Security Frameworks for Nanoscale Communication Networks

Frederick R. Carlson

Abstract Two new networks are the subject of intense research: terahertz networking and nanoscale molecular networking. Both are at the nano-scale and have enormous security implications, which have not yet been addressed. The IEEE recently released IEEE Standard 1906.1 - *Recommended Practice for Nanoscale and Molecular Communication Framework*, which provides the structure from which a security framework can be developed. This paper will undertake to scope these two networks with a security framework, which builds upon the NIST and ISO standards that currently articulate information security for electromagnetic processing and networking.

This paper will map the communication technologies that exist at the nanoscale and place them into a collection of four control domain groups - Access Control, Identification and Authentication, Audit and Accountability, and Systems/Communication Protection. It will then address Access Control and Systems/Communication Protection at the control level. Finally, the paper will provide a recommendation about the best control framework to begin to secure this new network space.

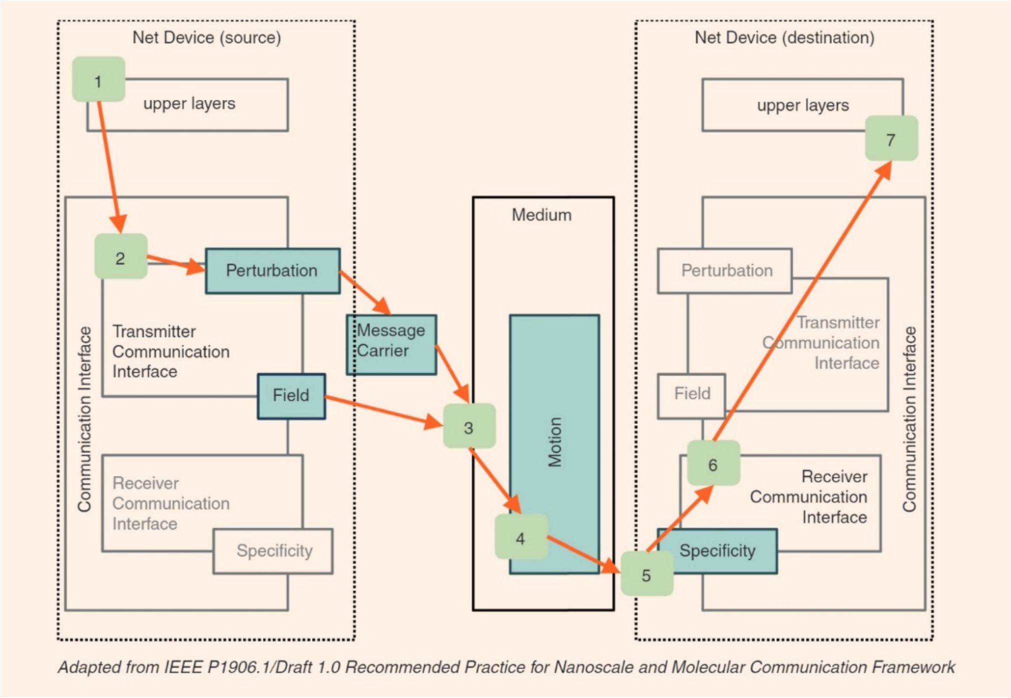
Research Question 1: Which type of standard is the better choice to secure terahertz and nanoscale molecular networks, a strategic framework, such as the International Standards Organization (ISO) 27000 family, or a more tactical framework, such as the National Institute of Standards and Technology (NIST) SP family of standards?

Research Question 2: Can existing control frameworks expand to address the topic of nanoscale networks at the NIST 800-53 control level of detail?

Keywords: communication networks, communication standards, communication systems, cybersecurity, IEEE 1906.1, information security, molecular communication, multi-scale network, nanobioscience, nanobiotechnology, nanobots, nanodevice, nanoelectrochemical systems, nanoelectromechanical systems, nanofluidics, nanomedicine, nanophysics, nanopositioning, nanoscale, nanoscale communication framework, nanoscale devices, nanosensors, nanostructured materials, nanotechnology, standards development, internet of things, security of information systems

Introduction

There is a current effort to create nanoscale communication networks across the globe. Figure 1 provides a systems-level view of a nanoscale communication network, including the relationship of the signal flow of nanoscale networks. This figure also depicts a general geometry, reference model and relationship diagram of the communications layers of nanoscale networks.



Adapted from IEEE P1906.1/Draft 1.0 Recommended Practice for Nanoscale and Molecular Communication Framework

Figure 1 - Nanoscale Network [1]

Generally, nanoscale communication networks function very differently from the familiar, widespread electromagnetically connected networks currently in use. Networks at the nanoscale can be based on carbon nanotubes, bacterial flagella, or molecular motors. A brief description is given for each of these nanoscale building blocks.

Carbon Nanotubes:

Carbon Nanotubes (CNT) appear like rolled chicken wire (polycyclic hexagonal) and are at the nanoscale in their diameter; they are extremely strong and can stretch to extreme lengths relative to their diameter. [2]

Bacterial flagellar motor:

Bacterial flagellar motors are extremely detailed “outboard motors” that some bacteria use to maneuver; they closely resemble mechanical motors. [3]

Molecular motor:

Molecular motors are like Bacterial flagellar motors with the difference being that there is significant human intervention in the design and function of these devices. [4]

The release of IEEE Standard 1906.1 – *Recommended Practice for Nanoscale and Molecular Communication Framework* ("IEEE 1906.1") created a standard lexicon and understanding of nanoscale communication. Nanoscale communication networks raise significant security concerns.

For example,

The insertion of nanomachines into our food or into invasive medical technology.

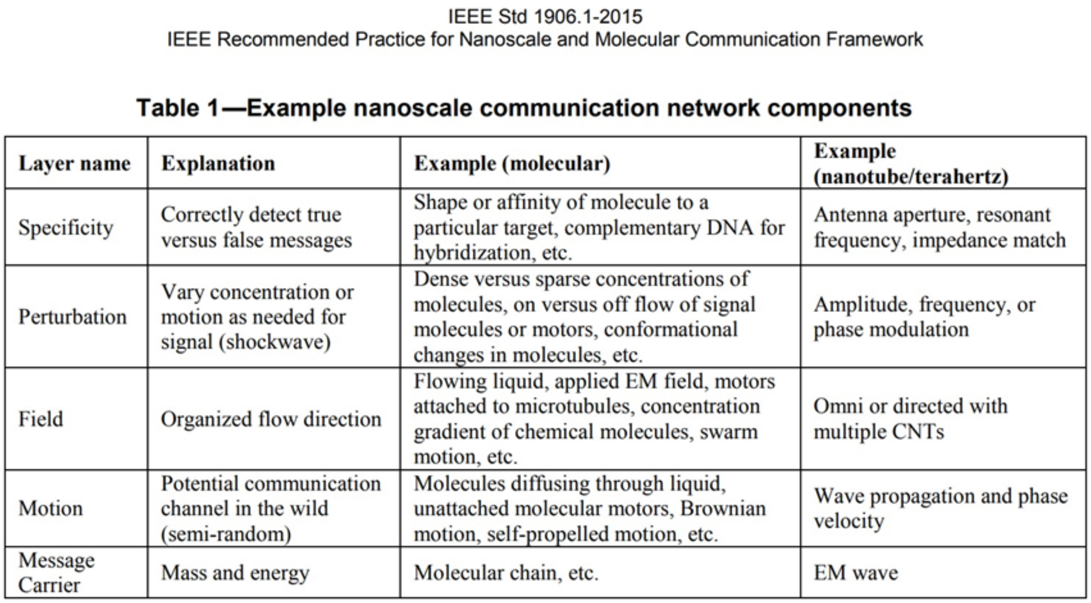
- The use of nanomachines to maliciously modify microscale and higher industrial control systems, particularly warning and safety systems.

