**Security Control Framework for Nanoscale Networks (DRAFT)  
Frederick R. Carlson**[fcarlson@brown.edu](mailto:fcarlson@brown.edu)

**Abstract.** Two new networks are coming down the road very, very rapidly: terahertz networking and nanoscale molecular networking. Both are at the nano-scale and have enormous security implications that have not even begun to be addressed. Further, the IEEE has recently released IEEE Standard 1906.1 - Recommended Practice for Nanoscale and Molecular Communication Framework which provides the needed structure to begin looking at creating a security framework. This paper will start the work to bound these networks with a security framework much like the ISO standards (27001) that capture the Information Security centered around electromagnetic processing and networking.

This paper will map the communication technologies that exist at the nanoscale and place them into a bin of 8 control domain groups - Access Control, Asset Management (Privacy), Cryptographic Procedures, Risk Management, Environmental Security, Disaster Recovery, Application Development Security, Governance. This paper will deeply address Access Control and Disaster Recovery and produce a decision matrix as to the best analogous control framework to begin to secure this new network space.  
  
**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

**Introduction.**

There is ongoing and progressive work being done worldwide to create Nanoscale Communication Networks. These networks function very differently (in most cases) than the ones we are familiar with - electromagnetically connected networks. Networks at the Nanoscale can be based on carbon nanotubes, bacterial flagellants, or molecular motors. The release of IEEE Standard 1906.1 – Recommended Practice for Nanoscale and Molecular Communication Framework has created a common lexicon and understanding of what Nanoscale communication is. The publication of this standard creates the opportunity to “work by analogy” to identify one (or more) security control regimes that can bound the immense security implications of this technology. Figure 1 below shows a systems-level view of what a Nanoscale Network is.

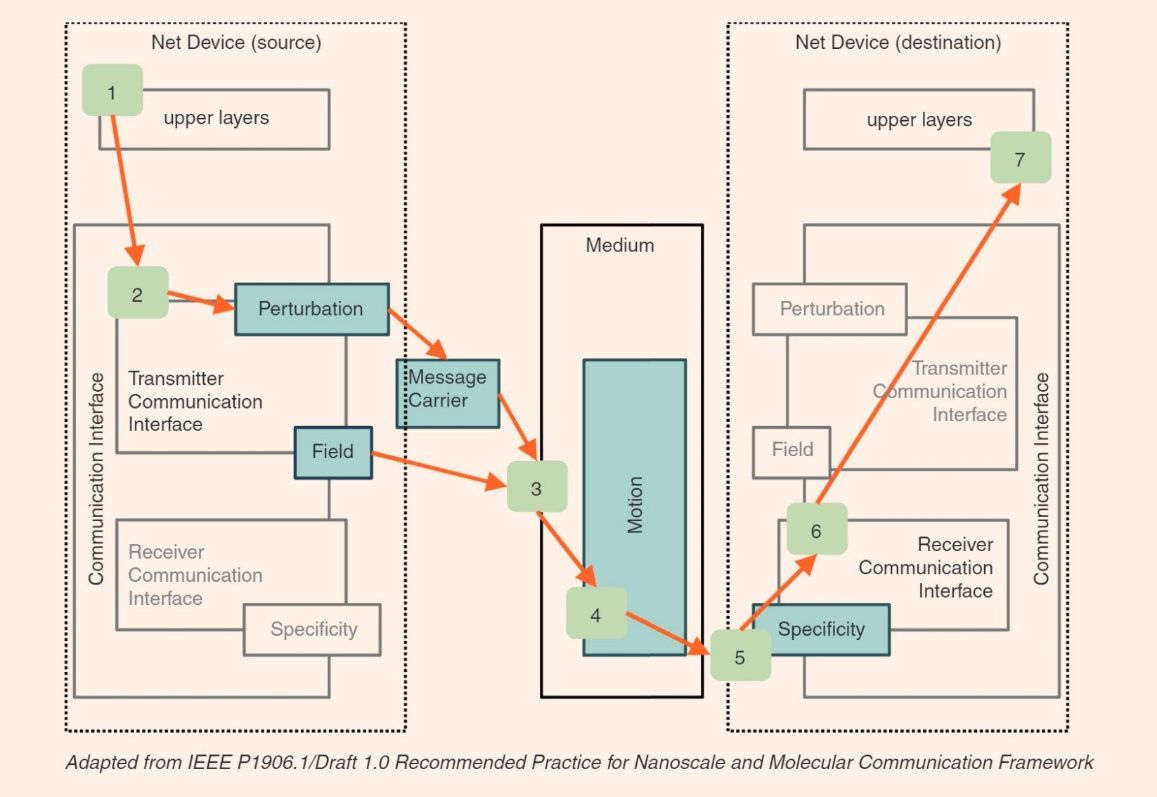


Figure - Nanoscale Network

The IEEE P1906.1 committee provided immense value in categorizing the signal flow from the source to destination in a way that allows for the insertion of incredibly variable technologies. 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 purer biological-based systems such as bacterial flagellants. Figure 2 from the IEEE P1906.1 document provides a good context for the use of these processes.

