computers

MDPI

Article

Modeling Networked Telemetry

Wondimu Zegeye, Richard Dean *, Mulugeta Dugda, Farzad Moazzami and Andargachew Bezabih

Electrical and Computer Engineering Department, Morgan State University, Baltimore, MD 21251, USA; wondimu.zegeye@morgan.edu (W.Z.); mulugeta.dugda@morgan.edu (M.D.); farzad.moazzami@morgan.edu (F.M.); anbez1@morgan.edu (A.B.)
* Correspondence: richard.dean@morgan.edu

Abstract: This paper presents the modeling of the networks supporting today's telemetry. The incorporation of networking features has significantly enhanced the capability and performance of modern telemetry systems. The development of Integrated Network-Enhanced Telemetry protocols and the use of networked telemetry applications has introduced a host of potential cybersecurity risks inherent in modern networking. This paper will investigate how telemetry applications are uniquely structured with wide-, local-, and micro-area networks that represent modern telemetry solutions. The development of these models and the traffic on these networks will enable analysis into the unique threats and vulnerabilities of telemetry networks. The core of this paper is the notion that telemetry networks are unique, and modeling these networks is key to the current work. The core premise of this paper is also that telemetry networks look and function like Supervisory Command and Data Acquisition (SCADA) networks. By digging deeply into both of these structures, we have shown here that SCADA architectures can be adapted to telemetry networks. This approach opens the door to a wealth of analysis, strategies, and solutions for telemetry networks that are well developed in the SCADA realm.

Keywords: telemetry; iNET; risk assessment; ICS-SCADA; network security

Citation: Zegeye, W.; Dean, R.; Dugda, M.; Moazzami, F.; Bezabih, A. Modeling Networked Telemetry. *Computers* **2021**, *10*, 45. https://doi.org/10.3390/computers10040045

Academic Editor: Reiko Heckel

Received: 13 February 2021
Accepted: 23 March 2021
Published: 3 April 2021

1. Introduction

It was reported that a working group on telemetry was founded in 1948 so that "a large amount of development effort could be saved by standardization" [1]. Versions of those upcoming standards started evolutionary sequencing in 1953, which later led to active use by multiple ranges in 1969, following approximately ten updates/revisions. Both commercial and military telemetry communities harvested the benefits of having invested in these standards after several decades. The Central Test and Evaluation Investment Program (CTEIP) instituted the Integrated Network-Enhanced Telemetry (iNET) project to foster an interoperable air-to-ground network telemetry capability. Since then, the standards created by the iNET project have been embraced as Chapters 21 through 28 of the Range Commanders' Council (RCC) standards. Moreover, the Telemetry Network Standards (TmNS) introduced a major improvement to the sequence of evolving the Range Commanders' Council (RCC) standards [1–3].

Components of future networked telemetry include network-enabled instrumentation, network-enabled ground stations, and mission control rooms, as well as ground support equipment. These components are considered a high-level subsystem of Integrated Network-Enhanced Telemetry (iNET) [4]. iNET is portrayed as a networked telemetry data system that can provide developmental flight tests. Figure 1 shows telemetry network instrumentation and a test article (TA) to ground station (GS) telemetry system proposed by Young [4]. This single TA to single GS communication is the basic building block for multiple distributed sites and consists of multiple TAs and GSs. The iNET paradigm is shown to have the benefits of test/data and spectrum efficiency as well as long-term sustainability and interoperability. In our effort to develop a telemetry network testbed, we build upon the concepts and implementation ideas developed for iNET and beyond.

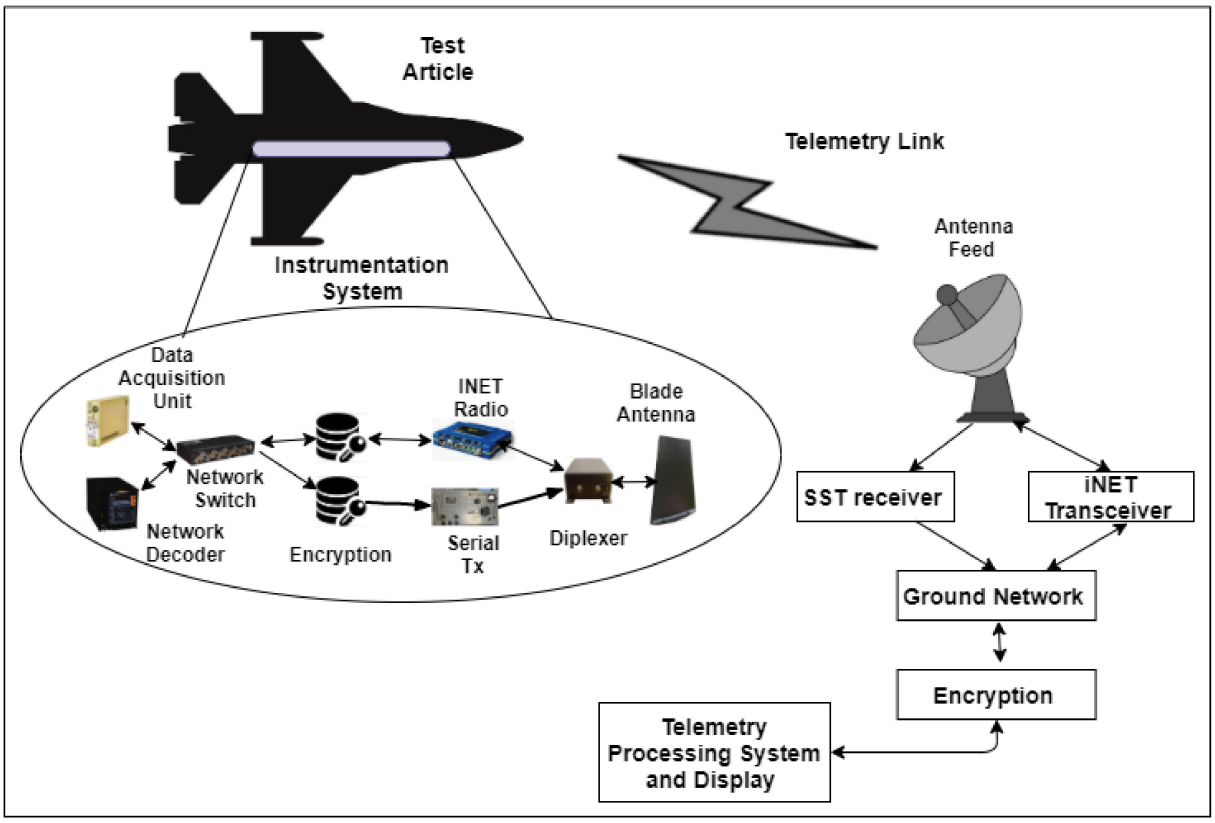

Figure 1. Telemetry network instrumentation and a test article aircraft [4].

Because of the complexity of modern aircraft as well as spectrum reduction in the Department of Defense (DoD), collecting important data from a test flight in real-time has become increasingly difficult. However, over the last five decades, aircraft flight test performance has been monitored by utilizing unidirectional telemetry links to the ground for the test article. Moreover, Integrated Network-Enhanced Telemetry (iNET) networks enable access to and the transmission of onboard aircraft data in an on-demand fashion using duplex datalinks [5]. This equips test engineers with the ability to control the instrumentation on board a test article from the ground. This capability of controlling the airborne instrumentation from the ground grants access to both the data recorder and the data acquisition systems' data formatting and sampling, which, in turn, can furnish the capacity for dynamic real-time adjustment of information streaming to the ground. The DoD test community has invested in iNET for the future of network telemetry [5].