- The use of nanomachines, combined with remote access technology to enhance the precision delivery of chemical and biological weapons. [5]

The publication of the IEEE 1906.1 offers the opportunity to "work by analogy" to identify one or more security control regimes, which can articulate the security implications of this technology. IEEE P1906.1 categorizes the signal flow from the source to destination in a manner that permits the insertion of a wide variety of technologies.

The rationale of IEEE 1906.1 was to resolve a communication issue between different nanoscale technical groups. IEEE 1906.1 provides the ability to bridge from one nanotechnology to another.

The processes of perturbation, field, message carrier, motion, and specificity can be used on a wide range of nanoscale technologies, from terahertz networking to the use of molecular machines and even to biological-based systems, such as bacterial flagellants. Figure 2 provides a useful context for the use of these processes.



IEEE Std 1906.1-2015
IEEE Recommended Practice for Nanoscale and Molecular Communication Framework

Table 1—Example nanoscale communication network components

Layer name	Explanation	Example (molecular)	Example (nanotube/terahertz)
Specificity	Correctly detect true versus false messages	Shape or affinity of molecule to a particular target, complementary DNA for hybridization, etc.	Antenna aperture, resonant frequency, impedance match
Perturbation	Vary concentration or motion as needed for signal (shockwave)	Dense versus sparse concentrations of molecules, on versus off flow of signal molecules or motors, conformational changes in molecules, etc.	Amplitude, frequency, or phase modulation
Field	Organized flow direction	Flowing liquid, applied EM field, motors attached to microtubules, concentration gradient of chemical molecules, swarm motion, etc.	Omni or directed with multiple CNTs
Motion	Potential communication channel in the wild (semi-random)	Molecules diffusing through liquid, unattached molecular motors, Brownian motion, self-propelled motion, etc.	Wave propagation and phase velocity
Message Carrier	Mass and energy	Molecular chain, etc.	EM wave

Figure 2 - Nanoscale Network Components [6]

In the same way that the creation of the Open Systems Interconnect (OSI) model was significant for the Internet, IEEE 1906.1 is important for the deployment of nanonetworks. By modularizing the signaling characteristics of nanoscale computing, engineers now have a way to "glue" their systems together and build protocols on top of the reference model. If IEEE 1906.1 follows the same trajectory as the OSI model for the Internet, rapid growth in systems, protocols, and applications using IEEE 1906.1 referenced networks may follow.

As a result of IEEE 1906.1, it is now feasible to investigate the security control frameworks that can be employed to manage the security implications of nanoscale communication networks. This paper will be inductive and use an analogy to propose control systems that manage capabilities of similar import and look to adapt them for use in securing these systems.

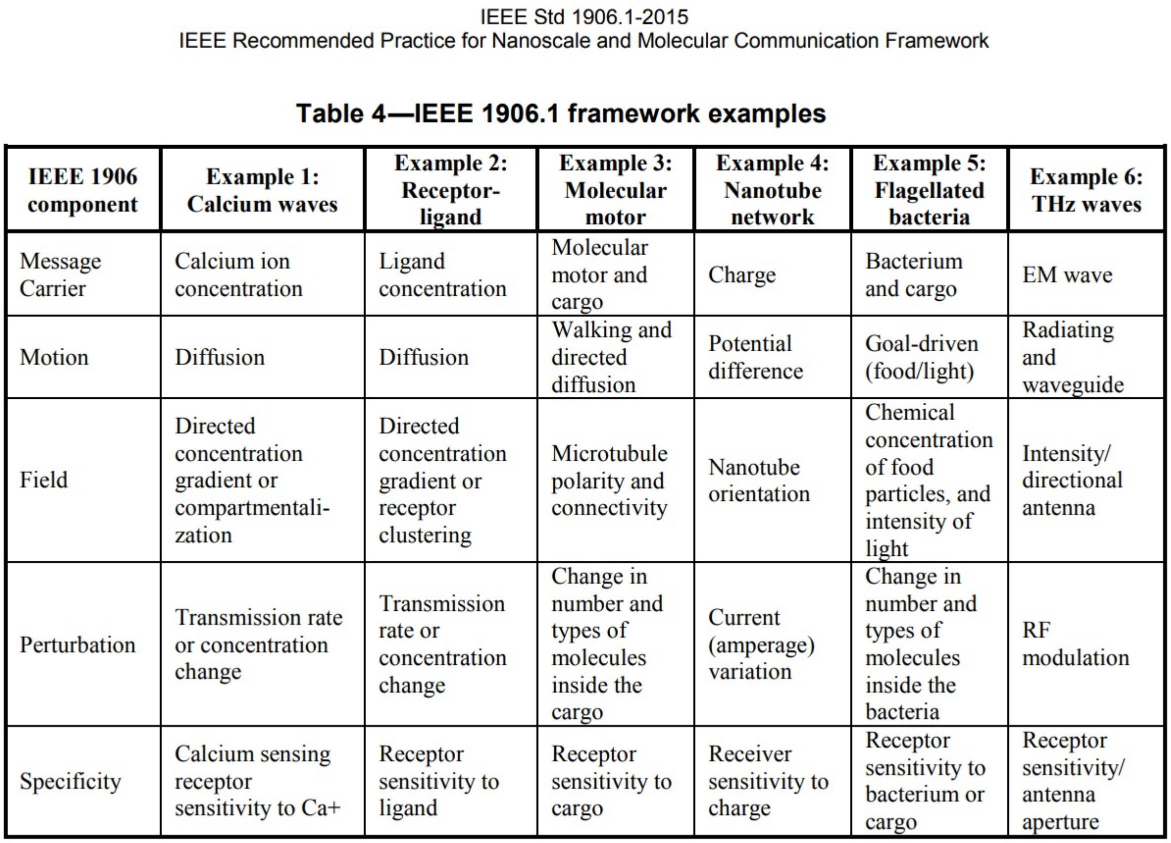
Nanoscale Communication Networks

Since there is a wide range of nanoscale communication networks from Terahertz networks to Nanotube-based communication systems, the chances of finding one security control framework that can adapt to this variety are slim. It is likely that more than one nanoscale security framework will be needed to address this problem.

There is a variable range of network transmission mechanisms in Nanoscale and Molecular Communications Systems, as illustrated in Figure 3 below. The universe of Nanoscale Systems ranges from diffused calcium waves to ligand receptors to molecular motors, to nanotubes, to flagellated bacteria, and finally to Terahertz networking.

This paper has touched on Molecular Motors, Flagellated Bacteria Motors, and THz waves. Two additional components are listed below, the “Receptor-ligand” and “Calcium Waves.” The first new component. “Receptor-ligand” describes the signal path of cellular communication with the interaction between the receiving molecule, the “receptor” and the traveling (or signaling) molecule, the ligand. The second new component, “Calcium Waves,” is a similar process. Cells use changes in calcium levels as a communication mechanism, usually through cell regions. [7]

Figure three also shows the IEEE 1906 components. By breaking this network into these components rather than attempting to invent protocol data units that are the analog to this in conventional networking, the standard allows a more efficient classification. This framework will allow different types of nanoscale networks to have a framework for interoperability, say between molecular motors and terahertz waves.



