NTNU | Norwegian University of Science and Technology

Swiss cheese on a cloudy day - Migration of OT functions and systems to the cloud

Vasileios Gkioulos

Associate Professor – NTNU – vasileios.gkioulos@ntnu.no

Product portfolio manager for OT Security – Telenor – vasileios.gkioulos@telenor.no

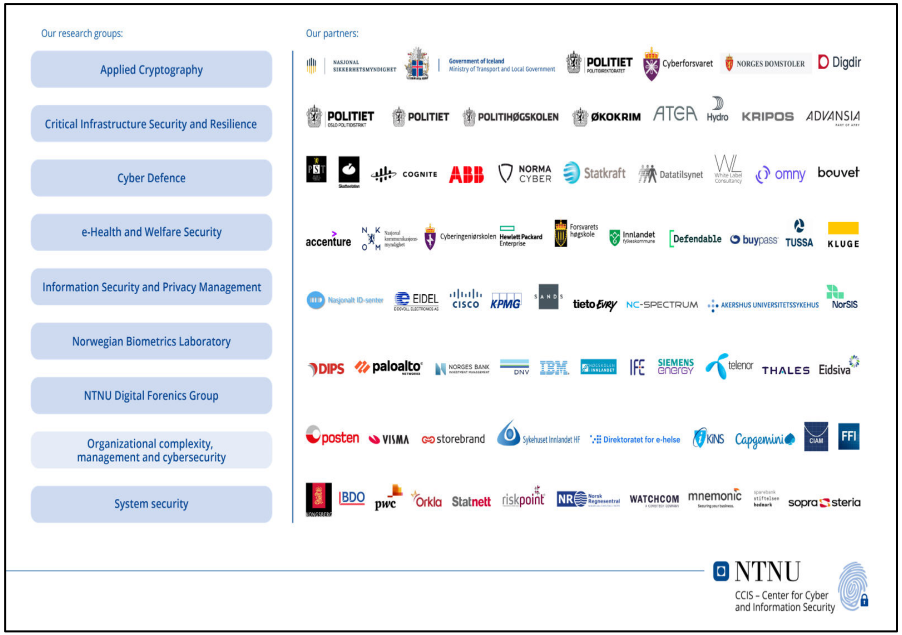
Institutt for informasjonssikkerhet og kommunikasjonsteknologi 2023

CISaR

Critical Infrastructure Security and Resilience

Safeguarding Norway's Critical Societal Functions:
Building Resilience Through Innovation, Research, and Education

NTNU | Norwegian University of Science and Technology

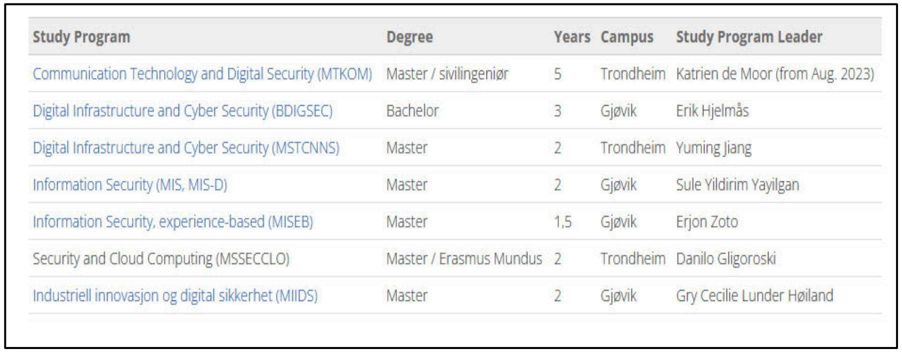


Our research groups:

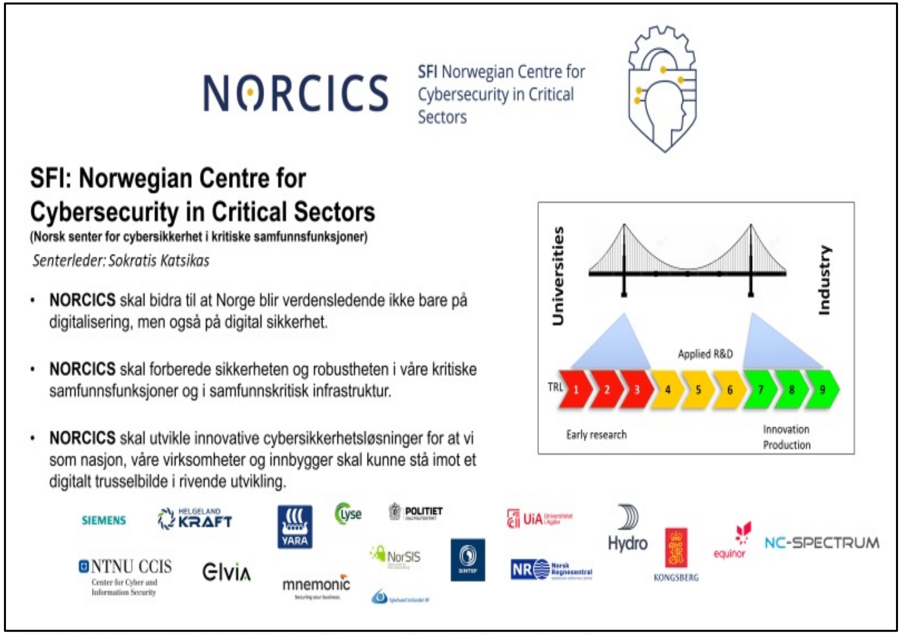
- Applied Cryptography
- Critical Infrastructure Security and Resilience
- Cyber Defence
- e-Health and Welfare Security
- Information Security and Privacy Management
- Norwegian Biometrics Laboratory
- NTNU Digital Forensics Group
- Organizational complexity, management and cybersecurity
- System security

Our partners:

NTNU
CCIS – Center for Cyber and Information Security



Study Program	Degree	Years	Campus	Study Program Leader
Communication Technology and Digital Security (MTKOM)	Master / sivilingeniør	5	Trondheim	Katrien de Moor (from Aug. 2023)
Digital Infrastructure and Cyber Security (BDIGSEC)	Bachelor	3	Gjøvik	Erik Hjelmås
Digital Infrastructure and Cyber Security (MSTCNNS)	Master	2	Trondheim	Yuming Jiang
Information Security (MIS, MIS-D)	Master	2	Gjøvik	Sule Yildirim Yayilgan
Information Security, experience-based (MISEB)	Master	1,5	Gjøvik	Erjon Zoto
Security and Cloud Computing (MSSECCLO)	Master / Erasmus Mundus	2	Trondheim	Danilo Gligoroski
Industriell innovasjon og digital sikkerhet (MIIDS)	Master	2	Gjøvik	Gry Cecilie Lunder Høiland