In modeling a telemetry network, we consider the ground station to comprise traditional enterprise network and Supervisory Command and Data Acquisition (SCADA) systems. This allows us to build on the many studies of cyber vulnerabilities in SCADA networks. SCADA systems are among the most widely used industrial control systems (ICSs) that enable the controlling and monitoring of process equipment on multiple sites that spread over large distances [6]. SCADA systems are cyber-physical systems with communication networks interfacing the monitoring and control system with the hardware and these could have multiple supervisory systems, programmable logic units (PLCs), remote terminal units (RTUs), human–machine interfaces (HMIs), process and control instrumentation, sensors, and actuator devices over a large geographical area. SCADA systems make use of both new and legacy systems, including traditional information systems [7]. SCADA systems are not only as vulnerable as any other networked computer systems, but their legacy systems create another layer of threat. Since many of these systems have existed for decades, their cybersecurity risks are unknown and challenging to analyze as well. These

SCADA systems resemble much of the networked telemetry systems that we intend to model and therefore represent a good starting point.

Due to their architecture, strict real-time specifications, network traffic functionality, and complex application layer protocols, there are security threats relevant to SCADA systems in particular [7,8]. As a result, specialized intrusion detection systems (IDSs) are desired to secure modern SCADA systems. In order to achieve the required performance of a real-time system operating continuously with the behavior of coexisting system failures, environmental conditions, human errors, and cyberattacks, there are three important factors to be considered for the design of SCADA-specific IDSs: hierarchical architecture, network traffic properties, and cyber vulnerabilities and attacks [6–12]. Having dedicated independent hierarchical architecture in SCADA systems, industrial control networks are characterized by different protocols and physical standards. SCADA physical and cybersecurity are converging these days. The forthcoming fourth-generation SCADA systems adopt industrial Internet of Things (IIoT) and Future Internet (FIN) technologies such as cloud/fog computing, big data analytics, mobile computing, etc. [11].

Here in this paper, we are envisioning the current telemetry network with the idea of building a general telemetry cybersecurity network testbed, which initially combines traditional network security controls with an industrial control system (ICS-SCADA) structure built with telemetry components.

The goal of this paper is to provide an architectural framework for telemetry networks for our testbed that meets the current and future requirements of network operations. It describes and classifies the current modules and components of a telemetry network system. It outlines the system architecture to help set a working foundation for telemetry network system vulnerability analysis that leads to a security solution. This is our contribution to the general telemetry cybersecurity community, where we capture the scope of these networks and frame this environment. This architecture will also allow us to explore machine learning and artificial intelligence for the real-time streaming of data to predict unique patterns in traffic in telemetry networks.

This paper introduces the telemetry network components. Test and ground stations are analyzed in Section 2. This section is organized into different subsections further analyzing both the test articles and the ground communication systems. The test article investigates the different communication devices onboard the test article that resemble a typical internet of things network, whereas the ground communication system subsection addresses different components such as the ground communication entities, protocols, and the Test and Resource Management Center. Section 3 dives deep into the SCADA architecture in our attempt to model and overlap the SCADA architecture to the telemetry network. This SCADA part envisions the most secured part of the telemetry network that is normally referred to as the mission control center.

2. Telemetry Architecture: Test Article and Ground Station

The Telemetry Network Standards (TmNS) investigate improvements in RF technologies, modulations, and waveforms, RF components (e.g.,linear amplifiers, multiband support), improved access schemes (e.g. TDMA, FDMA), and alternative wireless technologies that leverage spectrums not currently used for telemetry. They also develop tools to provide flexible and agile access to spectrum, enable the management of telemetry network resources, and test planning and system performance. In this regard, there is a huge pressure to share and manage telemetry spectrum resources due to the ever-increasing high demand for air-to-ground telemetry bandwidth. The spectrum management system (SMS) of DoD works on test range operations with advanced tools for frequency deconfliction and air-to-ground RF link quality prediction for forthcoming test flights. Moreover, the ever-increasing commercial interest in telemetry spectrum bands has created a need for test range operations personnel to plan and manage the available spectrum in the most efficient way possible. The Spectrum Efficient Technology (SET)-Spectrum Management System (SMS) project has been launched to help test range personnel deploy advanced capabilities

with efficient and improved spectrum resources [13]. Spectrum sharing between federal and commercial users is proposed by the FCC and NTIA to open up the 3.5 GHz band for wireless broadband [14]. Detection and subsequent allocation by other users of the available licensed spectrum for temporary use without interfering with the transmission of incumbent signals. Our research in the past has presented a spectrum-sharing opportunity and technology that will help reduce service interference between spectrum users. We developed a protocol model for spectrum sharing and implemented a cognitive radio media access sensing mechanism using a cyclo-stationary feature detector (CFD) [14].

Since the inception of TmNS, it has identified different capabilities for networked aeronautical telemetry [1]. These include, but are not limited to, the need for,

- Spectrum and access management.
- Solutions for the management of telemetry infrastructure.
- Management of telemetry network performance.
- Unified management tools.

One of the main goals of the iNET is to enhance reliable and secure communication between a test article (TA) and a ground station (GS), as shown in Figure 1, adapted from Young [4].

The bidirectional link between the TA and GS must be reliable, efficient, and secure. The ground control of onboard flight instrumentation can control all components configured in the network. This system can request data in real time and access the data without disturbing the recording capability. Since this telemetry network leverages the commercial network communication standards of Ethernet, TCP/IP, UDP/IP, SNMP, RTSP, FTP, XML, and PPTP1588, the risks associated with these protocols are inevitable in telemetry networks. However, this allows a bidirectional telemetry architecture with unconstrained potential for application-based functionality. This influences instrumentation configuration, acquisition sites, mission control rooms, components, and capability.

The iNET program in the US DoD has implemented a novel approach to telemetry in which the network architecture for airborne platforms replaces the serial instrumentation bus with industry-standard Ethernet. It also introduced a bidirectional network channel from the aircraft to the ground. Though iNET also makes use of serial streaming telemetry (SST) links for the safety of flight and other telemetry data, the introduction of new network-based communication channels will provide new functionalities that did not exist before. Moreover, iNET provides command and control of the instrumentation systems while the aircraft is in flight. For more than five decades, aircraft flight test performances were monitored using a unidirectional telemetry link for the test article to the ground. iNET eventually introduced the capability to access and transmit onboard data in a packetized IP-based format [4,5].

2.1. Test Article and Ground Station

2.1.1. Onboard Instrumentation System

The onboard instrumentation system on a TA consists of a networked system of device communication via different protocols such as Ethernet, WiFi, Bluetooth/BLE, ZigBee, and Zwave. These protocols belong to a class of IoT protocols. Hence, the onboard instrumentation can be viewed as a network of communication equipment that sends data from the IoT network, where the IoT devices mainly include different sensors on the Test Article. The flight onboard test bed also consists of the telemetry network system (TmNS) that includes a TmNS recorder, a TmNS radio, TmNS data acquisition units, and a TmNS switch.