IEEE Std 1906.1-2015
IEEE Recommended Practice for Nanoscale and Molecular Communication Framework

Table 4—IEEE 1906.1 framework examples

IEEE 1906 component	Example 1: Calcium waves	Example 2: Receptor-ligand	Example 3: Molecular motor	Example 4: Nanotube network	Example 5: Flagellated bacteria	Example 6: THz waves
Message Carrier	Calcium ion concentration	Ligand concentration	Molecular motor and cargo	Charge	Bacterium and cargo	EM wave
Motion	Diffusion	Diffusion	Walking and directed diffusion	Potential difference	Goal-driven (food/light)	Radiating and waveguide
Field	Directed concentration gradient or compartmentalization	Directed concentration gradient or receptor clustering	Microtubule polarity and connectivity	Nanotube orientation	Chemical concentration of food particles, and intensity of light	Intensity/ directional antenna
Perturbation	Transmission rate or concentration change	Transmission rate or concentration change	Change in number and types of molecules inside the cargo	Current (amperage) variation	Change in number and types of molecules inside the bacteria	RF modulation
Specificity	Calcium sensing receptor sensitivity to Ca+	Receptor sensitivity to ligand	Receptor sensitivity to cargo	Receiver sensitivity to charge	Receptor sensitivity to bacterium or cargo	Receptor sensitivity/ antenna aperture

Figure 3 - Nanoscale Network Examples [8]

Figure 4, Wireless Use Case, shows a comparatively conventional proposal for the use of these networks. The nodes inside the human figure are nanoscale networks involved in one, all, or more - healthcare informatics, diagnosis, cure, or symptom management. The different nanoscale subsystems have gateways that join to a common network node, which also functions to take the nanoscale information to the microscale, where it can join a command and control network on a TCP/IP based Internet connection.

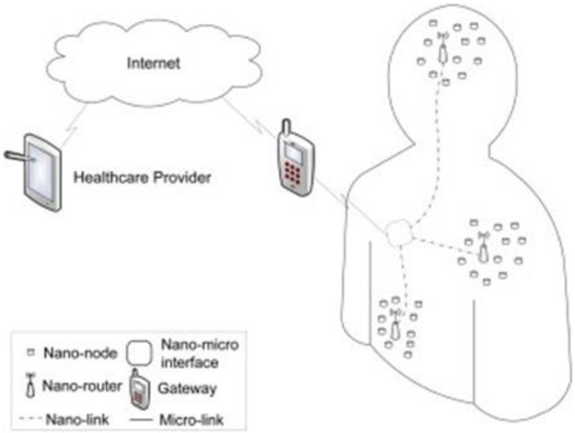


Figure 4 - Wireless Use Case [9]

Relationship of Nanoscale Communication Standards to the OSI 7 Layer Model

IEEE 1906.1 provides a mapping of the nanoscale components to the OSI Seven Layer Model.

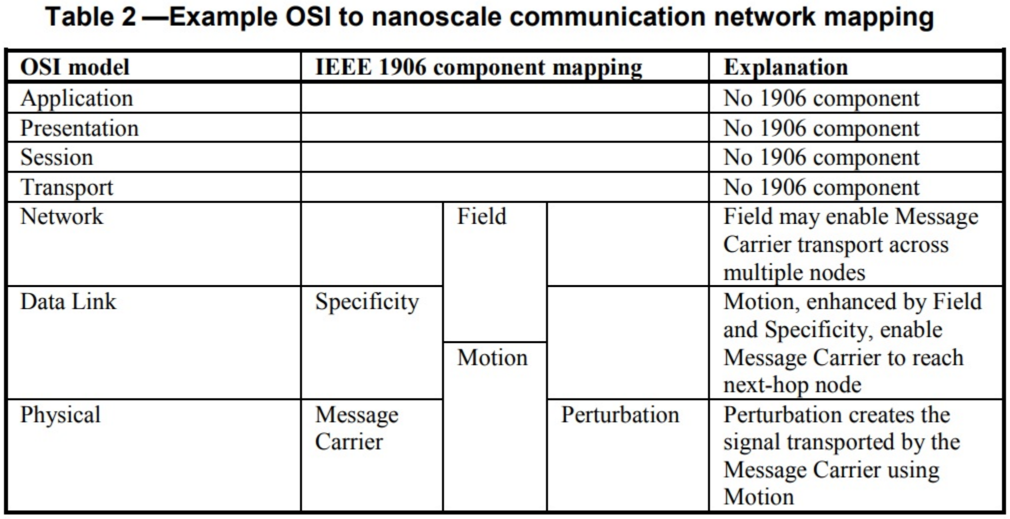


Table 2 —Example OSI to nanoscale communication network mapping

OSI model	IEEE 1906 component mapping			Explanation
Application				No 1906 component
Presentation				No 1906 component
Session				No 1906 component
Transport				No 1906 component
Network		Field		Field may enable Message Carrier transport across multiple nodes
Data Link	Specificity	Motion		Motion, enhanced by Field and Specificity, enable Message Carrier to reach next-hop node
Physical	Message Carrier		Perturbation	Perturbation creates the signal transported by the Message Carrier using Motion

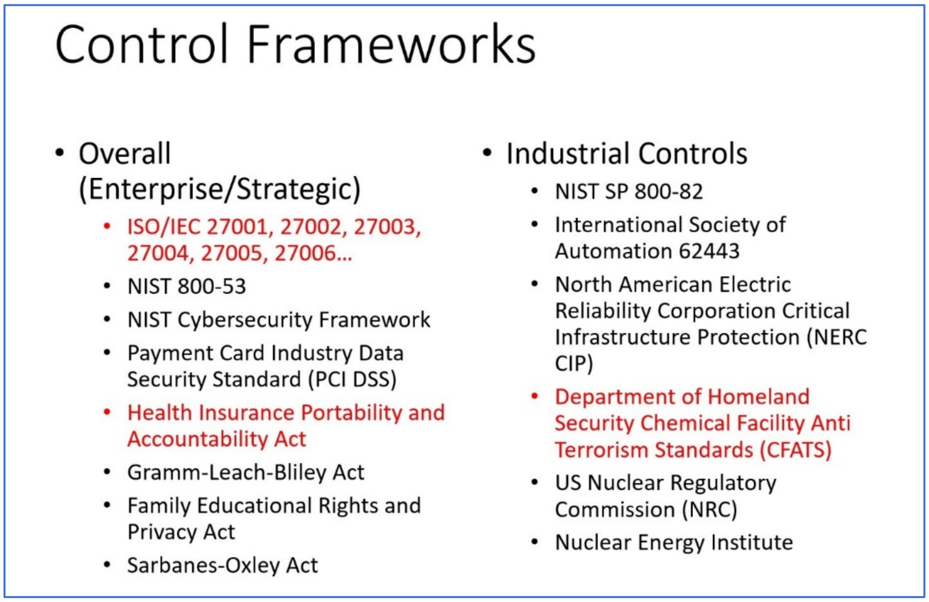
Figure 5 - Mapping of IEEE 1906.1 Standards to the OSI Model [10]

Importantly, there are no nanoscale components that are analogous to the four upper layer protocol data units. As a result, IEEE 1906.1 directs the security control frameworks to the three bottom layers. This structure differs significantly from the current model, as these frameworks have tended to drift up the OSI stack in recent years. The disconnected, message-based network creates significant localization, addressing, classification and segmentation problems and sets the opening moves to secure these systems to the areas of access control and boundary enforcement. This lack of upper protocol intelligence has significant implications for security. One issue is a persistent lack of state which leads to localization issues much like communications in other harsh environments. Fortunately, there is a significant body of work in “Delay Tolerant Networking” that has been around for nearly fifty years. This means that while IEEE 1906.1 has no real answers for connection-oriented networking; there is still a body of knowledge where we can begin to enforce boundaries.