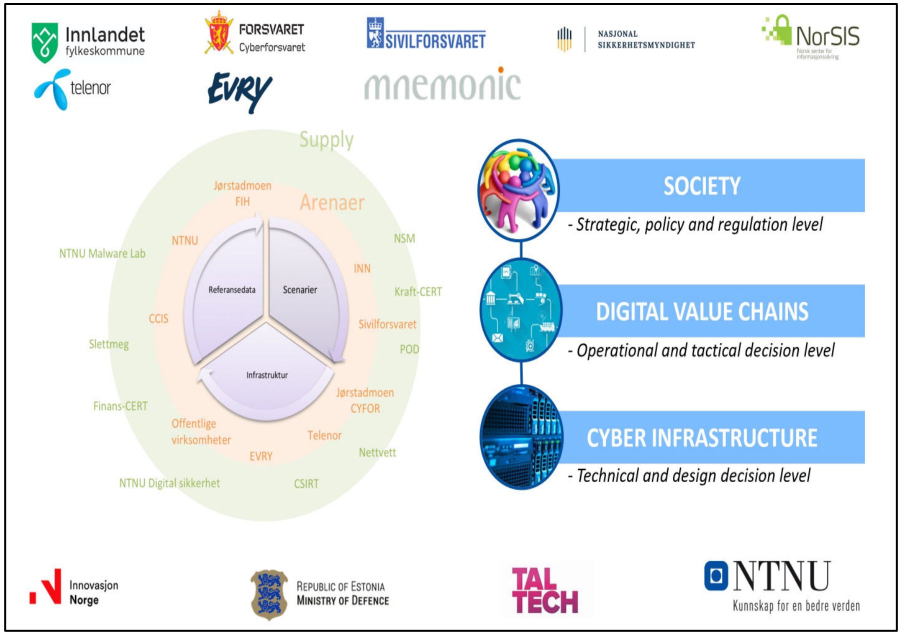
NORCICS SFI Norwegian Centre for Cybersecurity in Critical Sectors

SFI: Norwegian Centre for Cybersecurity in Critical Sectors

(Norsk senter for cybersikkerhet i kritiske samfunnsfunksjoner)

Senterleder: Sokratis Katsikas

- **NORCICS** skal bidra til at Norge blir verdensledende ikke bare på digitalisering, men også på digital sikkerhet.
- **NORCICS** skal forberede sikkerheten og robustheten i våre kritiske samfunnsfunksjoner og i samfunnskritisk infrastruktur.
- **NORCICS** skal utvikle innovative cybersikkerhetsløsninger for at vi som nasjon, våre virksomheter og innbygger skal kunne stå imot et digitalt trusselbilde i rivende utvikling.



SOCIETY
- Strategic, policy and regulation level

DIGITAL VALUE CHAINS
- Operational and tactical decision level

CYBER INFRASTRUCTURE
- Technical and design decision level

NTNU
Kunnskap for en bedre verden

The Critical Infrastructure Security and Resilience (CISaR) Group at IIK

CISaR

Critical Infrastructure Security and Resilience

Safeguarding Norway's Critical Societal Functions:
Building Resilience Through Innovation, Research, and Education

Academic staff

- Prof. Bernhard Hämmerli
- Prof. Siv Hilde Houmb
- Prof. Sokratis K. Katsikas (Group leader)
- Prof. Stephen Wolthusen
- Assoc. Prof. Vasileios Gkioulos
- Assoc. Prof. Georgios Spathoulas
- Assoc. Prof. Ernst Gunnar Gran
- Assoc. Prof. Jia-Chun Lin
- Assist. Prof. Marie Haugli-Sandvik
- Assoc. Prof. Ben Knox – affiliated
- Assoc. Prof. Katina Kralevska - affiliated

Lab Engineer

- Lama Amro

Postdocs & Researchers

- Dr Georgios Aggelinos
- Dr Aida Akbarzadeh
- Dr Ahmed Amro
- Dr Alessio Baiocco
- Dr Georgios Kavallieratos
- Dr Chhagan Lal
- Dr Pankaj Pandey
- Dr James Wright

PhD candidates

- Yana Bilous
- Jessica Barbosa Heluany
- Gizem Erceylan
- Vyron Kambourakis
- Kristian Andreas Kannelønning
- Arne Roar Nygård
- Håvard Ofte
- Aybars Oruc
- Samson Ogheneovo Oruma (HiØF)
- Xhesika Ramaj (HiØF)
- Øyvind Anders Arntzen Toftegaard

Current externally funded research projects

CISaR

Critical Infrastructure Security and Resilience

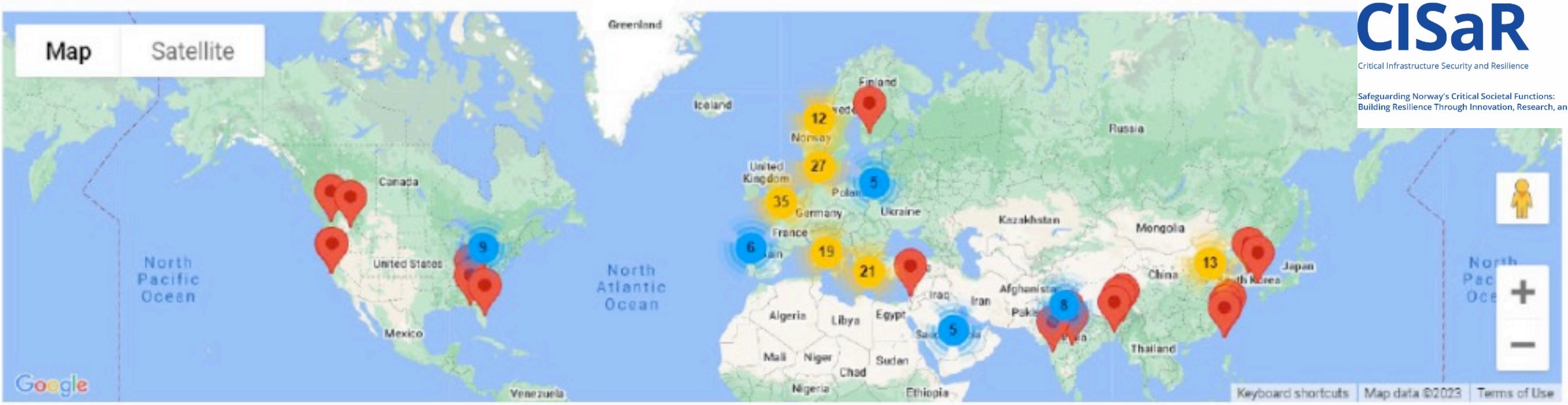
Safeguarding Norway's Critical Societal Functions:
Building Resilience Through Innovation, Research, and Education