The data encrypted by the TA's network are processed and displayed for real-time and offline visualization by the mission control system of the ground station. This control system is described in detail in the SCADA system (Section 3.1).

2.1.2. Ground Communication System

The ground segment contains the antenna system that creates a link to the TA or multiple TAs, as shown in Figure 1. The current link paradigm relies on a TM link, which is efficient in spectrum to increase the availability of required bandwidth. In addition, it is also efficient in providing improved test data and test efficiency.

2.2. Test and Resource Management Center

The Test Resource Management Center (TRMC) is the manager of the Joint Mission Environment Test Capability (JMETC). This subsection describes the architectures of the test and training environment that integrates the live and virtual environments [1,15,16]. Several perspectives of this environment are captured below from prior work that will allow us to develop our test bed model.

2.2.1. Test and Training Environment

Figure 2 shows the kind of network framework that we envision for our cybersecurity test environment. At the top in Figure 2 is shown some physical assets. These physical assets are connected through networks below them. We have a simulated environment below the networks. These physical and simulated real environments are somehow interfaced to virtual assets such as big data storage, big data analytics, and visualization through the middleware called Test and Training Enabling Architecture (TENA).

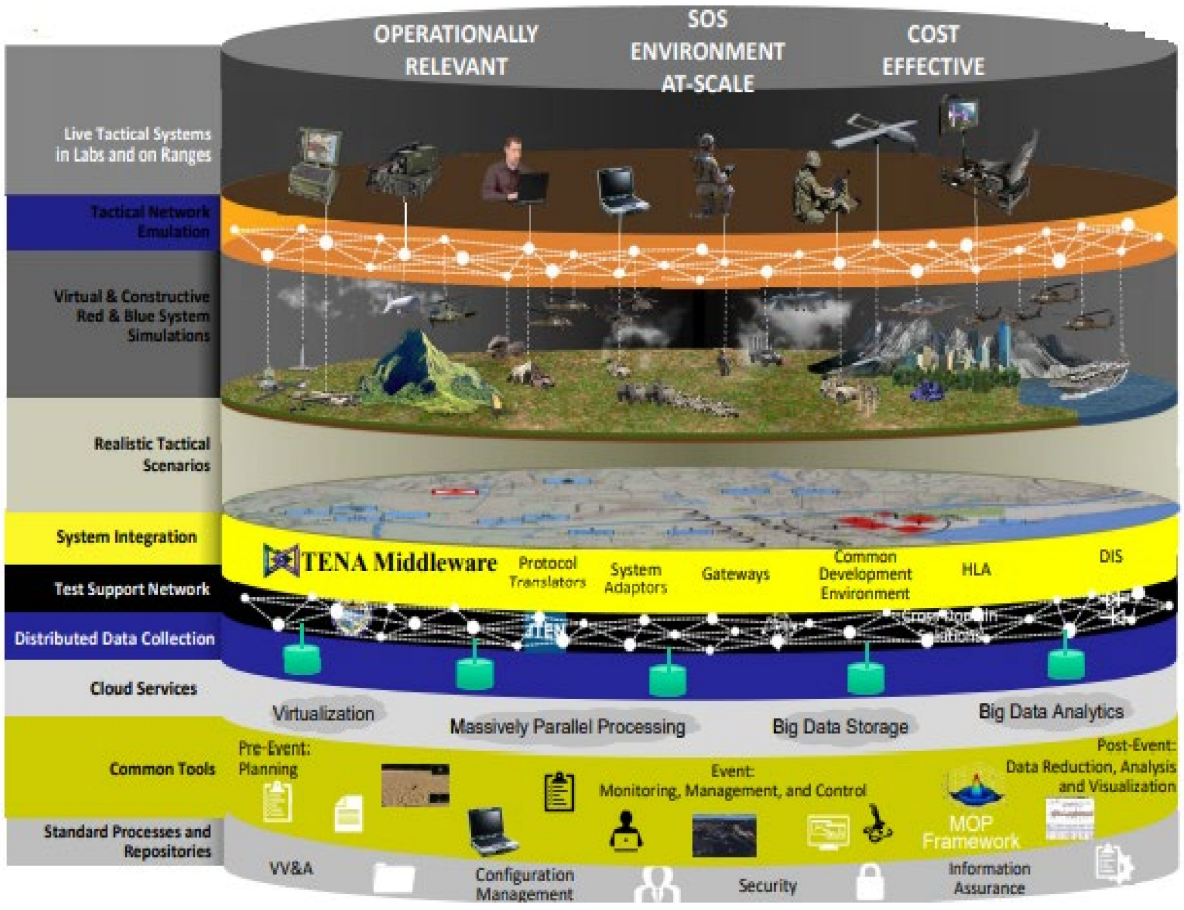

Figure 2. Virtual test and training environment [14].

Figure 2 shows a virtual test and training environment, JMETC, which reflects our objective in modeling a telemetry network. This test environment abstraction shows the many aspects of the future of telemetry [17].

JMETC provides a robust and secure distributed testing environment, including several government and industry range labs, cybersecurity testing and evaluation (T&E), and TENA. JMETC supports T&E Infrastructure Interoperability. One of the challenges in the original design of the DoD test range infrastructure was the lack of interoperability between different systems. TENA is a flexible infrastructure design for T&E operation with mature and continuously improving software architecture with integration capability [16].

JMETC has a hybrid network architecture:

(1) The JMETC Secret Network (JSN), which is the T&E enterprise network solution for Secret testingis based on the Secret Defense Research and Engineering Network (SDREN).
(2) The JMETC Multiple Independent Levels of Security (MILS), whereas The T&E Enterprise network solution for all classifications and cyber testing is Network (JMN).

JMETC supplies tools, services, and support that are all institutionally funded capabilities. JSN and JMN engineering and event support services are free to the user. JMETC capabilities are driven by user requirements and JMETC provided tools and services are based on user input. TENA is an architecture for ranges, facilities, and simulations to interoperate, to be reused, and to be composed into greater capabilities [16].

2.2.2. Net-Centric Systems Test Environment

Another look at the test environment with a distributed T&E Infrastructure is as shown in [6,18]. They can bring resources from different sites and combine them into a cohesive test environment as shown in Figure 3.