The “field” component (organized flow direction) is the only obvious choice to attempt to segment and bound these types of networks. The IEEE 1906.1 field component is somewhat similar to TCP/UDP based filters, such as stateless firewalls (router access lists). The field flow direction component may be the location to use as the gateway between high trust and low trust network segments.

Security Control Standards and Frameworks

Figure 6, Security Control Frameworks, organizes popular security control frameworks into two categories, Overall (Enterprise/Strategic) and Industrial Controls. This section will examine the following control frameworks as candidates to create a control framework focused on nanoscale systems: ISO 27001, the Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST) SP 800-82, NIST 1800-8, Securing Wireless Infusion Pumps, and the NIST 800-53 Security Control framework.



Control Frameworks

- Overall (Enterprise/Strategic)
  - ISO/IEC 27001, 27002, 27003, 27004, 27005, 27006…
  - NIST 800-53
  - NIST Cybersecurity Framework
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Health Insurance Portability and Accountability Act
  - Gramm-Leach-Bliley Act
  - Family Educational Rights and Privacy Act
  - Sarbanes-Oxley Act
- Industrial Controls
  - NIST SP 800-82
  - International Society of Automation 62443
  - North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
  - Department of Homeland Security Chemical Facility Anti Terrorism Standards (CFATS)
  - US Nuclear Regulatory Commission (NRC)
  - Nuclear Energy Institute

Figure 6 - Security Control Frameworks [11]

Evolution of Nanoscale Networks – 3 Cases

The evolution of nanoscale networks can be divided into three cases. Figure 7, Nanoscale Network

Evolution, shows a probable evolution of nanonetworks over time. The use case is an evolution of a medical infusion pump.

Figure 7 shows the evolution of an infusion pump that is currently governed by the NIST 1800-8

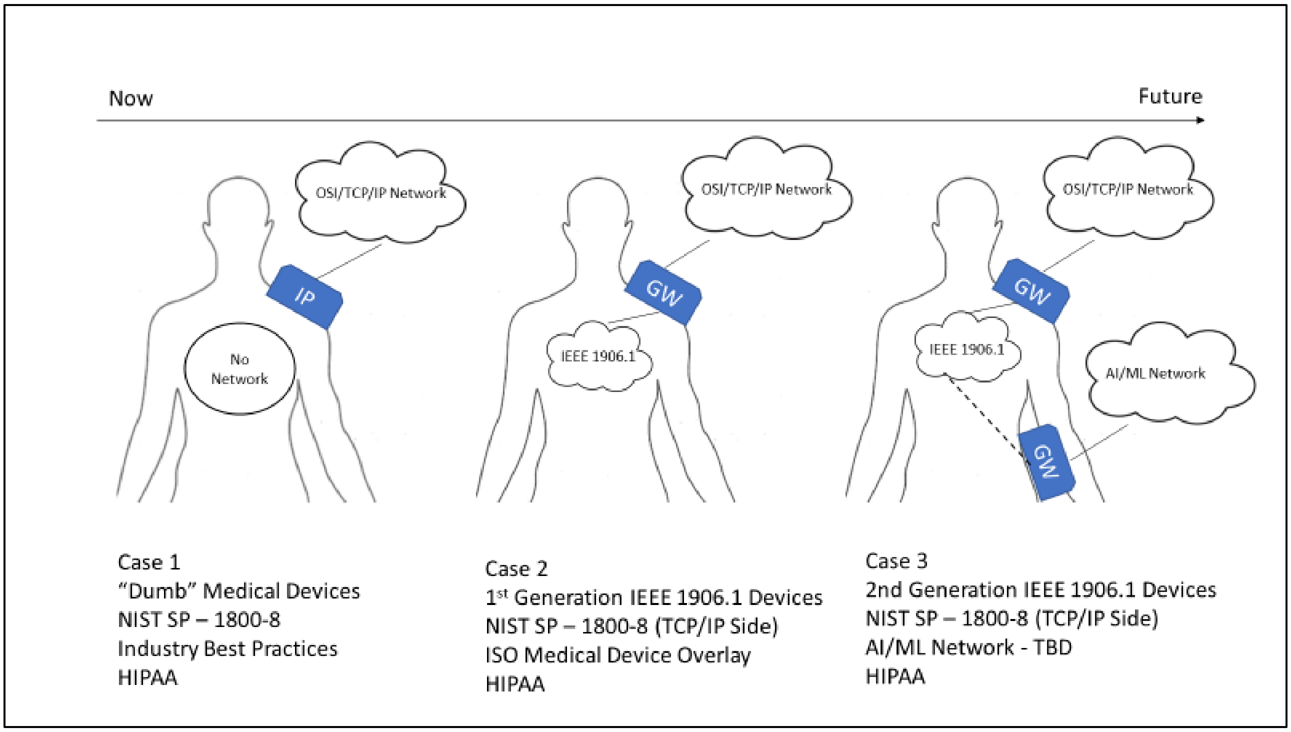


Figure 7- Nanoscale Network Evolution [12]

Standard to a first-generation IEEE 1906.1 Network and then to a second-generation IEEE 1906.1 network. Network connectivity conforming to the Open Systems Interconnect (OSI) standard is assumed in all three cases and a gateway device "GW" is shown for case two and three connecting the OSI Network to the IEEE 1906.1 network. Case three has a second gateway for connectivity to an artificial intelligence/machine learning network. That network is shown under the assumption that an AI/ML capability will be needed at some point to manage the IEEE 1906.1 network.

Nanoscale Threats and Vulnerabilities

The following tables are a summary of threats for the three cases: [13]

Threats	**Vulnerabilities**
Targeted Attacks	Lack of Encryption at Rest
Advanced Persistent Threats	Lack of Encryption in Motion
Malware Infections	Lack of Data Validation
Unintentional Misuse	Lack of sufficient Data Backup
Theft	Privacy Breach
Denial of Service	Improper third-party vendor connections
Vulnerable Systems physically connected to the device	Lack of Tamper Protection and Warning

Table 1 - Case 1: IP Connected Infusion Pumps [14]

Threats	**Vulnerabilities**
Targeted Attacks	Lack of Encryption at Rest
Advanced Persistent Threats	Lack of Encryption in Motion
Malware Infections	Lack of Data Validation
Unintentional Misuse	Lack of sufficient Data Backup
Theft	Privacy Breach
Denial of Service	Improper third-party vendor connections
Vulnerable Systems physically connected to the device	Lack of Tamper Protection and Warning
Man in the Middle	Delay Tolerant Networking susceptible to spoofing attacks
	Lack of Localization on DTN side of network.

