# The Internet of Dangerous Things

Author: Bryan K. Fite, bfite@meshco.com

September 12, 2016

Abstract

"When worlds collide!" is not just another random Seinfeld reference. Rather, it is a wake-up call for all security practitioners and cyber savvy citizens. Cyber was once the exclusive domain of digital denizens but now digital digits can reach out and "touch" someone. As more and more discretion is taken away from human operators and assigned to autonomous & semi-autonomous systems, our safety becomes dependent on ubiquitous sensor networks that are "Connected". New threat catalogs are required to design systems that are safe, secure and private. This paper will introduce a method of articulating the relevant attack surface, move beyond the hype and propose reasonable response strategies for surviving in a world where cyber and physical intersect.

## "When Worlds Collide!"

If innovation is the engine that drives change then technology, imagination and ambition are the fuel that powers *radical* change. The promised benefits represented by technology must be tempered with the understanding that it may also introduce additional, novel or previously mitigated risk. Relevant risks, in turn, are not captured because the new attack surface has not been articulated, acknowledged or otherwise treated. So how do we achieve risk reward equilibrium and perform the required due diligence?

The intersection of multiple domains is the focus of this paper. Specifically, the intersection of the cyber and physical domains. For purposes of this paper, we define *Cyber* and *Physical* the following way:

*Cyber* refers to the discipline associated with the understanding of the relevant security elements in a modern communication network effecting the sender, receiver, message or medium. These systems can ultimately be represented as 0's and 1's at their lowest level. Of course these systems operate in the physical realm but for our purposes it is useful to consider *Cyber* its own domain separate from the inherent constraints of the physical world. *Cyber* operates in the world of ***bits*** and tries to be **secure**.

*Physical* refers to the discipline associated with understanding and manipulating the "tangible" world with the goal of maximizing performance or improving our lives in a **safe** manner. It's the practical application of physics, chemistry and material sciences, normally associated with engineering and machinery. This domain encompasses an incredible number of relevant elements, including environmental tolerances, logistics, temporal elements, mechanical components, power considerations

and operators to name a few. *Physical* operates in the "real world", which is made up of ***atoms*** and is primarily[1] concerned with safety, performance and resiliency.

Therefore, when two domains interact as a system a change of state in the cyber domain can trigger an effector which directs an actuator to change some state in the physical domain. *Simply put, a state change in one domain can cause a state change in another domain when domains interact at touch points.*

## Humans Matter

The Internet is often described as a network of networks. We can apply a similar analogy to Cyber-Physical Systems. Cyber-Physical Systems are systems of systems. In theory, all Cyber-Physical Systems exist to benefit human wellbeing; health, happiness and wealth. Therefore, humans are key to developing practical tools for improving the safety and security of these intersecting domains.

Humans are represented in both the *Cyber* and *Physical* domains in various ways; beneficiary, consumer, operator, threat agent, victim…the list goes on and on. Many times humans will have different roles as they operate in each domain. Of all the elements this paper hopes to address, the human element is the most important and often the hardest to influence and control.

Atoms react in fundamentally predictable ways, discounting Quantum Physics of course. Although a young science, *Cyber* follows a similar well-worn path. Humans on the other hand, can operate in both domains and across stakeholder communities. They are often the "wild card" element and can be a system's biggest asset or biggest liability.

## Safety, Security & Privacy

Confidence comes from a combination of *Trust* and *Control*. Just because an individual Cyber-Physical Systems element is deemed acceptable does not mean when combined with other Cyber-Physical Systems elements it will be safe, secure or private. It's important to remember Cyber-Physical Systems are designed by humans for humans. As such, they are not infallible and should be assessed against the three pillars of confidence; safety, security and privacy.

We associate safety with the physical domain and can see many examples of physical systems being engineered to safety standards or otherwise designed to be safe for human interaction. Similarly for the *Cyber* domain, there is an entire industry devoted to computer and information assurance or what we commonly refer to as Cyber Security. Privacy also must be considered when protecting humans from harm. This is especially true in a world with ubiquitous sensors and data collection services that use meta-data to determine everything from your credit rating to insurability.