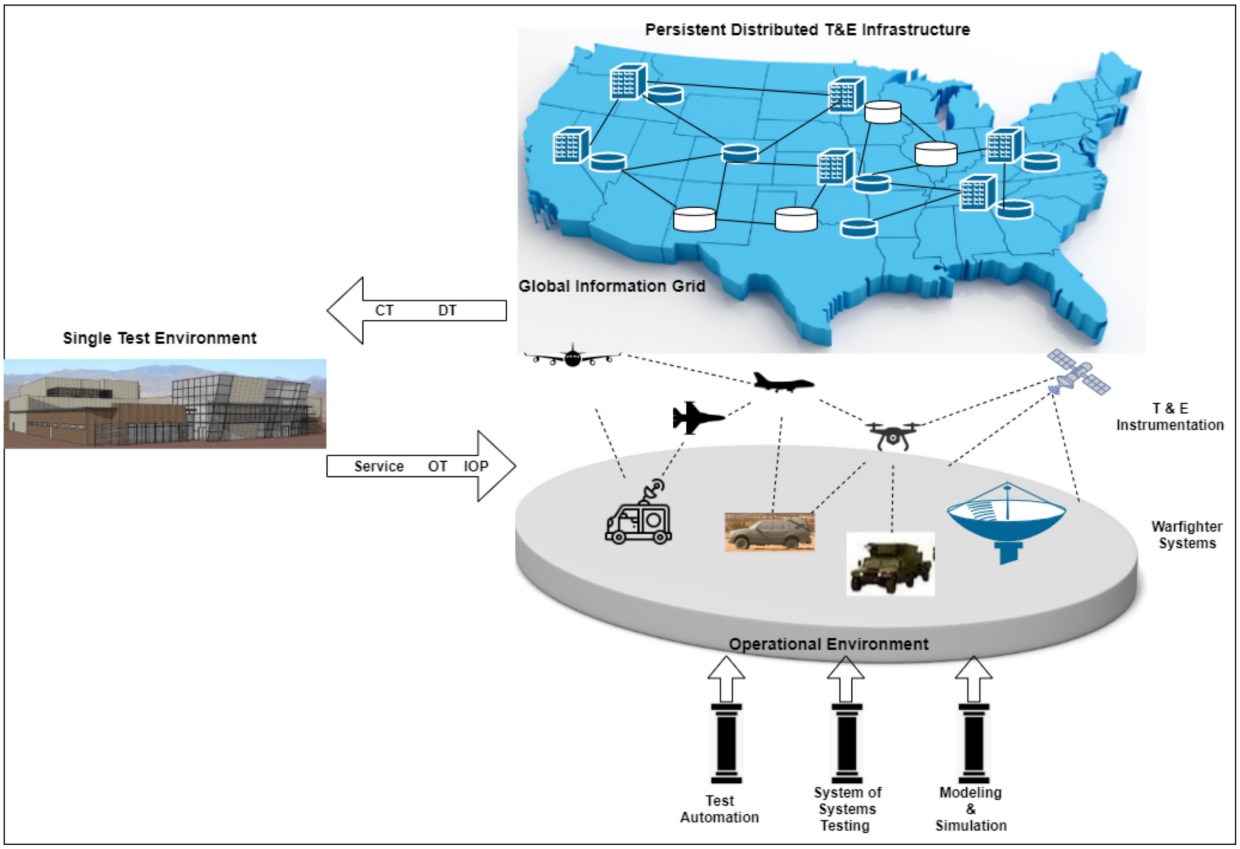

Figure 3. Net-Centric Systems Test (NST) environment [18].

The Net-Centric Systems Test (NST) single-test environment provides agile early and continual capability-based automated T&E for performance, interoperability, effectiveness, and sustainability. The NST cohesive environment domain focuses on test automation,

systems of system testing, and modeling and simulation. This network consists of a land network, surface network, aeronautical network, and space network.

2.2.3. Distributed Live and Simulated Systems T&E Environment

The distributed live and simulated environment adds the ability to provide system testing with the addition of simulated elements that interact with live systems under test. It requires advanced synchronization algorithms to remove test infrastructure bias in support of mission effectiveness T&E. It consists of simulated and live entities. The integrated live simulated environment shown in Figure 4 is controlled from a test and control analysis center.

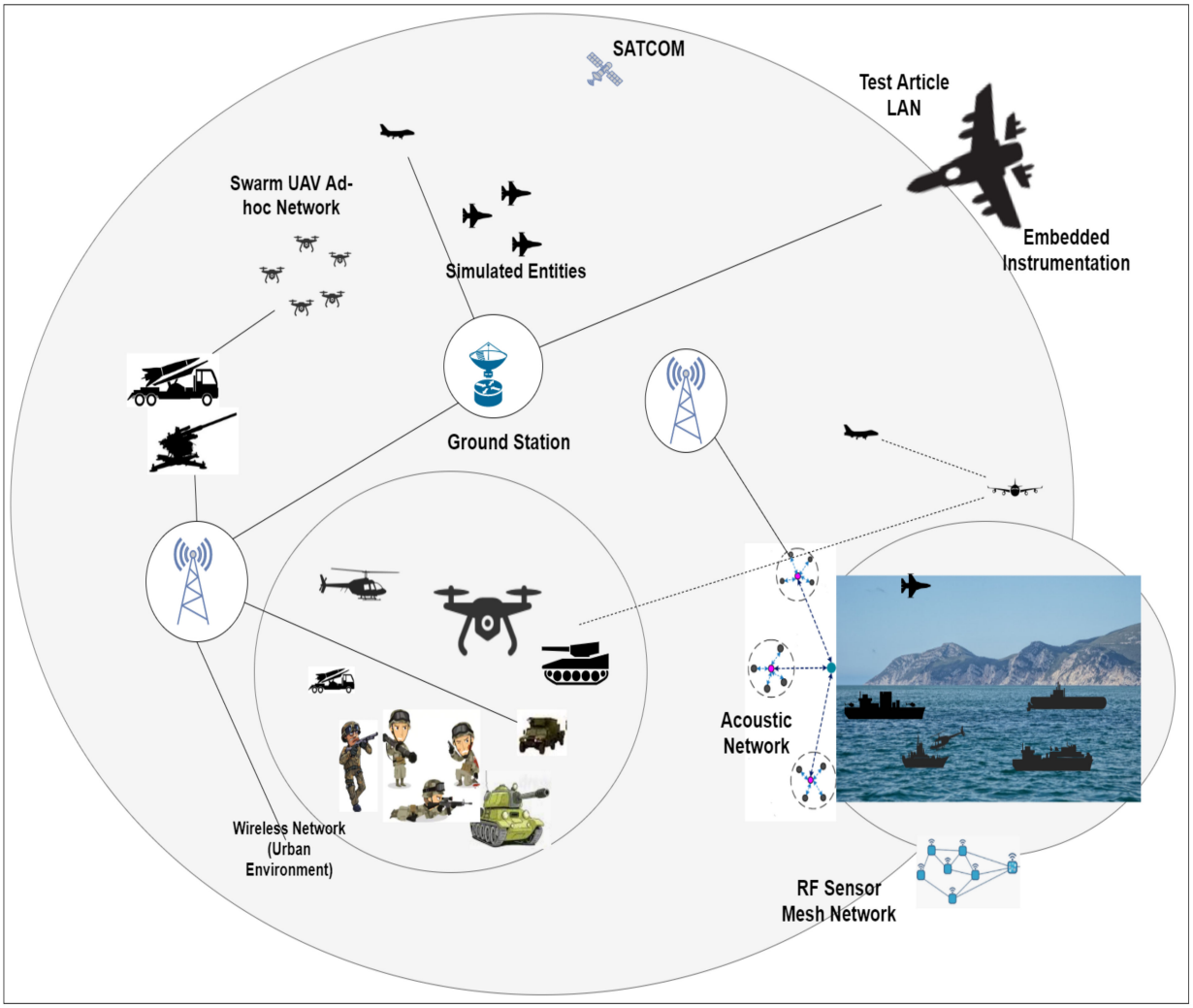

Figure 4. Integrated live simulated environment (modified from [16,19]).