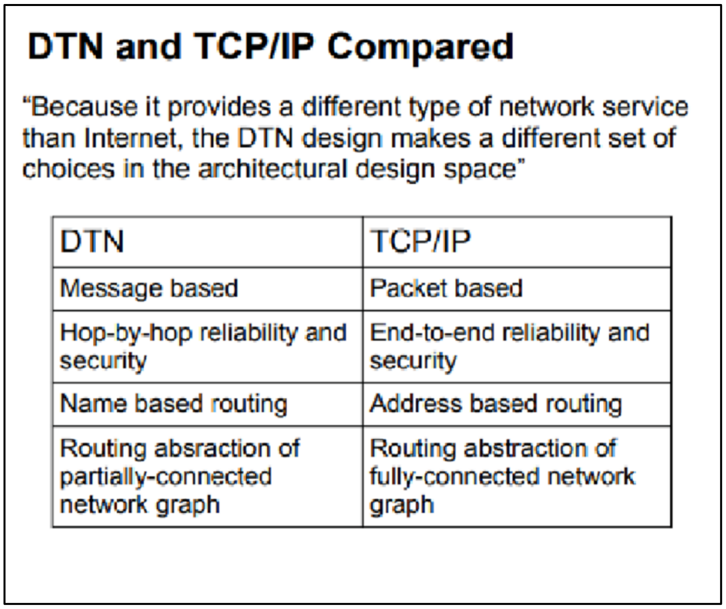
Table 2 - Case 2 - IEEE 1906.1 1st Generation [15]

Threats	**Vulnerabilities**
Targeted Attacks	Lack of Encryption at Rest
Advanced Persistent Threats	Lack of Encryption in Motion
Malware Infections	Lack of Data Validation
Unintentional Misuse	Lack of sufficient Data Backup
Theft	Privacy Breach
Denial of Service	Improper third-party vendor connections
Vulnerable Systems physically connected to the device	Lack of Tamper Protection and Warning
Man in the Middle	Delay Tolerant Networking (DTN) susceptible to spoofing attacks
Backdoor connection of AI network to IP network using IEEE 1906.1 as a transit route.	Lack of Localization on DTN side of the network.

Table 3 - Case 3 - IEEE 1906.1 2nd Generation [16]

Delay Tolerant Networking

IEEE 1906.1 compliant networks will almost certainly communicate using a somewhat esoteric method of data networking known as delay-tolerant networking (DTN). DTN was designed for extremely harsh communication environments and is positioned to become more widely adopted as technologies such as the Internet of Things (IoT) enter the mature phase of the product lifecycle. But, DTN has extremely limited addressing and localization functions. The utility of DTN will be diminished, therefore, because a security framework must address localization, which is a significant architectural issue. [17]
DTN communicates opportunistically by a store and forward method. An example is a satellite system that is masked from its ground station. DTN will hold the message until the ground station is within range, or, more interestingly, forward the message via broadcast to a node that can relay to the station. DTN is much different from IP networking because the latter knows the address of the packet it wishes to send. Figure 8, Differences between IP and DTN networks, shows the high-level differences between the two networks.



DTN and TCP/IP Compared

"Because it provides a different type of network service than Internet, the DTN design makes a different set of choices in the architectural design space"

DTN	TCP/IP
Message based	Packet based
Hop-by-hop reliability and security	End-to-end reliability and security
Name based routing	Address based routing
Routing absraction of partially-connected network graph	Routing abstraction of fully-connected network graph

Figure 8 - Differences between IP and DTN Networks [18]

Figure 9, System Level Diagram of IP to DTN communications, shows the interplay between these networks via a gateway. Using the IEEE 1906.1 terminology, we have the "field" layer on the DTN (NanoNet) side of the gateway and the "network" layer on the IP side of the gateway. It is important to note that DTN nodes and links may "die" after (or before) retransmitting the signal. This behavior is not the case with IP Routing which will forward if there is a route or will drop the packet if there is not a route.

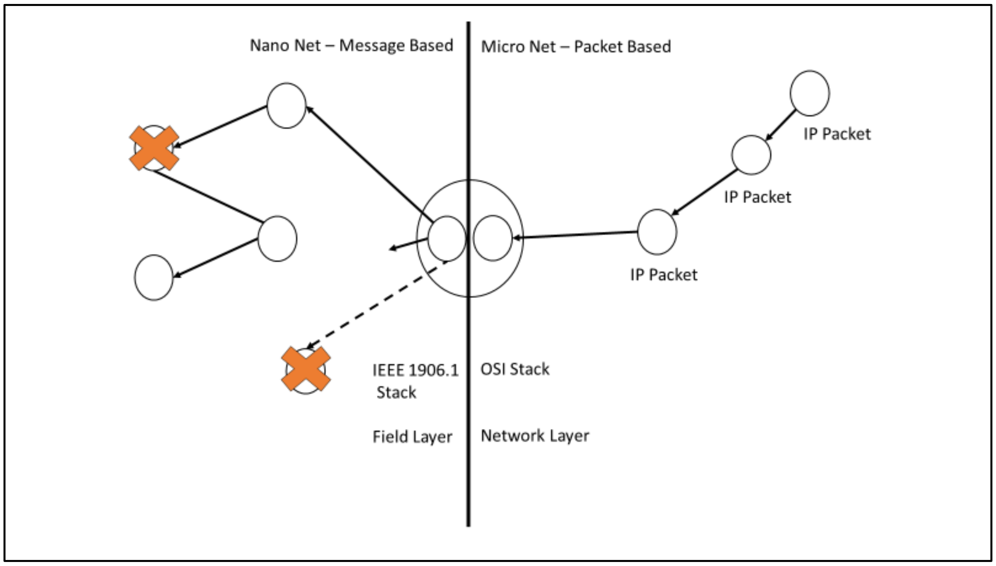
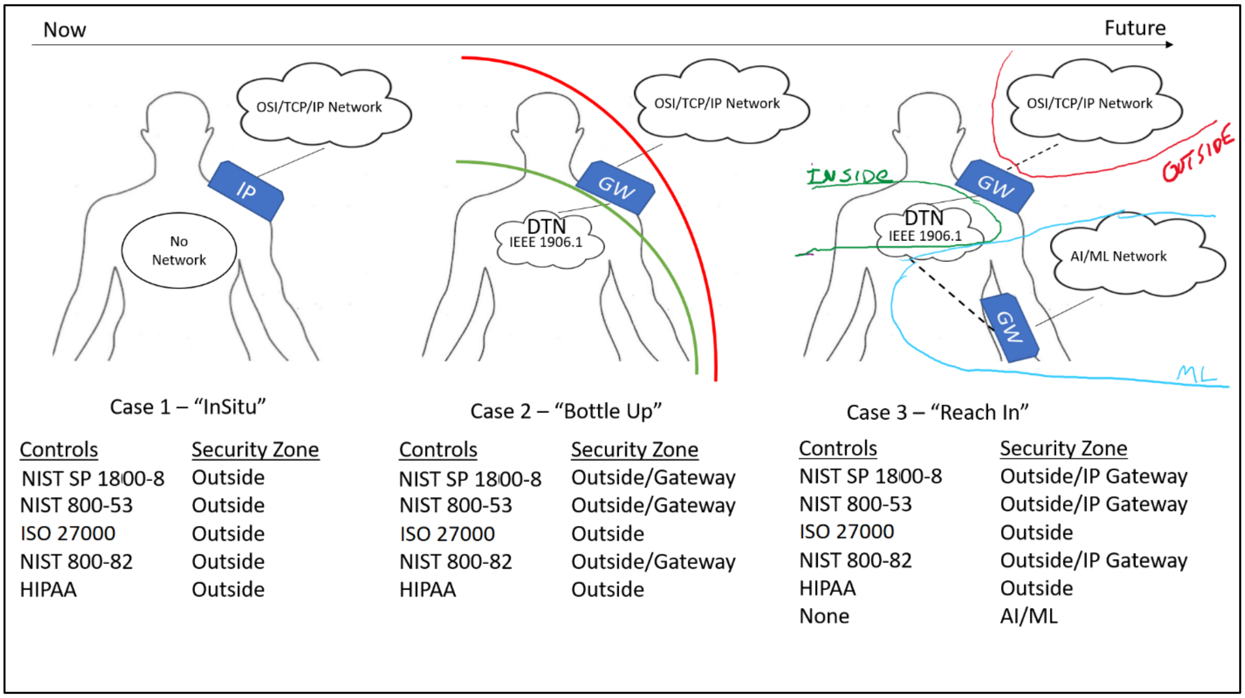