[1] *Physical* systems can also be concerned with security. Example: A physical lock and key system whose functional purpose is to provide security.

## How Did We Get Here?

It's useful to understand the dynamics involved in the inevitable fusion of the *Cyber* and *Physical* domains. We should consider the current trends driving the perfect storm we must soon weather. Critical physical systems, in many cases, were designed before the Internet, airplanes or electricity [think sanitation and banking]. Early Supervisory Control and Data Acquisition (SCADA), Power and Communication systems were supported by closed, dedicated and proprietary networks, running protocols that assumed a trusted and controlled environment. Even today, these systems often require enormous capital investment, have massive operational overhead and operate under regulatory constraints and obligations.

Therefore, it should come as no surprise that Innovation and its evil alter ego "cost cutting" have conspired to introduce off the shelf technology, executive dashboards, self-service portals, autonomous systems and a myriad of other elements that dramatically expand the attack surface and introduce interdependencies on untrustworthy system elements. Systems that had always been thought of as "air-gapped" can now, in some cases, be accessed via the Internet or by very inexpensive means. The barriers to entry; propriety knowledge, direct connectivity and cost prohibitive assets no longer exist.

## A Truly Wicked Problem

Unfortunately the trajectory to tragedy is accelerating. There are approximately 7.5 billion humans inhabiting the earth today. Mario Morales of IDC predicts a population of over 25 billion embedded and intelligent systems by 2020. This suggests humans are already outnumbered. The gap will expand by a factor of x3 in less than four years. Equally concerning is the amount of data these Cyber-Physical Systems will generate. Morales predicts 50 Trillion GB of data by 2020 is likely. These numbers are staggering and will grow exponentially of their own volition with the mass adoption of IPv6, low/no energy wireless technologies and advances in embedded systems.

The sheer number of system elements should give pause to any rational observer who considers how impactful (to humans) events like plane crashes, power outages, data breeches or chemical spills can be. The problem is compounded by multiple standards & taxonomies, questionable supply chain practices, stakeholder competition and the pace of change. Many times when Cyber-Physical Systems are designed they are not designed in a way that considers all the permutations of interaction with other Cyber-Physical Systems.

Cyber-Physical Systems will be comprised of elements that are not managed or do not have a clear life-cycle custodian. Even with clearly defined life-cycle custodians, it's not a trivial exercise to keep individual Cyber-Physical Systems elements properly maintained. In the world of *The Internet of Things* (IoT), devices are cheap, small and not necessarily directly connected or manageable.

The complexity of these systems will mean that most human beneficiaries will not have an effective way to determine if Cyber-Physical Systems are fit for purpose. These humans will likely use ***Brand*** as a barometer of trustworthiness. They may or may not have discretion in the selection of Cyber-Physical Systems elements they build dependencies on or otherwise use.

To address these and other evolving Cyber-Physical Systems issues we can expect Cyber-Physical Systems will be implemented in autonomous or semi-autonomous configurations. This carries its own inherent risks. Given our track record of managing the current “modest” population of connected systems with regards to safety, security and privacy, we can expect bad things to happen.

Example:

“How to create a killer robot without even trying.” (Figure 1)

An autonomous vehicle has a brake failure and cannot stop the vehicle or kill the engine. However, it can steer left or right. The dilemma we want to model is a scenario where there are three options. 1) Steer left and hit an elderly pedestrian. 2) Continue forward and hit a child in a stroller 3) Steer right and go over a cliff destroying the car and killing the driver. How will this Cyber-Physical System respond? Vler Scholz and Marius Kempf of mm1 address the moral dilemma in their paper on autonomous driving, which raises the specter of “killer robots” who will use math to resolve this moral dilemma.