- **cPAID:** Cloud-based Platform-agnostic Adversarial aI Defence framework– CPAID
- **CRESCENDO:** Cyber preparedness and RESilienCe of the Energy sector in the NorDic regiOn
- **ELECTRON**: rEsilient and seLf-healed EleCTRical pOwer Nanogrid (Horizon IA)
- **ENFIELD**: European Lighthouse to Manifest Trustworthy and Green AI (Horizon RIA)
- **CERTIFAI**: Agile conformance assessment for cybersecurity CERTIFication enhanced by Artificial Intelligence (Horizon RIA)
- **COMFORTAGE**: Prediction, Monitoring and Personalized Recommendations for Prevention and Relief of Dementia and Frailty (Horizon RIA)
- **CYBERUNITY**: Community for Integrating and Opening Cyber Range Infrastructures that Build an Interoperable Cross-Domain and Cross-Sector Cyber Range Federation (DEP)
- **BRUA**: National Coordination Centre on Cybersecurity – Norway (DEP)
- **FACT**: Federated Advanced Cyber physical Test range (EDF)
- **NEWSROOM**: Adapting Cyber Awareness for Evolving Computing Environments (EDF)
- **CYCLE**: CYberseCurityLEarning: Master's degree in Cybersecurity (ERASMUS+)
- **CORESIM**: Context-Based Real-Time OT-IT Systems Integrity Management (NFR KSPKOMPETANSE23)
- **CybAlliance**: International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (NFR INTPART)
- **RECYCIN:** Reinforcing competence in cybersecurity of critical infrastructures: a Norway-US partnership (NFR INTPART)
- **CIRMAN**: Circular Manufacturing research and educational collaboration with India and Japan (NFR INTPART)
- **PowerDig**: Digitalization of short-term resource allocation in power markets (NFR ENERGIX-Stort program energi)
- **Nemonoor -** en nasjonal hub for kunstig intelligens. European Digital Innovation Hub (DEP)

CISaR
Critical Infrastructure Security and Resilience

Safeguarding Norway's Critical Societal Functions:
Building Resilience Through Innovation, Research, and Education

Network



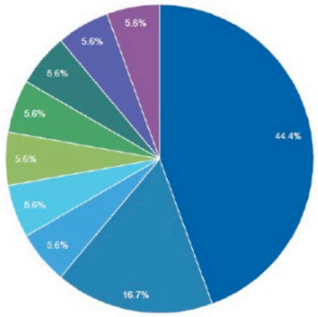
Key metrics

567
Publications

240
Institutions

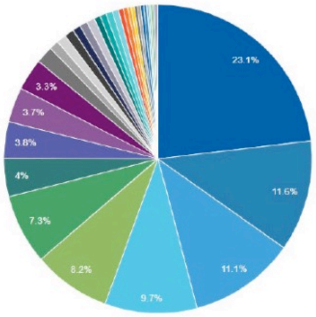
590
Persons

Publications for 2023



Norway
Greece
Turkey
Belgium
United States
Italy
Germany
Canada
Spain

Co-authors grouped by country

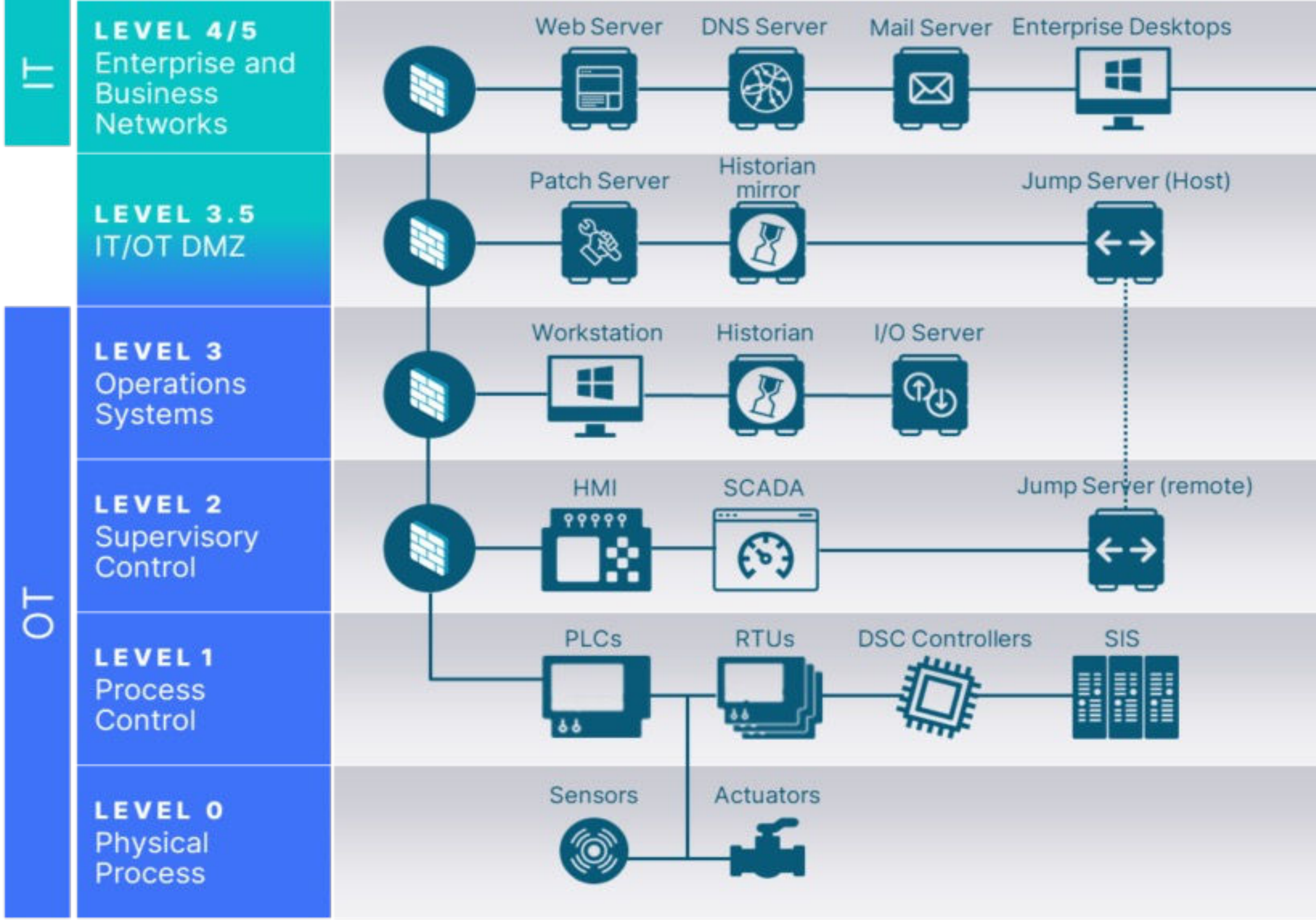


Norway
Greece
China
United States
India
Germany
United Kingdom
Spain
Canada
Italy

IT vs OT

Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of **data or information**

Programmable systems or devices that interact with the **physical environment** (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events.