Figure 9 - System Level Diagram of IP to DTN communications [19]

A few notes here about Figure 9. First, on the left-hand side of the gateway (Nano-Net) notice that the signal can be stopped either by a node dying after transit or a transmission getting lost in the noise. This robustness is not the case with IP routing (nuclear war survivability myths notwithstanding), where the packet is routed to its destination in a deterministic way. DTN has no real end to end path and is akin to a simple broadcast network that opportunistically finds neighbors and communicates when it can. This makes DTN the only current candidate to achieve communications in the extremely harsh environment of the human body. The problem is that, again, this freewheeling protocol may work well, but has very little chance to be secured without much help. [20] [21]

Research Question Number One

Can we use a strategic framework like the International Standards Organization to secure these new networks or is a more tactical framework like the National Institute of Standards and Technology (NIST) SP family of standards a more reasonable choice? This question may be answered by revisiting the use cases and dividing the cases into security enclaves. Figure 10, Control Frameworks and Security Zones, shows these enclaves at the top of the graphic and the relevance of the zone to a specific control family, or in the case of HIPAA, federal law, at the bottom of the graphic.



Case 1 – "InSitu"

Controls	Security Zone
NIST SP 1800-8	Outside
NIST 800-53	Outside
ISO 27000	Outside
NIST 800-82	Outside
HIPAA	Outside

Case 2 – "Bottle Up"

Controls	Security Zone
NIST SP 1800-8	Outside/Gateway
NIST 800-53	Outside/Gateway
ISO 27000	Outside
NIST 800-82	Outside/Gateway
HIPAA	Outside

Case 3 – "Reach In"

Controls	Security Zone
NIST SP 1800-8	Outside/IP Gateway
NIST 800-53	Outside/IP Gateway
ISO 27000	Outside
NIST 800-82	Outside/IP Gateway
HIPAA	Outside
None	AI/ML

Figure 10 - Control Frameworks and Security Zones

Figure 10 shows our three use cases with three names for the security strategy that presents itself. The first case "InSitu," is simply a dumb device that communicates with a client with no real network level knowledge of anything on the inside of the device, represented by a human body. The second case, "Bottle Up," is a situation where all intelligence is brokered through the gateway. There is only sparse security communication inside the DTN, mostly centered around integrity and boundary controls. It was a close call not to have NIST 800-53 as having an impact on the inside security zone, but the enforcement of any 800-53 control must happen at the gateway.   The last case, “Reach In,” is highly speculative but essentially shows a case where security controls will hold up like case two, except for the out of band AI/ML network, which there are no existing security controls that I could locate.

What this picture shows is that we can build by analogy with both the NIST and OSI frameworks, but the NIST framework can probably be used more rapidly in case 2 because of the security strategy of boundary enforcement through the “nano to micro” gateway.

Case 3, “Reach-In,” has the same answer as Case 2 for boundary enforcement and access control from the DTN to the IP network, but has no answer from the NIST or OSI frameworks on the myriad issues regarding the use of AI to govern nanonetworks. [22] This is where the OSI international and very strategic level approach will have value.

The answer to this research question is that the tactical control frameworks like NIST will hold up if we have a microprocessor centered network as a gateway. However, when the technology becomes available to do security command and control directly on the nanomachines, this almost certainly means AI, which means a complete strategic rethink. The ISO is probably the organization that has the staffing and expertise to design an entirely new control framework, which will be needed for case 3.

Research Question Number Two

Can existing control frameworks expand to address the topic of nanoscale networks at the control level of detail?

Figure 11 shows the NIST 800-53 Control Families: [23]

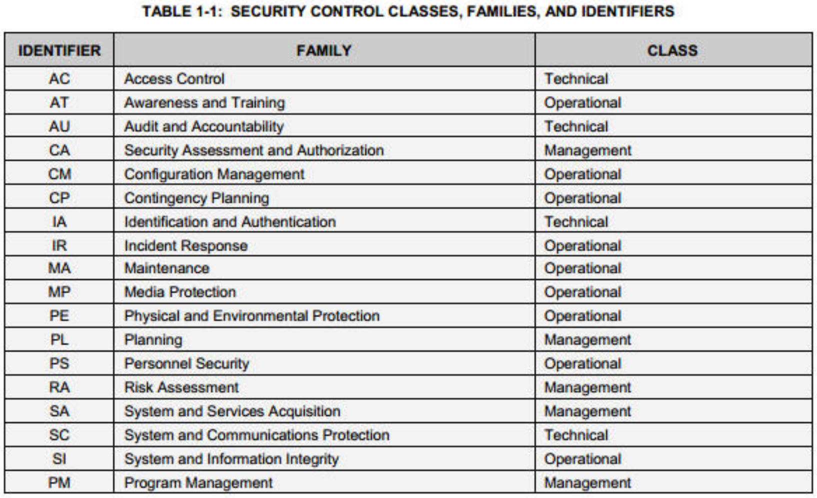


TABLE 1-1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

Figure 11 - NIST 800-53 Control Families

Two control families are selected to determine if they can be extended from the world of IP networking to the world of DTN networking. The control families that are selected are Access Control – AC and Systems and Communications Protection – SC.   We further select two controls, one from each group. They are AC-4 – Information Flow and SC-7 – Boundary Protection.

Second level Control #1 – AC4: Information Flow.

Figure 12, AC4: Information Flow in an IEEE 1906.1 Environment shows two control measures for doing dynamic information flow control. The first control is on the IEEE 1906.1 network and is a "DTN Bastion," which is an integrity check on the DTN network in the form of a message inspection. [24] On the IP network we have a generic time to live (TTL) limitation feature common to several OSI referenced networks (the most well-known being Border Gateway Protocol).

