS environment of various critical sectors of FMCG, Defence and Manufacturing.

**Product: DORJE**

Product Description: Dorje is an agentless device designed to provide comprehensive visibility, monitoring, and detection capabilities to safeguard industries from cyber threats. With full visibility into assets and risks across the IoT/OT environment, it offers continuous monitoring for threats and vulnerabilities using behavioral analytics and threat intelligence. In India, more than 6 lakh manufacturing industries exist, out of which 70K+ utilize OT network-based technologies, the adoption of Dorje is expected to increase due to growing adoption of IIoT.

**4.2. GRIDsentry Private Limited**



About: GRIDsentry Private Limited founded in 2021 and led by Devika Jay, who is an experienced professional with a decade of experience in Power Distribution and Transmission field is a Powergrid Cybersecurity startup focusing on securing electric powersubstationsfromcyberattacks. They provide intrusion protection, detection and mitigation solutions based on defensive deception technologyandAI/MLtechniques. The company has successfully deployed its solution for CPS environment of various critical sectors of Power and Energy.

**Product: Ghide**

Product Description: The high interactive deception for Intrusion Protection System employs a defensive deception-based

technology to replicate an OT network and integrate it into the real network, to deviate attackers from the actual system. This prevents the flow of critical messages in the network to select devices, prevents attack by luring the attacker to the decoy system rather than the actual system, replicates the behaviour of a real OT network and interact with the attacker to give the operator buffer time for implementing mitigation steps and raises an alarm in case of a detected attack.

**Product: Gids**

Product Description: Intrusion detection system for realtime and forensic analysis · Perform deep packet inspection of data packets in the network. Statistical, data and physics-driven anomaly identification of packets to detect an attack. Help network operators distinguish major and minor anomalies and generate an alarm for faster identification of attacks. · Have a historian for storing and processing data for forensic analysis.

**4.3. Saptang Labs Private Limited**

About: Saptang Labs was founded in 2021 with the vision of filling the critical gaps in the cybersecurity preparedness of the customers using innovative products and services



leveraging advances in the field of artificial intelligence and machine learning, and is led by Sai Krishna B, who is an experienced professional with 15 years of experience in multiple technology-driven companies. They work with government departments, law enforcement agencies and private sector companies to help them boost up their capabilities. They customize their offerings as per the customer needs. Their OT firewall solution is suitable for adoption

in multiple critical sectors like Power, Energy and Manufacturing.

**Product: FilterCoffee - SCADA OT Firewall Solution**

Product Description: The intelligence collected about the threat actors is used by Sarvagya or Excalibur, to power the fully indigenous SCADA and OT Device firewall solution (FilterCoffee) which is powered by indigenously developed Shakti Processor and can be deployed easily for defending the OT assets from cyber-attacks.

**4.4. Infopercept Consulting Private Limited**

# Infopercept

About: Infopercept Consulting Private Limited is founded in 2014 and led by Jaydeep Ruparelia, who is an experienced

professional with over 15 years of experience in cybersecurity is serving global clients in all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools.

**Product: Invisense OT Security Solution**

Product Description: Invisense OT Security Solution a comprehensive suite of services including Invisense Firewall and Invisense OTIDS, to address the threats faced by the global OT systems. The OTIDS uses predefined signatures and rules to detect known threats, including malware and attack patterns commonly seen in OT environments. When the sensor detects a potential security threat or anomaly, it generates alerts and notifications, allowing security teams to respond promptly to potential incidents.







05

Initiatives





05

## Initiatives

Recognizing the critical role played by OT in the contemporary industrial landscape and with an objective focused on innovation, research, collaboration, and tangible advancements in SCADA/OT security technology within the country, NCoE, in partnership with Infopercept Consulting Pvt. Ltd. and C-DAC (Centre for Development of Advanced Computing) launched the SCADA/OT Security Acceleration Program on November 23, 2022.

The primary objectives of the program were:

- Accelerate technology, product, and solution development in OT security.
- Attract attention of engineering minds and assist Start-ups.
- Identify use cases for indigenous development and research intervention.
- Create visibility, awareness, and adoption about research with aim of leading translation of research effort into market ready products.
- Accelerate start-ups ready to venture in indigenization of the SCADA/OT Security.