It is one scenario of the NST system of system testing. It can consist of live entities such as ground stations, swarm UAVs, which are in an ad-hoc network, and SATCOM, as well as simulated entities that include things such as soldiers, tanks, and fighter helicopters, added to create a comprehensive ground wireless environment. The live entities communicate with the swarm of UAVs and the wireless network (urban environment) via cellular networks. This network communicates to a TA via a ground station. A TA has an onboard instrumentation system that has several sensors interconnected via LAN and short-range communication protocols such as Bluetooth and Zigbee.

2.2.4. T&E Simulated and Cyberspace Threat Environment

Figure 5 shows the T&E simulated environment and cyberspace threat environment, which, together, form a cohesive structure of warfighting systems. This system includes a global information grid, which is the DoD Internet, and it also involves simulated threats.

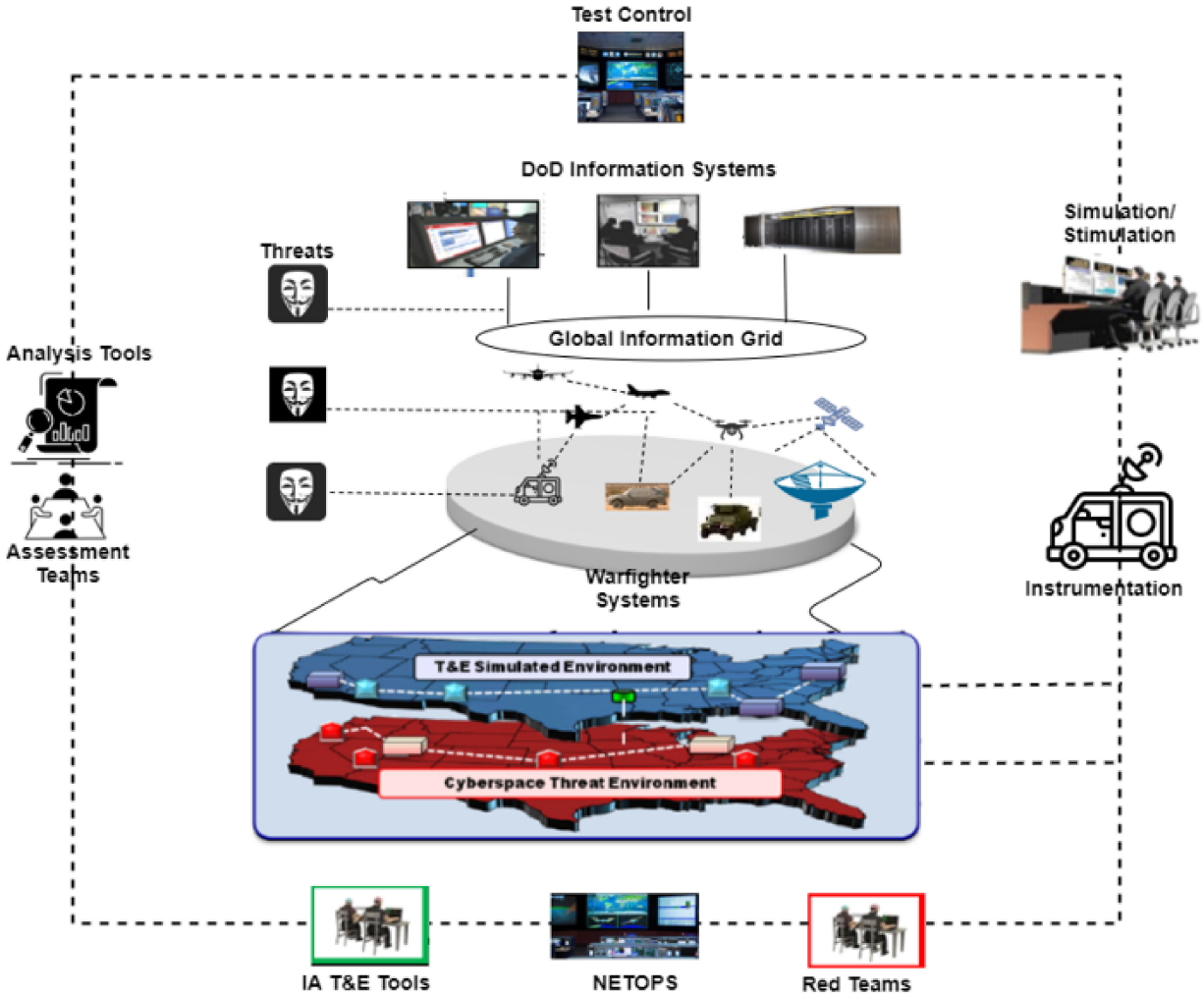

Figure 5. Testing and evaluation (T&E) simulated and cyberspace threat environment [18].

The T&E accurately and affordably measures cyberspace effectiveness and vulnerability of warfighting systems and DoD information systems to verify the war fighter's capability to achieve mission success while operating in cyberspace. This cyberspace threat environment is made up of the execution domain (visualization and analysis tools, intelligent analysis instrumentation, network intelligent analysis instrumentation, and sanitization instrumentation), threat domain (simulation/stimulation), and test planning domain (scenario/test design and control).

3. General Networked Telemetry Architecture

This section outlines the general telemetry architecture envisioned in this paper. This approach models telemetry systems as an industrial control system (ICS) SCADA. These systems have received significant attention, so analysis and conclusions of this work will apply directly to our efforts to model telemetry systems for cybersecurity purposes. The architecture consists of a typical enterprise network and an ICS/SCADA representation of a telemetry system ground station, as shown in Figure 6. Here, the emphasis is on the ICS-SCADA representation of telemetry systems, which is described in detail in Section 3.1. Section 3.2

presents the core of this paper, which is the general networked telemetry architecture. The SCADA system architecture evolution is as shown in Tables 1 and 2, and the model we consider will be the Purdue reference architecture.