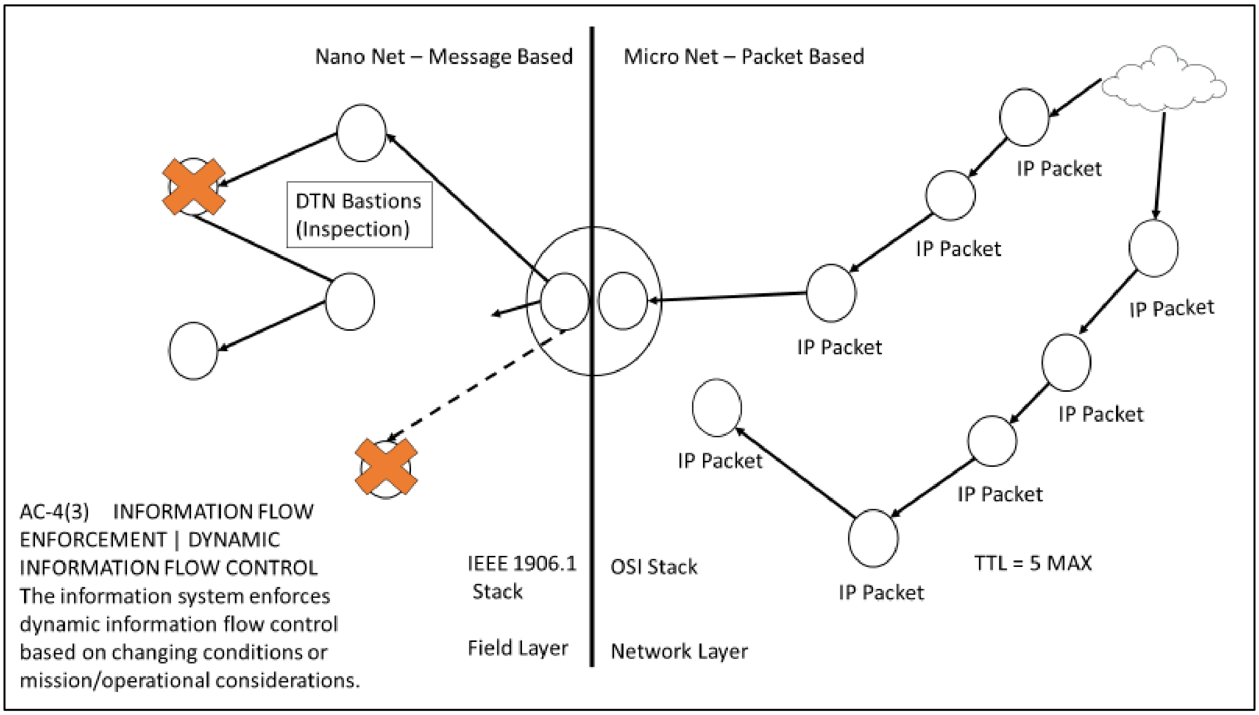
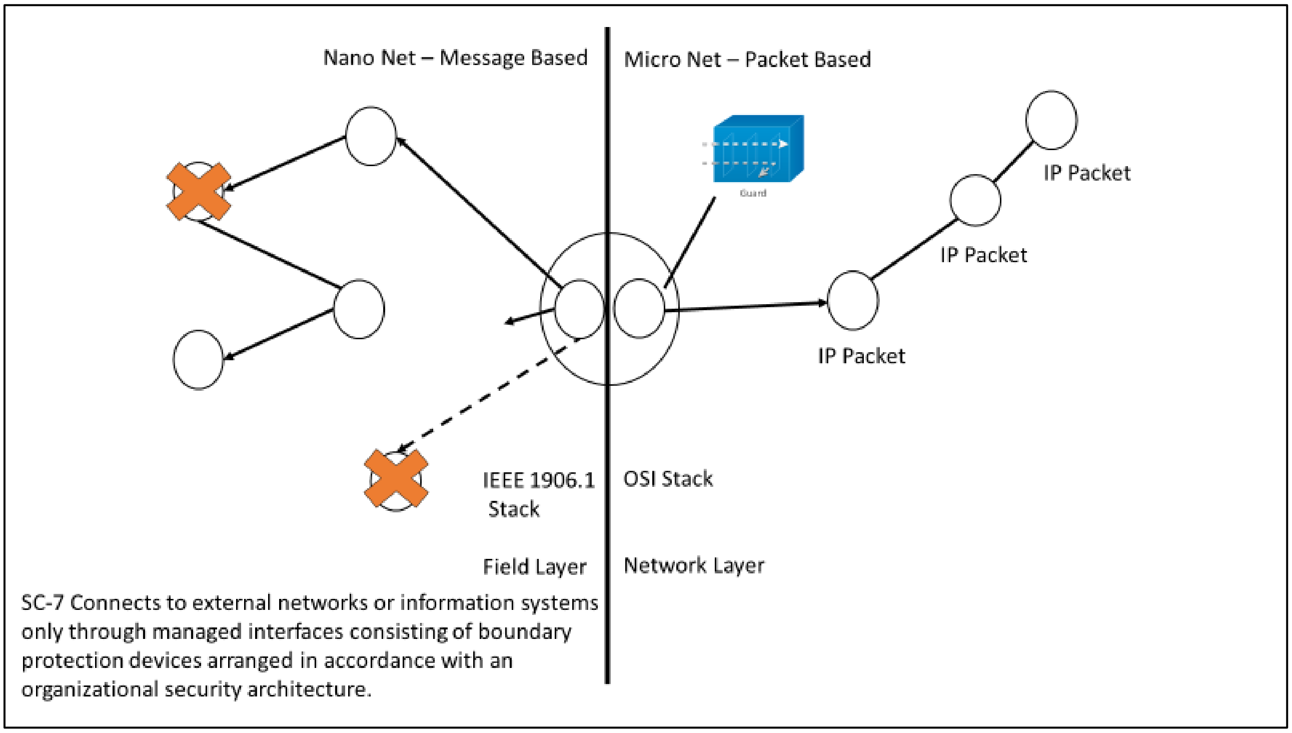

Nano Net – Message Based
Micro Net – Packet Based
DTN Bastions (Inspection)
IP Packet
IP Packet
IP Packet
IP Packet
IP Packet
IP Packet
IP Packet
IP Packet
TTL = 5 MAX
IEEE 1906.1 Stack
Field Layer
OSI Stack
Network Layer
AC-4(3) INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL
The information system enforces dynamic information flow control based on changing conditions or mission/operational considerations.

Figure 12 - AC4: Information Flow in an IEEE 1906.1 Environment [25] [26]

Second level Control #2 – SC-7 Boundary Protection

Figure 13, SC7 – Boundary Control, shows a somewhat extreme insertion of a TCP/IP One Way Guard on the OSI (or Micro) side of the network boundary. This example reinforces the flexibility security professionals will have on the Micronet side of the boundary.



SC-7 Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Figure 13 - SC7 - Boundary Control [27]

If the OSI portion of the network is in play, it stands to reason that the NIST family of controls, probably all of them, can be used at the control level. This condition only holds for case 2.

Conclusion

Nanonetworks will progress in a way that will allow control standards to remain relevant in the mid run and they can be extended by analogy or using overlays. At the operational and tactical level, we can use the NIST standards to “build on success” via analogy. This “work by analogy” provides the greatest chance of success to have a new standards committee convened to address this issue at the strategic level.