IT

OT

LEVEL 4/5
Enterprise and Business Networks

LEVEL 3.5
IT/OT DMZ

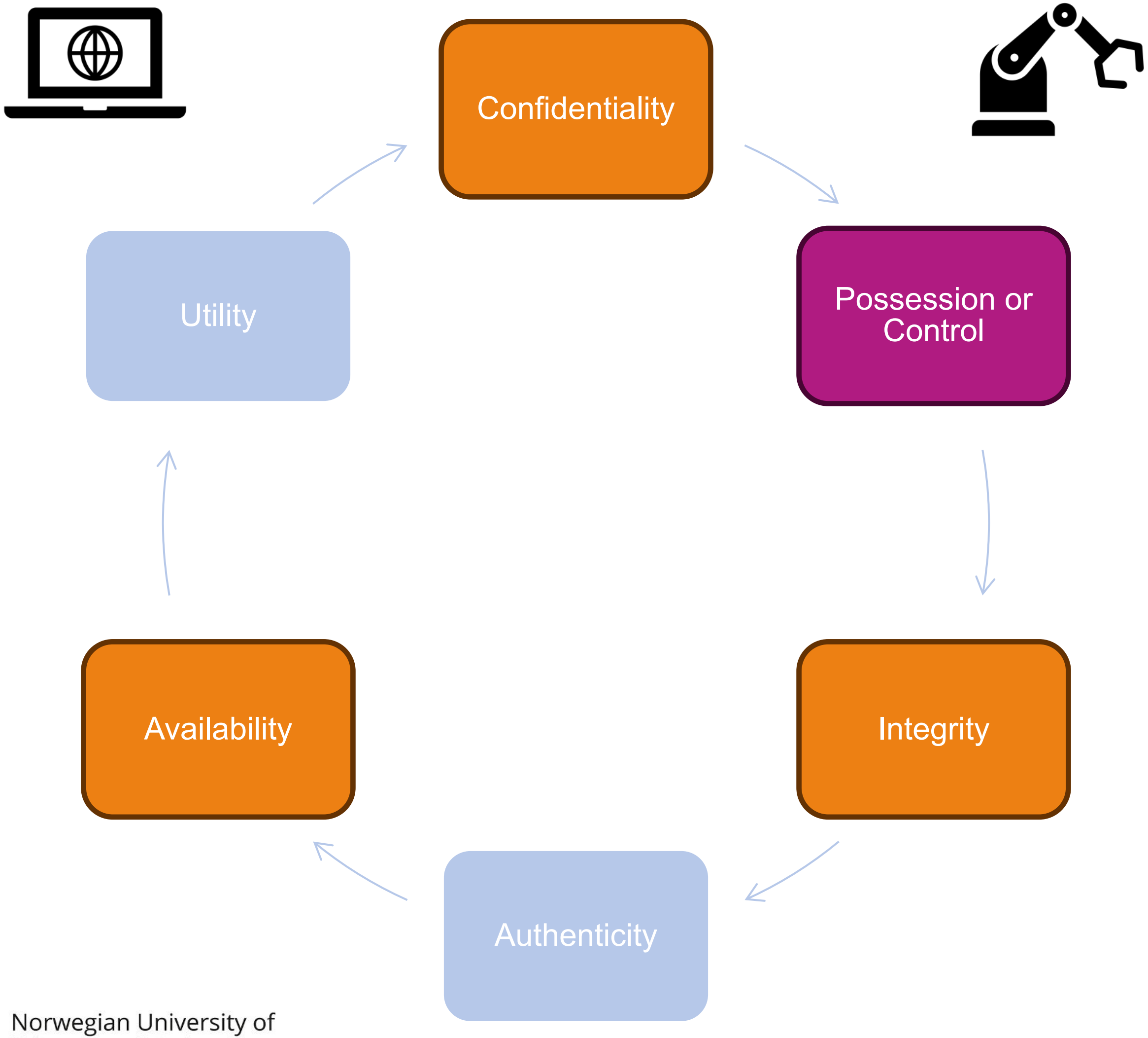
LEVEL 3
Operations Systems

LEVEL 2
Supervisory Control

LEVEL 1
Process Control

LEVEL 0
Physical Process

IT vs OT



Confidentiality

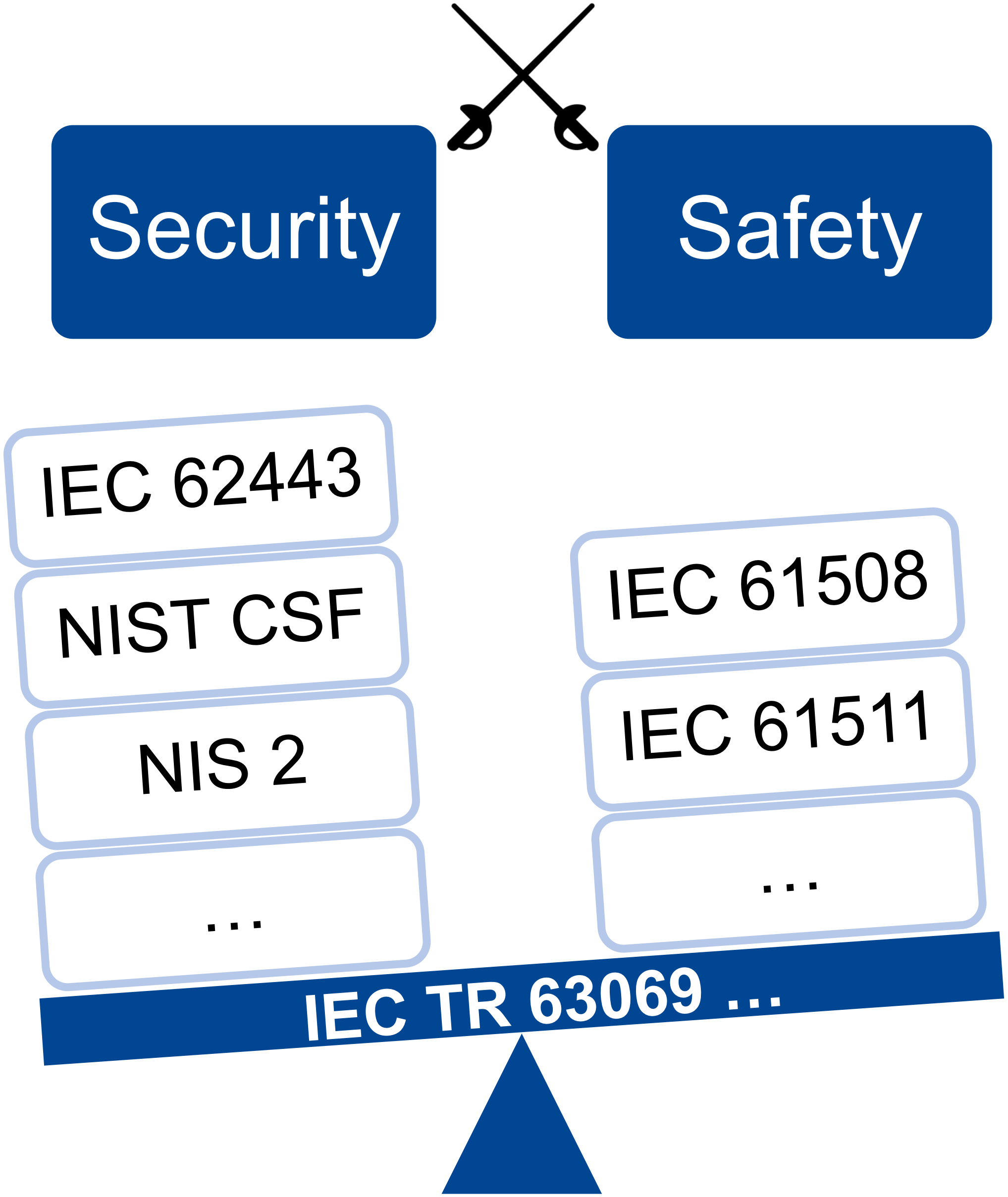