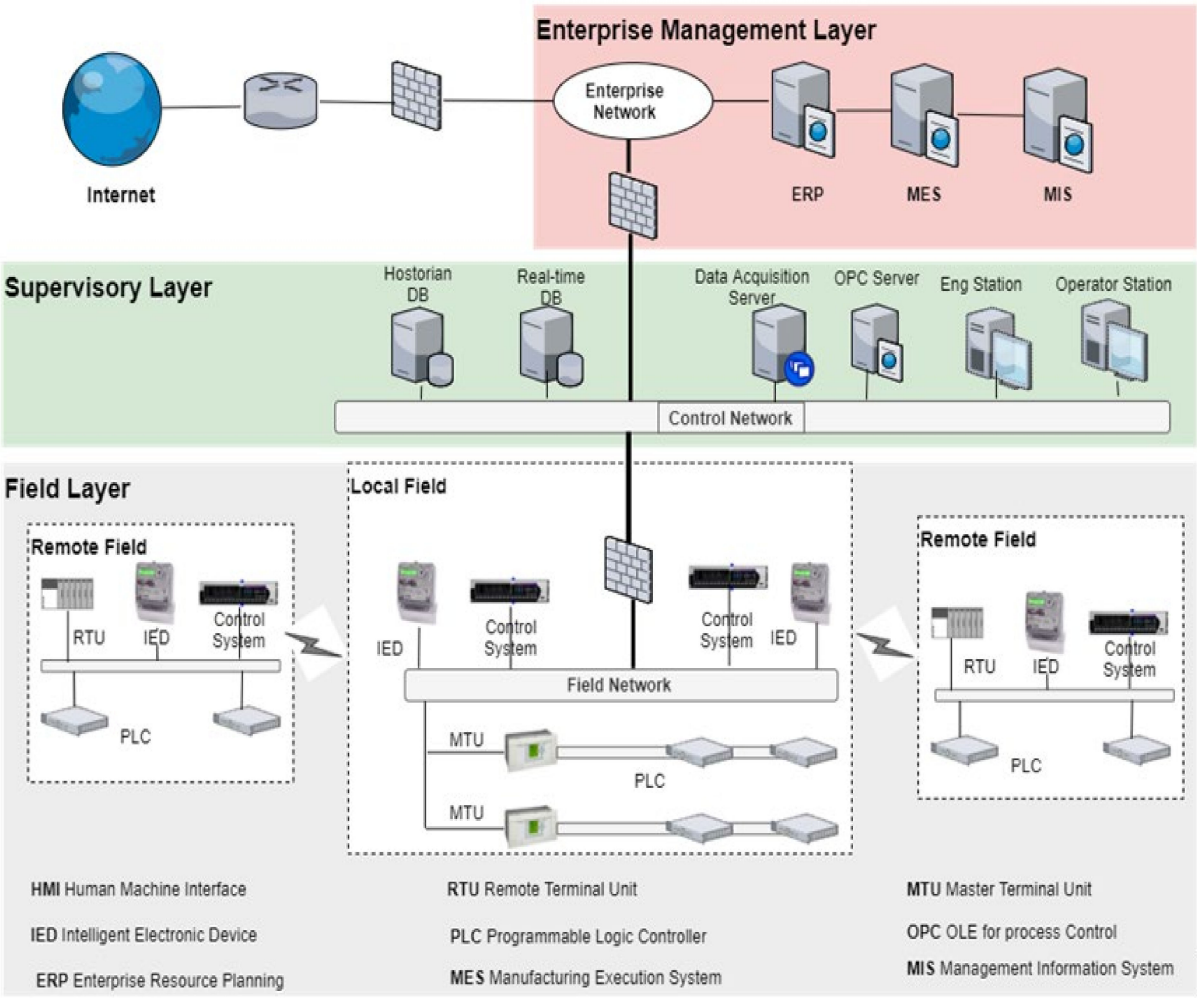

Figure 6. Industrial control system (ICS) network architecture.

Table 1. Supervisory Command and Data Acquisition (SCADA)system architecture evolution.

Process Control Network		**Purdue Reference Architecture**		
Manufacturing Operations	Level 3	Enterprise	Business	Level 4
Control Systems	Level 2	DMZ	DMZ or 3.5	
Intelligent Devices	Level 1	Manufacturing	Manufacturing Operations	Level 3
Process	Level 0	Plant HMI	Control Systems	Level 2
			Intelligent Devices	Level 1
			Process	Level 0

Table 2. Supervisory Command and Data Acquisition (SCADA) IoT/IIoT system architecture evolution.

IoT/ IIoT Reference Architecture		
The Cloud	Business	Level 4
	DMZ or 3.5	
The Edge	Manufacturing Operations	Level 3
	Control Systems	Level 2
	Intelligent Devices	Level 1
	Process	Level 0

The ICS model includes three independent layers: the enterprise layer, the supervisory layer, and the field layer. The industrial control system (ICS) network model maps telemetry test range control elements into the ICS supervisory layer and the telemetry test article into the ICS field layer. The ICS system's field layer can be connected to the enterprise network for management purposes via the supervisory layer separated by a firewall [20–22].

The ICS is different from a traditional enterprise system due to its close connections to the physical layer of devices. For example, if we consider a single telemetry ground station, the sensors distributed on a test article consist of the intelligent electronic devices (IEDs) in the ICS model.

3.1. Industrial Control System (ICS)

The industrial control system (Levels 0–3) of the Purdue architecture maps into the TA and ground segment of iNET. Levels 0–2 from Purdue are the field layers of Figure 6, whereas Level 3 from Purdue is the supervisory layer. The field layer of the ICS system consists of the following networked components [20–22]. These components are described below to show how they could map to the envisioned SCADA-based ground control room, T&E center's field layer.

(1) Human–Machine Interface (HMI)

It is usually a computer terminal interface that presents the cycle information to be constrained by a human administrator. It is utilized by connecting to the SCADA framework's product projects and data sets for providing the administrator data, including the planned support systems, point-by-point schematics, strategic data, and moving and demonstrative information for a particular sensor or machine. HMI frameworks encourage the working administrators to see the data graphically. In telemetry networks, the HMIs represent ground station control room computer interfaces for mission control and T&E simulations.

(2) Remote Terminal Unit (RTU)

All field hardware is associated with the RTU. It is an agent of an independent microprocessor-controlled unit that screens and controls hardware in the field. Field devices in SCADA frameworks are interfaced with microchip-controlled electronic gadgets called remote terminal units (RTUs). These units transmit telemetry information to the master system and retrieve messages from the master supervisory system for controlling the associated devices. Consequently, these are additionally called remote telemetry units.

(3) Programmable Logic Controller (PLC)

In SCADA frameworks, PLCs are associated with sensors for gathering sensor output signals and changing those sensor signals into computerized information. PLCs are utilized rather than RTUs due to the advantages of PLCs such as adaptability, arrangement, flexibility, and tolerance compared to RTUs.

Different programmable logic controllers (PLCs) are arranged and control a subset of processes known as Supervisory Control and Data Acquisition (SCADA). PLCs gather measurement information and send commands to field devices by executing control logic.

(4) Communication (Transmission System)

Communication equipment permits the exchange of data and information to and from the master terminal unit (MTU) and the RTU. For the most part, a mix of radio and direct wired connections are used for SCADA frameworks, yet in the event of large-scale systems such as power stations and railroads, SONET/SDH are often used. Even if there are several SCADA communications protocols functional for SCADA systems, only a handful of them are standardized. SCADA vendors only recognize the standardized protocols for sending information when the supervisory station polls the RTUs.

(5) The master terminal unit (MTU) gathers and logs data collected by the field layers, shows data to the human–machine interface (HMI), and may create activity dependent on distinguished events.
(6) Supervisory System

A supervisory system is utilized for conveying data between the hardware of the SCADA framework; for example, RTUs, PLCs, sensors, and so forth, as well as the HMI programming utilized in the control room workstations. The master station or administrative station involves a solitary PC in more modest SCADA frameworks, and, in the event of bigger SCADA frameworks, the administrative framework includes dispersed software applications, catastrophe recuperation locales, and various workers. These numerous servers are designed in a hot-backup development or dual-redundant, which continuously controls, and screens should an occurrence of a server malfunction arise.

(7) SCADA Programming

SCADA programming mainly uses the C language or derived programming languages. Data collected from RTUs must be read, which requires HMI and MTU, grouped and stored in history databases. These stored data are further analyzed to display trends that will give significant situational data if there should arise an occurrence of a failure event or process.

The above components are parts of the control network in Figure 6. Additional components in the ICS system are IEDS, which are intelligent sensors required to acquire data. The supervisory layer in Figure 6 is made up of several servers such as Historian and Database servers. It also includes workstations for different user groups, engineering, and operators. Network protocols in ICSs are mainly Ethernet TCP/IP, Modbus, and Modbus TCP.