### 5.1 Leader's Perspective: Setting the Path for Development of OT Security in India

Gracing the launch of the program, Dr. Sanjay Bahl, DG, CERT-In emphasized that, "SCADA/OT Cyber Security is significant for the country's infrastructure, like aerospace, power, oil & gas, food processing, and multiple other industries. The threat vectors in the cyberworld can weaponize OT environments and put nations critical infrastructure at risk. The work being undertaken by various Govt. and Industry bodies in SCADA/OT is towards building robust and resilient SCADA Cyber security solutions and services. The efforts of DSCI-NCoE in nurturing innovative minds to solve key problems of SCADA/OT Security is appreciated."

Dr. S D Sudarsan, Executive Director, C-DAC, highlighted that "Real-time and non-real-time issues during IT/OT integration, presence of multi-generation hardware/software, and diversity of priority between IT-OT are key focus areas for strategic sectors in terms of confidentiality, availability, integrity, privacy, and safety. He also highlighted the need to collaborate and co-create across the industry, academia, research, government as well as professional organizations such as DSCI."



Mr. Vinayak Godse, CEO, DSCI, said, “There is an urgent need to attract engineering and innovative minds to solve problems in nationally important areas such as SCADA/OT Security. The Acceleration Program is devised to seek contribution from organizations working in critical sectors in creating SCADA/OT security technologies capabilities and enterprise-ready products with the help of start-ups. With the support from MeitY and CERT-In, and partnership with C-DAC and Infopercept, and other industry stakeholders committed to work in the area, the concerted efforts of this Acceleration Program will see emergence of new technology start-ups in this field.”

As a way forward, a series of impactful initiatives were undertaken to accelerate the development of OT security technology to deliberate on the challenges and opportunities within the field.

### **5.2 Workshop on SCADA/OT Security: Empowering India’s Innovation Capability and Research**

In collaboration with Infopercept Consulting Pvt. Ltd., DSCI’s NCoE organized a day-long

workshop in Ahmedabad. Held on March 10th, 2023, the workshop aimed to foster collaboration among stakeholders, including researchers, start-ups, and public sector companies, to enhance India’s capabilities in OT security. The workshop covered the current landscape of SCADA/OT security, international standards/frameworks, and featured panel discussions on challenges and potential use cases in power and energy, oil and gas, aviation, and manufacturing sectors. Sessions on indigenously developed IDS, vulnerability and patch management, and the establishment of a common test bed for start-ups and researchers were also conducted. The workshop witnessed participation from key stakeholders in SCADA/OT security, including Ministry of Power, CERT-IN, ONGC, HPCL, CDAC, IIT Kanpur, VJTI, SASTRA University, GMR, Defentos, Beacon Security, and SIEMENS Technology, India. It provided a platform for knowledge sharing and networking, emphasizing the urgent need for focused attention on SCADA and OT security.



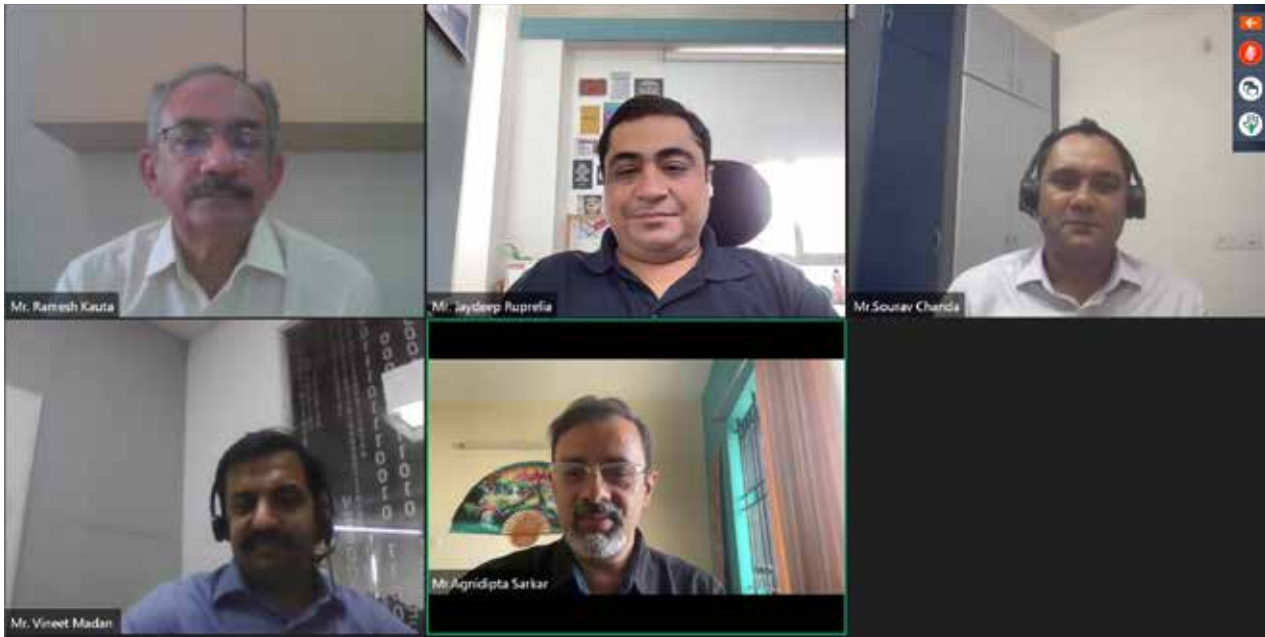
### **5.3 Healthcare Sector Webinar: Challenges and the Future of Healthcare Ecosystem**