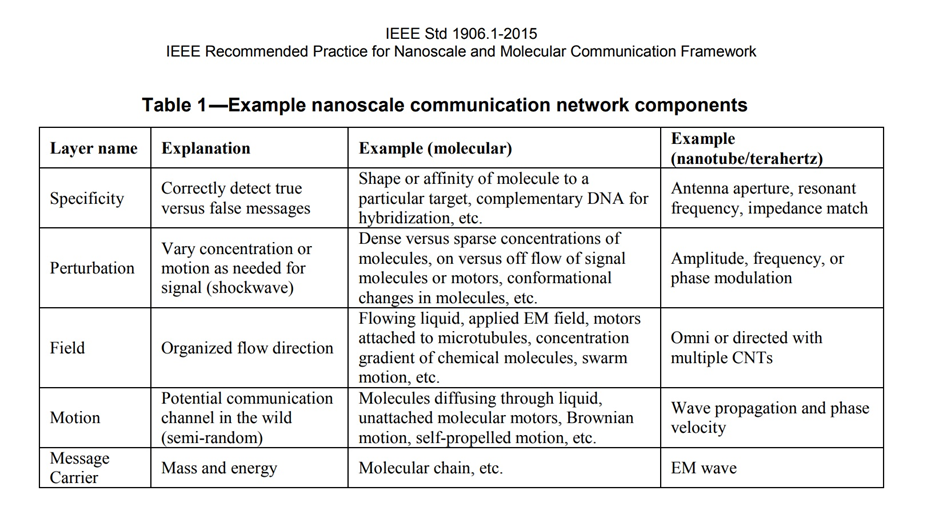


Figure - Nanoscale Network Components

With this important work by the IEEE 1906.1 committee released, it is a feasible task to look at what security control frameworks can be used to manage the security implications of these technologies. This paper will be inductive and use an analogy to pull control systems that manage capabilities of similar import and look to adapt them for use in this problem space. The nature of nanoscale networks is extremely variable, 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 highly likely that more than one framework or a collection of hybrids will be needed even to begin to address this problem.