3.2. General Integrated Networked Telemetry (iNET) Architecture

The telemetry architecture described in this section models telemetry network test sites, which includes an enterprise level that follows the SCADA model and control and field network levels. This architecture, as shown in Figure 7, has two test sites (T&E Centers), each of which has three SCADA levels. The Global Grid is the DoD Internet connected to both test sites and the T&E Resource Center through high-speed internet. Interfaces between two connected sites are secure connections. There are telemetry radio links between the test sites and test articles, which can be aircraft or ships. These communications links are targets of cyber threats such as denial of service on the radio network or intrusion on the enterprise, control, or field networks or the test article [23,24].

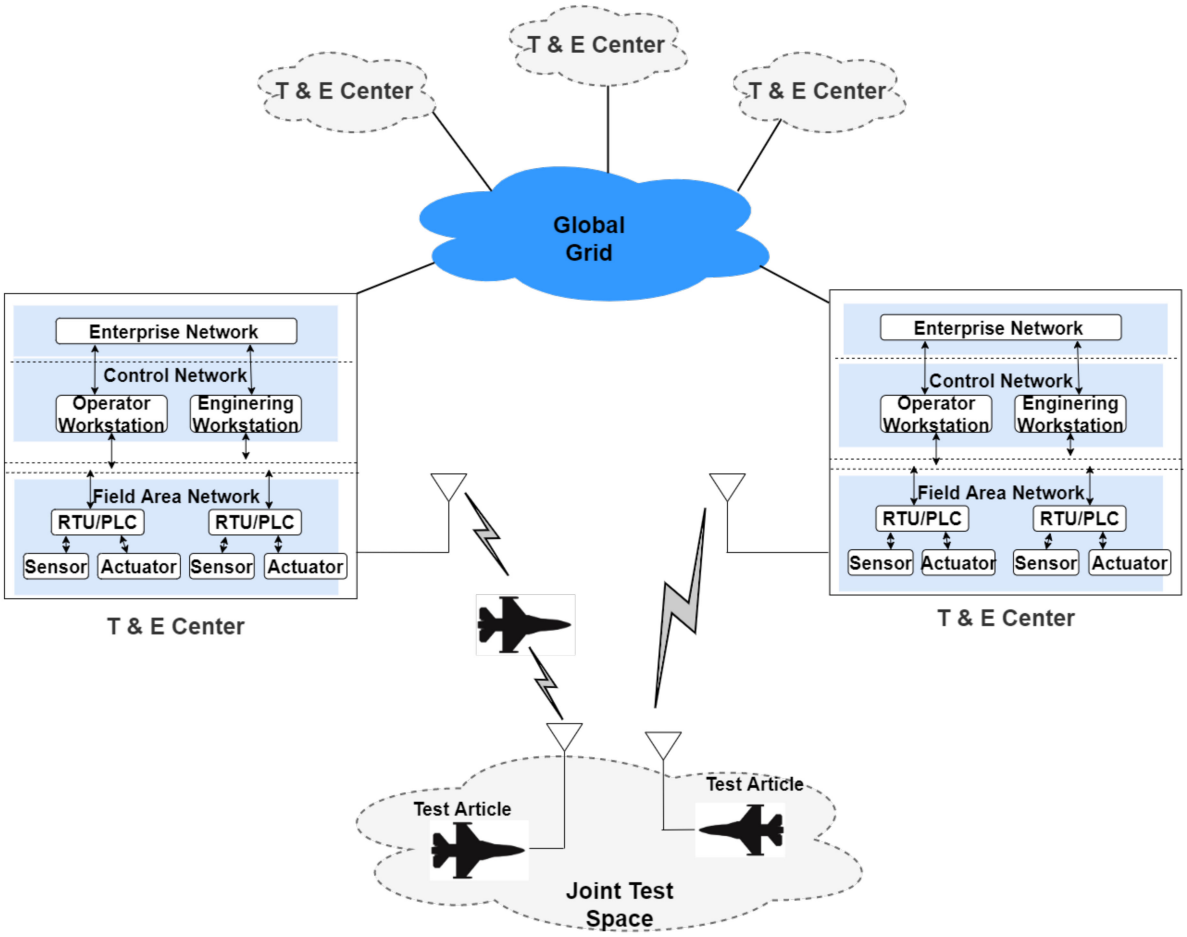

Figure 7. General telemetry architecture.

The general telemetry architecture proposed in this article is shown in Figure 7. It consists of different test and evaluation centers that are interconnected via the global grid. Figure 7 also shows two T&E centers connected to the global grid. The detail of each T&E site consists of the ICS-SCADA control room and enterprise network, which is described in Figure 6. The two T&E centers can communicate via the internet, which is secured via VPN, across the global grid. It also shows a joint test space made up of two test articles communicating via a reliable link, but they belong to two different T&E centers.

3.3. Mapping the Old Scada System to the Industrial 4.0

Verifiably, ICSs were truly isolated from the rest of the world, so it was hard to put forth a business defense for network safety given that they used to be completely isolated [23]. The attention was on keeping the process running, not network protection against cyberattacks.

Historically, the SCADA system architecture has evolved in the past from the process control network to the Purdue reference architecture (PERA) then to the industrial Internet of Things (IIoT) architecture, as shown in Table 2. Purdue was acquired as an operational model that sections the organization into coherent segments, bringing about an enterprise zone, a manufacturing/industrial zone, and the industrial DMZ (IDMZ) (gateway). The IDMZ (Level 3.5) is the authentication boundary between information technology (IT) and operation technology (OT). While the IT consists of Levels 4 and 5, the OT consists of Levels 0–3. This segmentation restricts traffic into the OT layers, and access to the lower layers happens from within the OT zones, where security can be better assured.

The expansion to the industrial Internet of Things (IIoT) architecture can be viewed as a significant spark to move to the Zero Trust segmentation, since it overturns the classically

stacked and hierarchical nature of the PERA model [9,25]. This stemmed from industrial manufacturing systems that are looking to take advantage of business continuity and operational analytics benefits. IIoT architecture further fragments the network of IIoT devices, which are parts of the OT layer and can communicate with the IT layers. They can send their data to Layer 3, which communicates with Layers 4 and 5. However, this direct connection exposes the underlying manufacturing layer for vulnerability. If proper isolation mechanisms are in place, a compromised IIoT device can be an attack launching pad to the rest of the OT segment it belongs to. It is easy to imagine the extent of this magnitude when there are a vast number of devices, each with its own possible security issues. Hence, it is essential to consider the security of IIoT devices as that of the other segments of the network. It is also important to weigh the benefits of a direct connection from the lower OT layers directly to the IT layer and the challenges to cybersecurity. We envisioned the telemetry network as a Purdue reference architecture. However, with the recent projects of the Department of Defense (DoD) such as JEDI, IIoT Reference architecture is also an alternative.