A transformative webinar held on September 21<sup>st</sup>, 2023 explored the challenges and future

of the healthcare ecosystem in the context of SCADA/OT security. The discussion delved into the digital transformation of the healthcare sector, cyber-physical systems, emerging technologies, and strategies

for secure implementations. The webinar addressed critical concerns such as cyber threats to medical devices, the impact of 5G technology on security, and the need for standardized data monitoring for Operational Technology (OT) in healthcare. A call for collaboration between the

healthcare sector, pharmaceutical industry, and cybersecurity experts highlighted the session. Overall, the webinar provided strategic insights and proposed innovative solutions to enhance security measures in healthcare.



### 5.4 Hands-on Technology Workshop: Understanding and Dissecting Cyber Physical System Protocols

The hands-on technology workshop, themed “Understanding and Dissecting Cyber Physical System Protocols,” aimed to foster knowledge and interest in OT security among professionals, students, and researchers. Held on March 10th, 2023, the workshop covered ICS cybersecurity landscape, architecture, network resilience, network traffic analysis using tools like

Wireshark, Modbus architecture, and insights into APT groups targeting ICS. The hands-on sessions included live demonstrations, practical exercises on ICS protocol exploitation, and discussions on securing ICS through policies, compliance measures, and best practices. The workshop facilitated networking and collaboration, offering valuable insights into ICS cybersecurity challenges and emphasizing the importance of collaborative efforts in securing critical infrastructure.





06

## Conclusion

The SCADA/OT Acceleration Program exemplified the collaborative spirit fostered by NCoE. Its commitment to facilitating innovation, cultivating cross-sector partnerships, and addressing challenges played a pivotal role in achieving the program's objectives. These objectives included attracting engineering talent and supporting startups, identifying use cases for indigenous development and research intervention, increasing visibility, awareness, and adoption of research to lead the translation of research efforts into market-ready products, and accelerating startups ready to venture into the indigenization of SCADA/OT Security.

Throughout the program's duration, NCoE organized various activities, such as webinars, hands-on technology workshops, and industry-academia interactions. These

efforts aimed at elevating the collective understanding of challenges and potential solutions within the SCADA/OT security domain.

A notable achievement within the program was the smooth technology transfer of the Operational Technology Intrusion Detection System (OT IDS) from SASTRA Deemed University to Infopercept Consulting Pvt. Ltd. This accomplishment, a collaborative effort involving NCoE, academia, and industry, demonstrated the successful translation of research into practical technology adoption.

In essence, the entire acceleration program underscored collaboration and collective progress in laying the groundwork for collaborative excellence in addressing cybersecurity challenges.











The National Centre of Excellence (NCoE) for Cybersecurity Technology Development is a joint initiative between the Ministry of Electronics & Information Technology (MeitY), Government of India, and the Data Security Council of India (DSCI). Its primary objective is to catalyze and accelerate cybersecurity technology development and entrepreneurship within the country. NCoE plays a crucial role in scaling up and advancing the cybersecurity ecosystem, focusing on various critical and emerging security areas. Equipped with state-of-the-art facilities, including advanced lab infrastructure and test beds, NCoE facilitates research, technology development, and solution validation for adoption across government and industrial sectors. Adopting a concerted strategy, NCoE endeavors to translate innovations and research into market-ready deployable solutions, thereby contributing to the evolution of an integrated technology stack comprising cutting-edge, homegrown security products and solutions.


## For more information

scan the code to navigate to the website



 +91-120-4990253 | [ncoe@dsci.in](mailto:ncoe@dsci.in)

 <https://www.n-coe.in/>

 4<sup>th</sup> Floor, NASSCOM Campus, Plot No. 7-10,  
Sector 126, Noida, UP -201303

## Follow us on

 @CoeNational

 nationalcoe

 nationalcoe

 NationalCoE