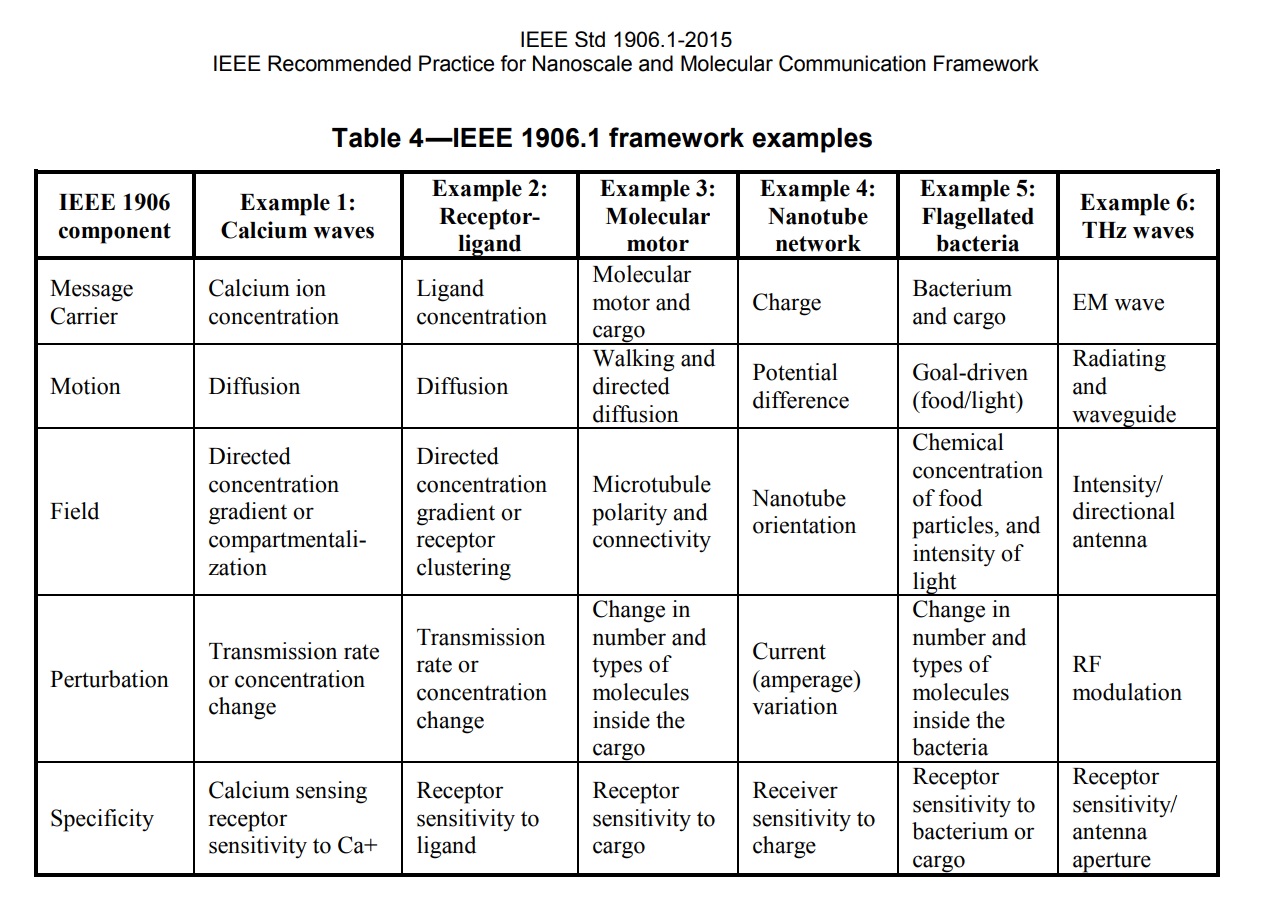
**On Nanoscale Communications**  
There is an incredibly variable range of network mechanisms in Nanoscale and Molecular Communications System. Table 3 below, taken from the IEEE Standard 1906.1 shows this variety. The universe of Nanoscale Systems ranges from diffused calcium waves to ligand receptors to molecular motors, to nanotubes, to flagellated bacteria, and finally to Terahertz networking.   
Figure three also shows the incredible importance of 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 effective classification. Even more impressive is that this framework will allow different types of nanoscale networks to have a framework for interoperability, say between molecular motors and terahertz waves.  
  


Figure - Nanoscale Network Examples

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 - health care informatics, diagnosis, cure, or symptom management. The different nanoscale subsystems have gateways that join to a common network node that 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.

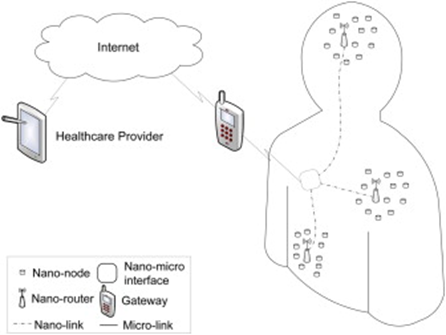
****

Figure - Wireless Use Case

**Nanoscale Standards and Relation to the OSI 7 Layer Model**  
One of the most useful portions of the IEEE 1906.1 Standard is a mapping of the Nanoscale Components to the Open Systems Interconnect Seven Layer Model. This mapping is shown in Figure 5, Mapping of IEEE 1906.1 Standards to the OSI Model.