Looking to the future, the adoption of AI in the operational management of nanoscale communication networks will trigger game-changing security requirements. The use of NIST controls to “bottle up” the network within the DTN to IP gateway will fall apart rapidly. In preparation, ISO should commence work on a foundational security framework for nanoscale communication networks, much as it did years ago in developing the ISO 27000 security specifications. [28] [29]

Notes

1. Bush, Stephen F. "On Information Assurance in Nanoscale Networks." In Proceedings of the 3rd Annual Symposium on Information Assurance. Proceedings of 3rd Annual Symposium on Information Assurance (ASIA ’08), Empire State Plaza, Albany. Accessed January 12, 2018. https://www.albany.edu/iasymposium/proceedings/2008/12-BushEdit.pdf.

2. "CNT Technology Overview." What Are Carbon Nanotubes? Accessed February 01, 2018. https://www.nanoscience.com/applications/education/overview/cnt-technology-overview/.

“A carbon nanotube (CNT) is a tube-shaped material, made of carbon, having a diameter measuring on the nanometer scale. CNT is unique because the bonding between the atoms is very strong and the tubes can have extreme aspect ratios. A carbon nanotube can be as thin as a few nanometers yet be as long as hundreds of microns. To put this into perspective, if your hair had the same aspect ratio, a single strand would be over 40 meters long.”

“Uses for carbon nanotubes is in structural reinforcement, heat sourcing, insulators, semiconductors and chemical carriers. Specific drugs can be attached to a CNT that can target and attack only certain types of cells, including cancer cells.”

3. Xue, Ruidong, Qi Ma, Matthew A. B. Baker, and Fan Bai. "A Delicate Nanoscale Motor Made by Nature—The Bacterial Flagellar Motor." Advanced Science. September 2015. Accessed February 01, 2018. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5115386/.

“The bacterial flagellar motor (BFM) is a molecular complex ca. 45 nm in diameter that rotates the propeller that makes nearly all bacteria swim. The motor self-assembles out of ca. 20 different proteins and cannot only rotate at up to 50 000 rpm but can also switch rotational direction in milliseconds and navigate its environment to maneuver, on average, towards regions of greater benefit. The BFM is a pinnacle of evolution that informs and inspires the design of novel nanotechnology in the new era of synthetic biology.”

4. “Molecular Motors.” Accessed February 01, 2018. http://www.cs.unc.edu/~nanowork/motors/index.html.

“One of the central themes of nanotechnology is the scaling down of electromechanical devices or machines to the molecular scale. In this project, we pursue this goal with the help of nanomachine systems that nature has already created: ‘biomotors’ or ‘molecular motors.’”

“Within every living cell is a complex highway system of tiny motors that move along filamentous tracks. Biomotors and the tracks they move on are ubiquitous in the myriad processes occurring within the cell. They are responsible for muscle contraction, cell division, and transport of vesicles. They also power bacteria’s flagella and the cilia in our lungs. These systems serve a host of other cellular functions, many of which we are only beginning to understand. For example, these ‘highway systems’ which serve structural, transport and motility purposes, may also provide a communication function across the intercellular environment.”

5. Dressler, F., and F. Kargl. "Security in Nano Communication: Challenges and Open Research Issues."

“Assuming wide-spread use of nano communication, it is only logical to assume malicious actors trying to negatively affect nano communication in the same way as it happens today in the Internet. Given the criticality of the envisioned application domains and the close embedding of nano machines into our environment, food, or even our body, manipulation of such processes could have disastrous consequences, far beyond what a normal Internet attack would be able to achieve. Examples of such attacks may include:

• Disruption of medical applications, e.g. drug delivery, in order to harm or kill persons using specific substances or radio communication;

• Interfering communication with denial-of-service attacks to prevent alarms in industrial communication, e.g., when water is intoxicated;

• Modifying operation of nano-machines in environmental applications.”

6. Bush, Stephen F., and Andrew Eckford, eds. IEEE Recommended Practice for Nanoscale and Molecular Communication Framework. New York: IEEE, 2016.

7. Ibid.

8. Ibid.

9. Akyildiz, Ian F., and Josep Miquel J. "Electromagnetic Wireless Nanosensor Networks." Nano Communication Networks. May 02, 2010. Accessed January 27, 2018. https://www.sciencedirect.com/science/article/pii/S1878778910000050.

10. Bush, Stephen F., and Andrew Eckford, eds. IEEE Recommended Practice for Nanoscale and Molecular Communication Framework. New York: IEEE, 2016.

11. Bodungen, Clint E., Bryan L. Singer, Aaron Shbeeb, Stephen Hilt, and Kyle Wilhoit. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions. New York: McGraw-Hill Education, 2017.

12. United States. Department of Commerce. National Institute of Standards and Technology. Securing Wireless Infusion Pumps in Healthcare Delivery Organizations. By Gavin O'Brien, Sallie Edwards, Kevin Littlefield, Neil McNab, Sue Wang, and Kangmin Zheng. May 1, 2017. Accessed January 27, 2018. https://www.nccoe.nist.gov/publication/1800-8/.

13. Ibid.

14. Ibid.

15. Ibid.

16. Ibid.

17. Farrell, Stephen and Cahill, Vinny "Security considerations in space and delay tolerant networks," 2nd IEEE International Conference on Space Mission Challenges for Information Technology (SMC-IT'06), Pasadena, CA, 2006.

18. Fall, Kevin. "A Delay-Tolerant Network Architecture for Challenged Internets." SIGCOMM [03. https://www.cs.cmu.edu/~prs/15-744-F12/lectures/DTN-Sam.pdf

19. Cerf, Vint. "RFC 4838 - Delay-Tolerant Networking Architecture." IETF. Accessed January 27, 2018. https://www.ietf.org/rfc/rfc4838.txt.

20. Bush, Stephen. Nanoscale Communication Networks. Boston: Artech House, 2010.

21. Farrell, Stephen and Cahill, Vinny "Security considerations in space and delay tolerant networks," 2nd IEEE International Conference on Space Mission Challenges for Information Technology (SMC-IT'06), Pasadena, CA, 2006.

22. Bostrom, Nick. Superintelligence: Paths, Dangers, Strategies. 2014.

23. United States. Department of Commerce. National Institute of Standards and Technology. Recommended Security Controls for Federal Information Systems and Organizations. By Joint Task Force Transformation Initiative. Accessed May 1, 2010. https://csrc.nist.gov/publications/detail/sp/800-53/rev-3/archive/2010-05-01.

24. Farrell, Stephen and Cahill, Vinny "Security considerations in space and delay tolerant networks," 2nd IEEE International Conference on Space Mission Challenges for Information Technology (SMC-IT'06), Pasadena, CA, 2006.

25. Cerf, Vint. "RFC 4838 - Delay-Tolerant Networking Architecture." IETF. Accessed January 27, 2018. https://www.ietf.org/rfc/rfc4838.txt.

26. Recommended Security Controls for Federal Information Systems and Organizations. By Joint Task Force Transformation Initiative. Accessed May 1, 2010. https://csrc.nist.gov/publications/detail/sp/800-53/rev-3/archive/2010-05-01.

27. Ibid.

28. Kurzweil, Ray. The Singularity Is Near: When Humans Transcend Biology. 2016.

29. Drexler, K. Eric. Engines of Creation: The Coming Era of Nanotechnology. Los Altos, CA. Eric Drexler, 2000.