Possession or Control

Integrity

Authenticity

Availability

Utility



Security

Safety

IEC 62443

NIST CSF

NIS 2

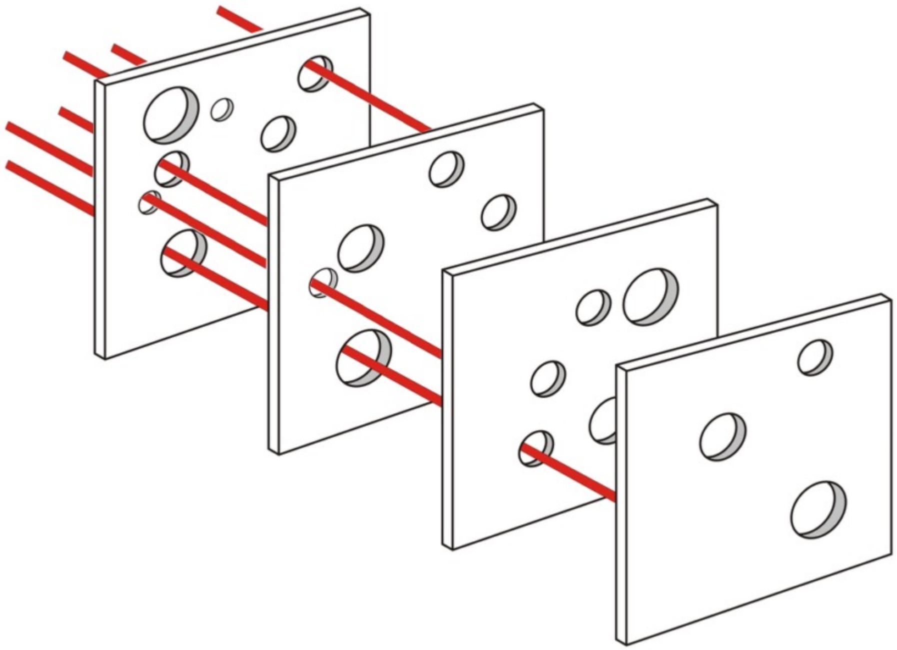
...

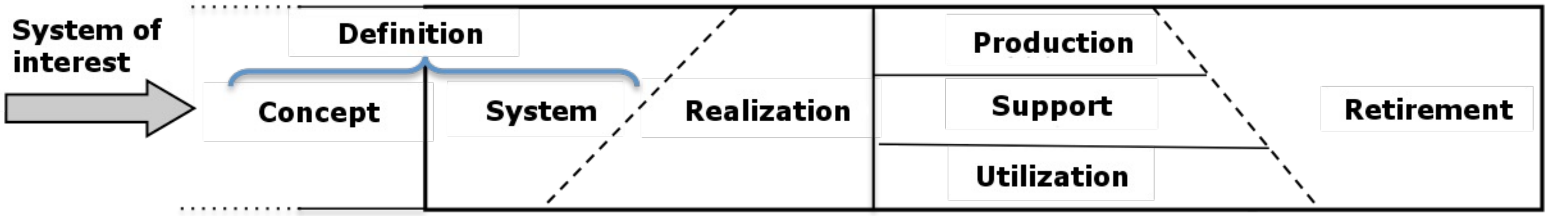
IEC 61508

IEC 61511

...

IEC TR 63069 ...