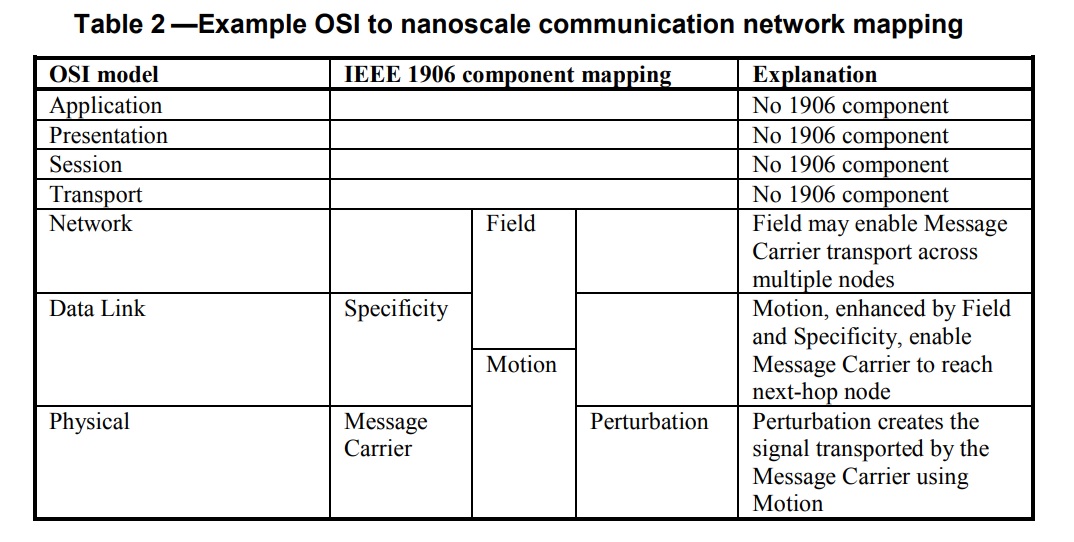


Figure - Mapping of IEEE 1906.1 Standards to the OSI Model

The most important portion of this work is what it does not show. Namely, that there are no nanoscale components that are analogous to the upper layer protocol data units. This reality turns the focus of almost all of the cybersecurity technical control frameworks on their head as they have tended to drift up the OSI stack in recent years. This reality creates a significant classification and segmentation problems and sets the opening moves to secure these systems to the areas of physical security, environmental security, and access control.

The other thing to note is that the “field” component (organized flow direction) is the only obvious choice to attempt to segment and bound these types of networks. This IEEE 1906.1 component is described as something similar to TCP/UDP based filters like stateless firewalls (router access lists). This flow direction component may be the location to use biological cryptography as the gateway between high trust and low trust network segments.

**Security Control Standards and Frameworks**

Figure 6, Security Control Frameworks, breaks down popular control frameworks into two bins. The first is an “Enterprise/Strategic” bin and the second is a binning based on Secure Controls for Industrial Control Systems. This paper will examine the following control frameworks as candidates to create a control framework focused on nanoscale systems – all ISO Standards, HIPAA, NIST SP 800-82 and the Department of Homeland Security Chemical Facility Anti-Terrorism Standards (CFATS)



Figure - Security Control Frameworks

How Nanoscale is Different – What analogies hold?  
  
Editorial Note: My strong suspicion is that the CFATS will need to be looked at very, very hard as the analog we are looking for. This is incredibly powerful technology and of all of the standards I have looked at the CFATS is by far the most aggressive as for as compliance. This, however, creates an issue as this must be an international specification for it to do much good. This is why the ISO standards are also critical, if a bit to high level to be of obvious use.   
  
**Nanoscale Controls – Decision Matrix**  
  
< Insert Decision Matrix Here. > Ed Note – This will be a table based Decision Tools.  
  
**Conclusions and Recommendations**

In this section it must be stressed to “build on success” via analogy. This provides the greatest chance of success to have a new standards committee convened to address this issue.

**Bibliography**

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

Bush, Steven F. "On Information Assurance in Nanoscale Networks." IEEE XPlore.

http://www.albany.edu/iasymposium/proceedings/2008/ASIA08ProceedingsFinal.pdf#page=45.

Dressler, F., and F. Kargl. "Security in Nano Communication: Challenges and Open Research Issues." Security in Nano Communication: Challenges and Open Research Issues. Accessed June 15, 2017. doi:doi: 10.1109/ICC.2012.6364977.

"Molecular Communication: Harnessing Biochemical Materials to Engineer Biomimetic Communication Systems." Molecular Communication: Harnessing Biochemical Materials to Engineer Biomimetic Communication Systems - ScienceDirect. Accessed June 15, 2017. http://www.sciencedirect.com/science/article/pii/S1878778910000074.

"Nano Communication Networks." NanoCommunication Networks - Elsevier. Accessed June 15, 2017. https://www.journals.elsevier.com/nano-communication-networks.

"Nanonetworks: A New Communication Paradigm." Nanonetworks: A New Communication Paradigm - ScienceDirect. Accessed June 15, 2017. http://www.sciencedirect.com/science/article/pii/S1389128608001151.  
  
IEEE Recommended Practice for Nanoscale and Molecular Communication Framework, IEEE Standard 1906.1, 2015  
  
Brotherston, Lee, and Amanda Berlin. *Defensive Security Handbook Best Practices for Securing Infrastructure*. Beijing: O'Reilly Media, Incorporated, 2017.  
  
Drexler, K. Eric. *Engines of Creation: The Coming Era of Nanotechnology*. Los Altos, CA.: Eric Dresler, 2000.

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.