4. Conclusions

In this paper, we have captured a network-enhanced telemetry architecture for the purpose of modeling and analysis for cybersecurity risks. We show how telemetry systems can be modeled as an ICS-SCADA system that merges with an enterprise network. In addition, it shows how this architecture can be transformed into an IoT reference architecture to make use of cloud service capabilities. The main goal of this paper is to lay the network foundation to explore cybersecurity issues with an Integrated Network-Enhanced Telemetry architecture. This cyber domain is going to include vulnerabilities associated with ICS-SCADA, enterprise networks, and cloud networks. Future work will develop a cyber telemetry test bed for vulnerability analysis. It reflects our understanding of telemetry and SCADA and the commonalities and paves the way for our future work for the International Foundation for Telemetry (IFT). This will enable setting up and configuring a hybrid (hardware and virtual machine)-based telemetry testbed, exploring different domains of cyber vulnerability analysis, looking into different threat actors with an emphasis on insider attacks, and modeling and developing cyber defense methodologies.

Author Contributions: Conceptualization, W.Z. and R.D.; methodology, W.Z., R.D. and M.D.; writing—original draft preparation, W.Z. and M.D.; writing—review and editing, W.Z., R.D., M.D. and A.B.; supervision, R.D. and F.M.; project administration, R.D. and F.M.; funding acquisition, R.D. and F.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the International Foundation for Telemetering (IFT).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors in the Wireless Network Security Laboratory, Electrical and Computer Engineering department of Morgan State University would like to thank the International Foundation for Telemetering (IFT) for the funding of this project.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Grace, T.B.; Abbott, B.A. Telemetry Network Standards Overview. *Eur. Test Telem. Conf. ettc* **2018**, *2018*. [CrossRef]
2. Reynolds, R.S. IRIG Telemetry Standards 1969. In Proceedings of the International Telemetering Conference, Washington, DC, USA, 15–17 September 1969; Volume 5.
3. *Document 106-17 Telemetry Standards July 2017 Prepared by Telemetry Group*; Secretariat Range Commanders Council: US Army White Sands Missile Range, NM, USA, 2017.

4. Young, T. I integrated Network Enhanced Telemetry, iNET: Impacts to Telemetry Community, Distribution A: Approved for Public Release. 412TW-PA-18138. 17 May 2018. Available online: https://www.itea.org/wp-content/uploads/2018/05/Young-Tom.pdf (accessed on 2 April 2021).
5. Young, T. Integrated Network Enhanced Telemetry (iNET): Impact to the Telemetry Community for the ettc2018. In Proceedings of the European Test and Telemetry Conference, Nürnberg, Germany, 26–28 June 2018. [CrossRef]
6. Rakas, S.V.B.; Stojanović, M.D.; Marković-Petrović, J.D. A Review of Research Work on Network-Based SCADA Intrusion Detection Systems. *IEEE Access* **2020**, *8*, 93083–93108. [CrossRef]
7. Urias, V.; Leeuwen, B.V.; Richardson, B. Supervisory Command and Data Acquisition (SCADA) system Cyber Security Analysis using a Live, virtual, and constructive (LVC) testbed. In Proceedings of the 2012 IEEE Military Communications Conference, Orlando, FL, USA, 29 October–1 November 2012. [CrossRef]
8. Markovic-Petrovic, J.D.; Stojanovic, M.D. An Improved Risk Assessment Method for SCADA Information Security. *Elektron. Elektrotech.* **2014**, *20*, 69–72. [CrossRef]
9. Hu, Y.; Yan, A.; Li, H.; Sun, Y.; Sun, L. A survey of intrusion detection on industrial control system. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 1550147718794615. [CrossRef]
10. Nazir, S.; Patel, S.; Patel, D. Assessing and augmenting SCADA cyber security: A survey of techniques. *Comput. Secur.* **2017**, *70*, 436–454. [CrossRef]
11. Stojanovic, M.; Bostjancic-Rakas, S.; Markovic-Petrovic, J. SCADA systems in the cloud and fog environments: Migration scenarios and security issues. *Facta Univ. Ser. Electron. Energ.* **2019**, *32*, 345–358. [CrossRef]
12. Probst, C.; Hunker, J.; Bishop, M.; Gollman, D. Countering Insider Threats. *ENISA Q. Rev.* **2009**, *5*, 13–14.
13. Madon, P.; Young, T.; O'Brien, T.; Radke, M. Spectrum Management System—Frequency Assignment De-Confliction and RF Link Quality Prediction. In Proceedings of the International Telemetering Conference Proceedings, Glendale, AZ, USA, 5–8 November 2018; Volume 54.
14. Oyediran, D.; Dean, R.; Farzad, M. Spectrum sharing mac protocol applications for the proposed 3.5 GHz Band. *Int. Telem. Conf. Proc. Int. Found. Telem.* **2018**, *54*, 11.
15. U.S. Army Program Executive Office for Simulation Training & Instrumentation. Cyberspace Test Technology Science & Technology (CTT S&T) Test Technology Area (TTA). Broad Agency W900KK-12-R-0010 ISSUE DATE: 31 January 2012, Expiration Date: 30 September 2016.
16. Norman, R. Improving Distributed Test & Evaluation with JMETC & TENA. Joint Mission Environment Test Capability (JMETC) Program Overview; JMETC Program in; Test Resource Management Center (TRMC). 2018. Available online: https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2017/systems/Thursday/Track2/19925_Norman.pdf (accessed on 1 August 2020).
17. Arnwine, M. Cheaper, Faster, and with Less Risk Using Distributed Testing to Accelerate T&E Capabilities Joint Mission Environment Test Capability (JMETC), Joint Mission Environment Test Capability. 19 September 2012. Available online: https://www.itea.org/images/pdf/Events/2012_Proceedings/2012_Annual_Symposium/track_4_arnwine_cheaperfasterandwithlessriskusingdistributedtestingtoacceleratetecapabilities.pdf (accessed on 1 August 2020).
18. Macdonald, T. The DoD T&E/S&T Program, Test Resource Management Center: Net-Centric Systems Test (NST) Overview, Industry/Academia Days. 9 August 2011. Available online: https://web.wpi.edu/Images/CMS/ECE/Test_and_Evaluation-Tom_Macdonald(1).pdf (accessed on 1 August 2020).
19. Rumford, G. TheDoD T&E/S&T Program, NDIA. In Proceedings of the 12th Annual Science & Engineering Technology Conference, North Charleston, SC, USA, 21–23 June 2011.
20. US-CERT. Cybersecurity and Infrastructure Security Agency, Control Systems Security Program. US Department of Homeland Security, 2021. Available online: https://us-cert.cisa.gov/ics (accessed on 11 November 2020).
21. Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), NIST Special Publication 800-82 Revision 2. Available online: http://dx.doi.org/10.6028/NIST.SP.800-82r2 (accessed on 1 December 2020).
22. Galloway, B.; Hancke, G.P. Introduction to industrial control networks. *IEEE Commun. Surv. Tuts.* **2013**, *15*, 860–880. [CrossRef]
23. Cardenas, A.A.; Amin, S.; Sastry, S. Research Challenges for the Security of Control Systems. In Proceedings of the 3rd USENIX Workshop on Hot Topics in Security (HotSec '08), Associates with the 17th USENIX Security Symposium, San Jose, CA, USA, 29 July 2008.
24. Stouffer, K.; Falco, J.; Kent, K. *Guide to Supervisory Control and Data Acquisition (Scada) and Industrial Control Systems Security*; Sp800-82; NIST: Gaithersburg, MD, USA, 2006.
25. *Cybersecurity for Critical Infrastructure (ICS, SCADA &IIoT)*; Palo Alto Networks: Santa Clara, CA, USA, 2020.