System of interest

Definition

Concept

System

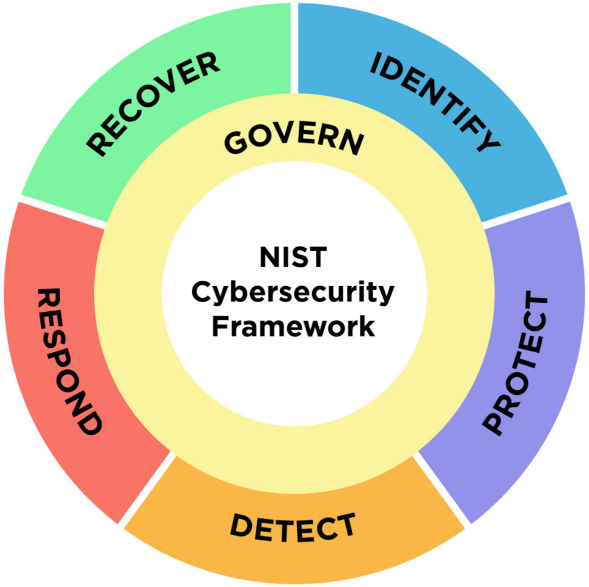
Realization

Production

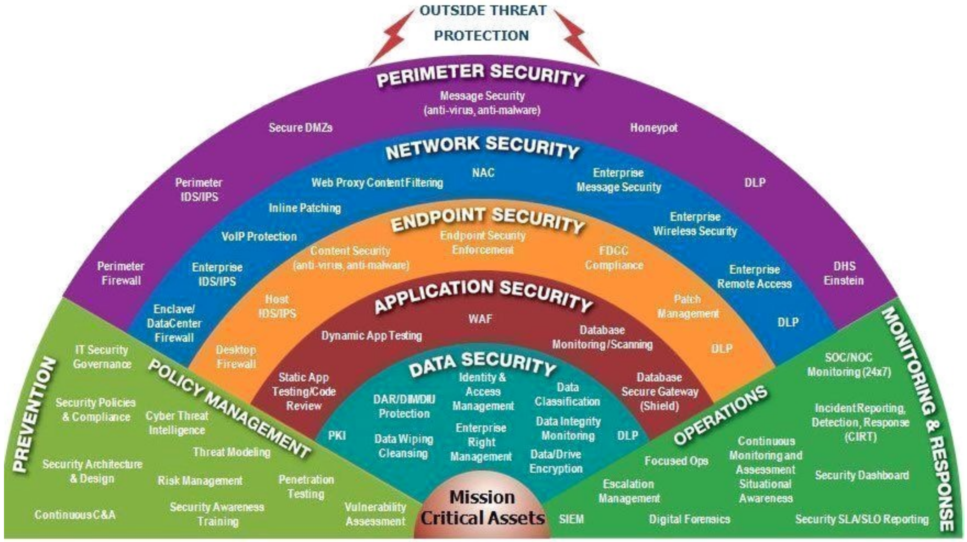
Support

Utilization

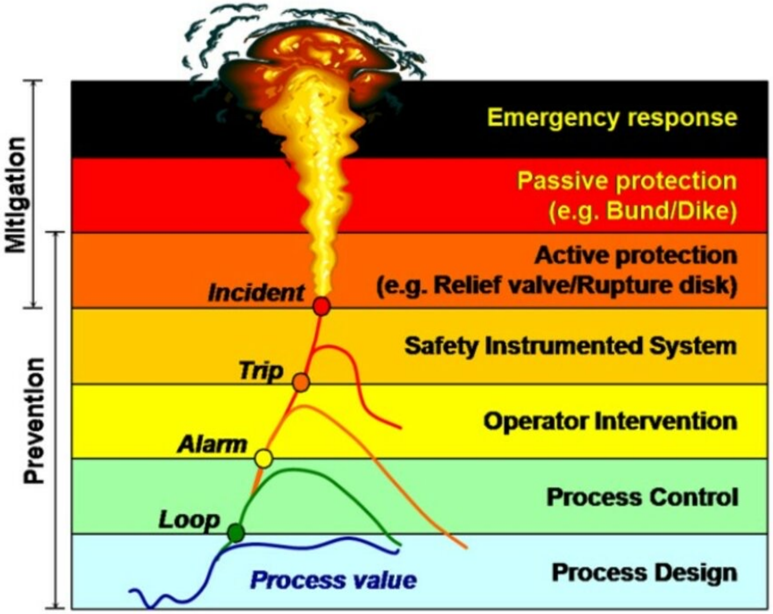
Retirement



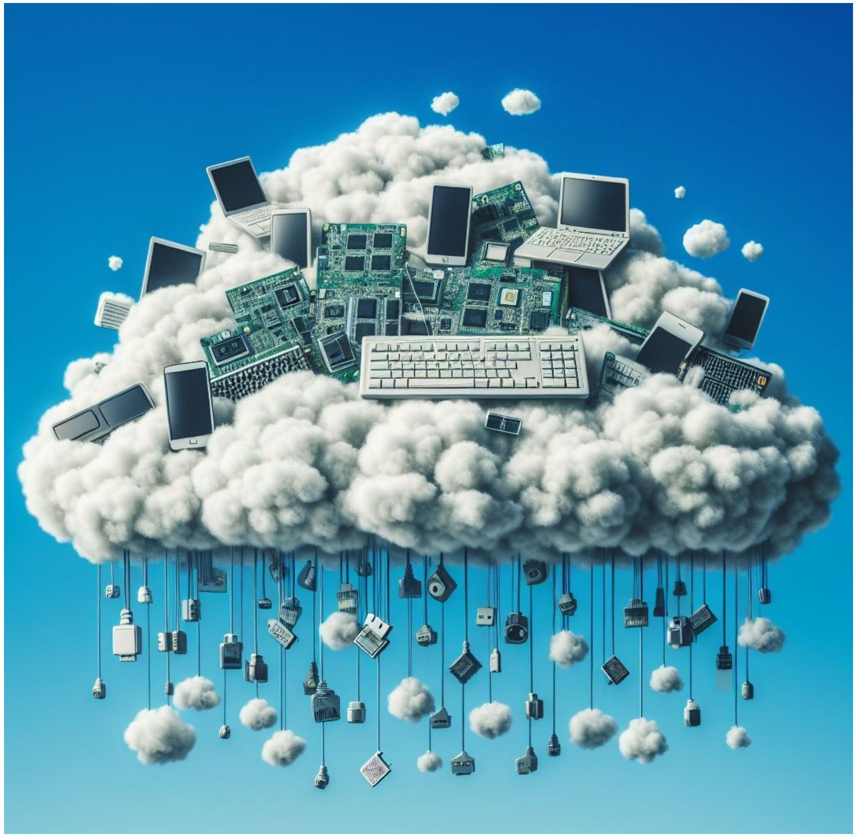
NIST
Cybersecurity
Framework
GOVERN
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER



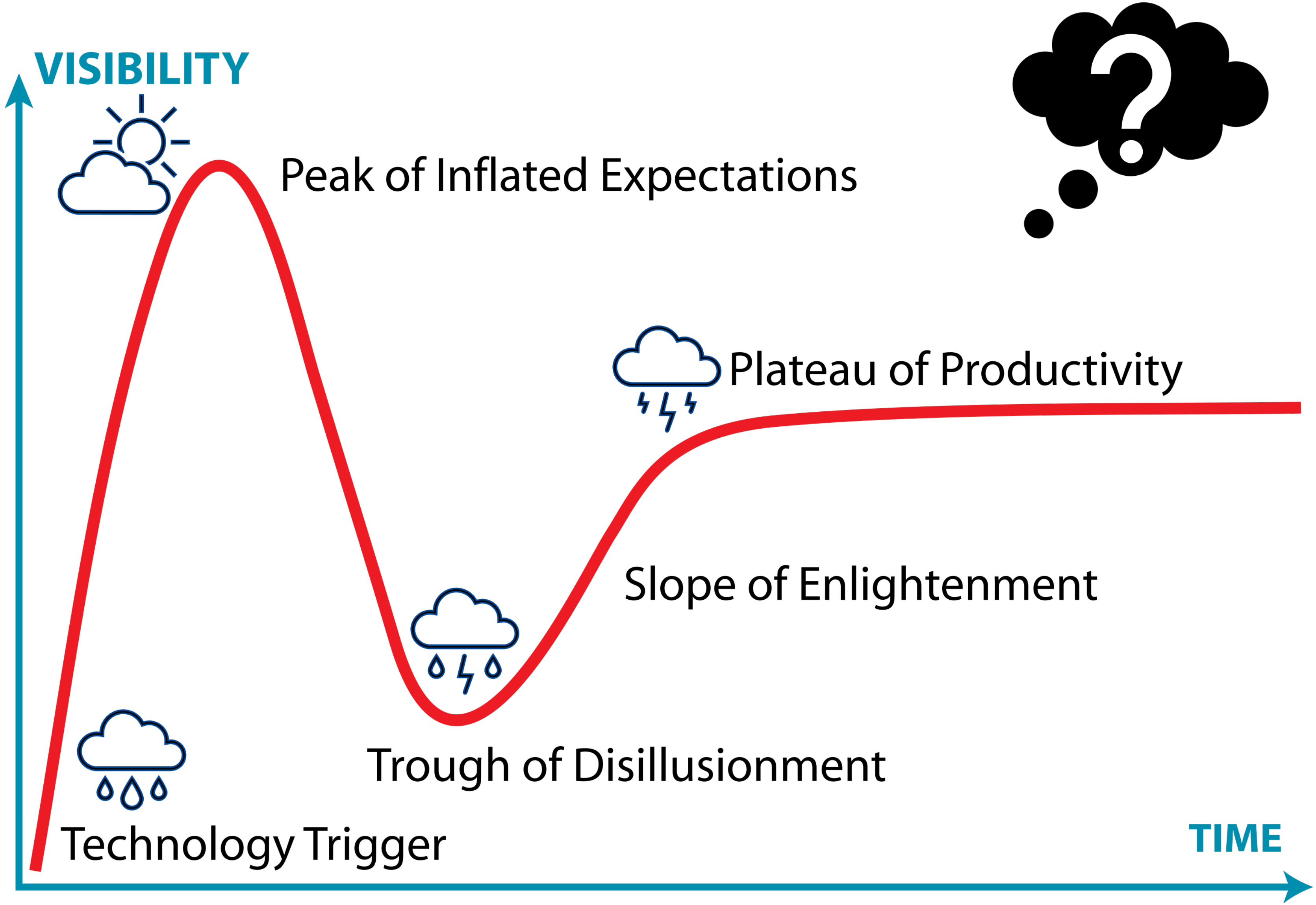
OUTSIDE THREAT
PROTECTION
PERIMETER SECURITY
Message Security
(anti-virus, anti-malware)
Secure DMZs
Honeypot
Perimeter
IDS/IPS
DLP
Perimeter
Firewall
DHS
Einstein
NETWORK SECURITY
Web Proxy Content Filtering
NAC
Enterprise
Message Security
Inline Patching
VoIP Protection
Enterprise
Wireless Security
Enterprise
IDS/IPS
Enterprise
Remote Access
Enclave/
DataCenter
Firewall
DLP
ENDPOINT SECURITY
Endpoint Security
Enforcement
Content Security
(anti-virus, anti-malware)
FDCC
Compliance
Host
IDS/IPS
Patch
Management
Desktop
Firewall
DLP
APPLICATION SECURITY
WAF
Dynamic App Testing
Database
Monitoring/Scanning
Static App
Testing/Code
Review
Database
Secure Gateway
(Shield)
DATA SECURITY
Identity &
Access
Management
Data
Classification
DAR/DIM/DIU
Protection
Data Integrity
Monitoring
PKI
Data Wiping
Cleansing
Enterprise
Right
Management
DLP
Data/Drive
Encryption
Mission
Critical Assets
PREVENTION
IT Security
Governance
POLICY MANAGEMENT
Security Policies
& Compliance
Cyber Threat
Intelligence
Threat Modeling
Security Architecture
& Design
Risk Management
Penetration
Testing
Continuous C&A
Security Awareness
Training
Vulnerability
Assessment
MONITORING & RESPONSE
SOC/NOC
Monitoring (24x7)
OPERATIONS
Incident Reporting,
Detection, Response
(CIRT)
Continuous
Monitoring and
Assessment
Focused Ops
Situational
Awareness
Security Dashboard
Escalation
Management
SIEM
Digital Forensics
Security SLA/SLO Reporting



Mitigation
Prevention
Emergency response
Passive protection
(e.g. Bund/Dike)
Active protection
(e.g. Relief valve/Rupture disk)
Incident
Safety Instrumented System
Trip
Operator Intervention
Alarm
Process Control
Loop
Process value
Process Design



There is no cloud
it’s just someone else’s computer



VISIBILITY

Peak of Inflated Expectations

Plateau of Productivity

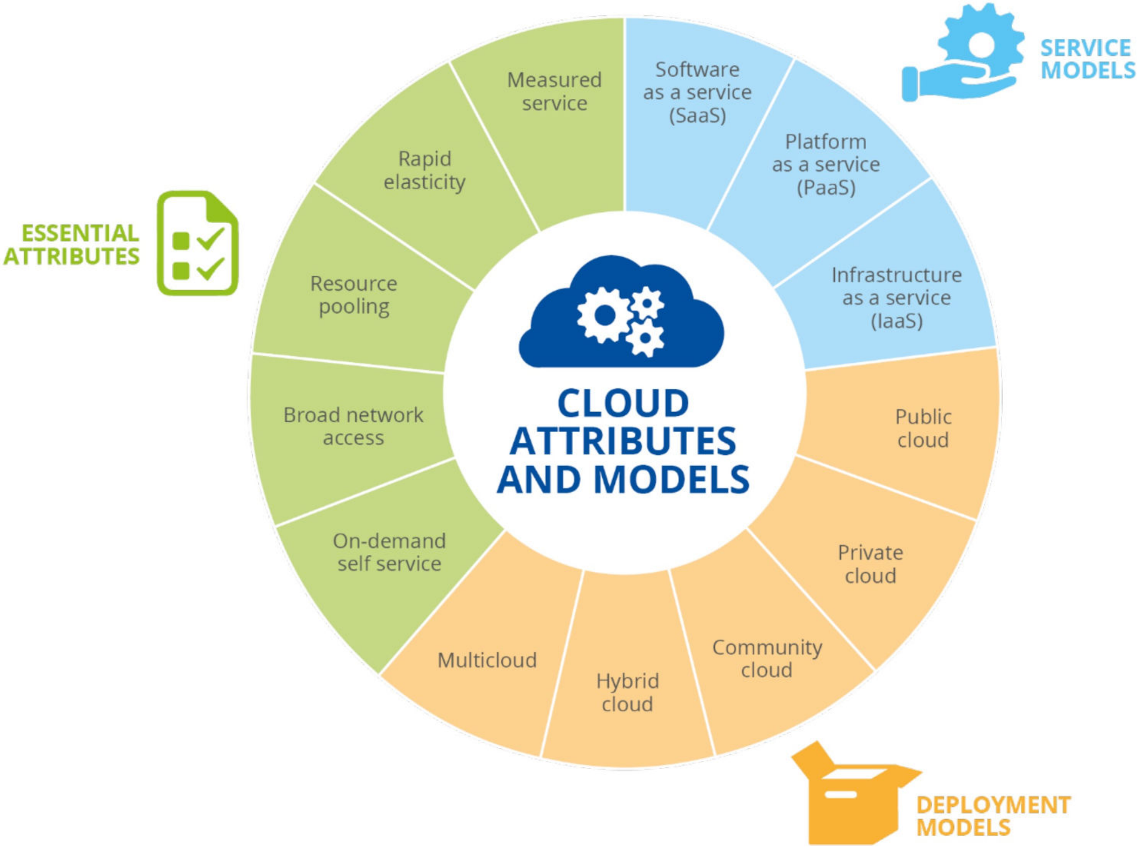
Slope of Enlightenment

Trough of Disillusionment

Technology Trigger

TIME

Cloud as a cold stand-by
Hybrid for analytics
Hybrid for control
Full migration

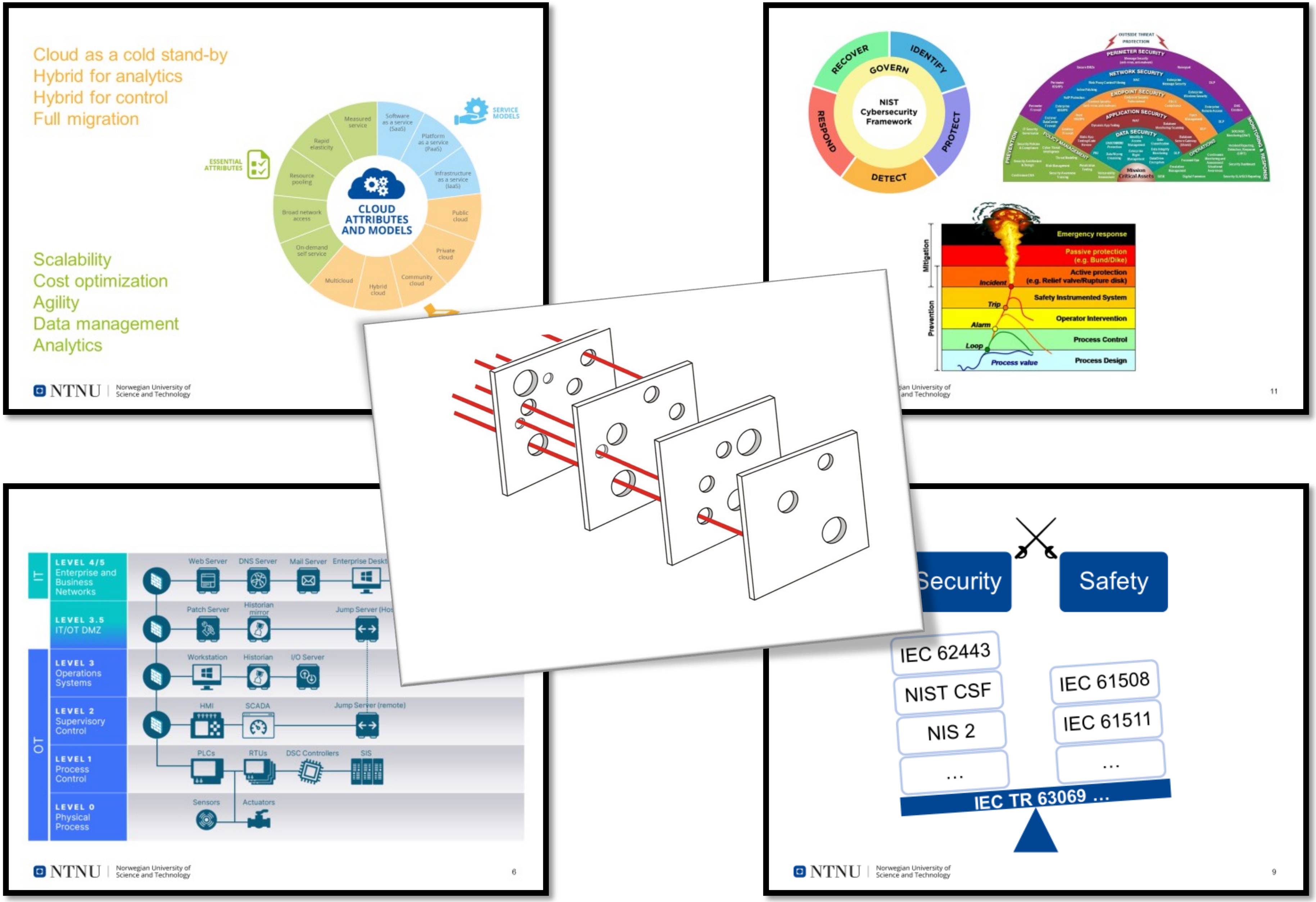


Scalability
Cost optimization
Agility
Data management
Analytics

- Moving to the cloud doesn’t simply change where a SCADA system is hosted; it fundamentally alters the traditional management, security boundaries, connectivity model, and access control mechanisms, as the system is now internet-connected.

National Cyber Security Centre

Access control	Audit	Authorization	Availability
Chain of trust	Chain of responsibility	Compliance	Control
Confidentiality	Incident management	Identification	Authentication
Integrity	Multi-tenancy	Privacy	Storage
Latency	Classification	Organizational readiness	Policy management



Cloud as a cold stand-by
Hybrid for analytics
Hybrid for control
Full migration

Scalability
Cost optimization
Agility
Data management
Analytics