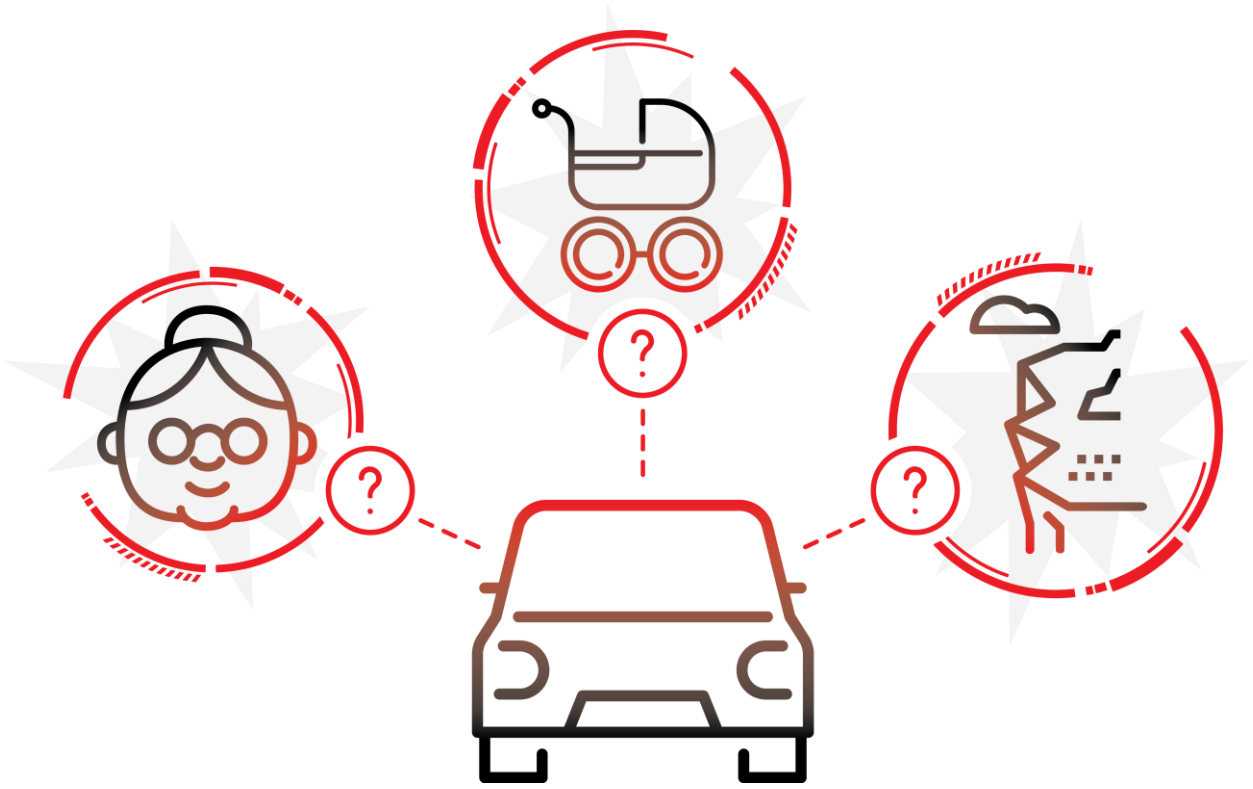



Figure 1

As more machines than people populate the physical domain, expect unforeseen catastrophic failure that will impact humans in negative ways. We also recognize that autonomous Cyber-Physical Systems will benefit humans in many ways. However, the number of connected and projected connected elements necessitate an informed dialog and action with regard to the safety, security and privacy of these Cyber-Physical Systems.

## Reasonable Response

The future is uncertain, so humanity must plan accordingly. I propose a programmatic approach that accepts the inevitability of humans being outnumbered by autonomous and semi-autonomous Cyber-Physical Systems. This methodology also acknowledges the desire to reap the benefits of technology. We should look to achieve risk reward equilibrium with the realization that humans are the ultimate beneficiaries. Therefore, we should not harm one population to benefit another.

Thinking like a species, reasonable might look like this:

- ***Create a cross domain taxonomy*** –This will allow the various stakeholder communities to discuss the risk and reward elements inherent in any Cyber-Physical Systems in an intelligent and consist manner.
- ***Develop a Modeling and Assessment capability*** – By modeling the relevant system elements we can then assess the Cyber-Physical Systems against a myriad of criteria and standards designed to identify the safety, security and privacy issues.
- ***Establish known theoretical attack surface***[2] – It's important to understand as many avenues of Cyber-Physical Systems compromise as possible. This is the main purpose of modeling said Cyber-Physical Systems. I've taken the liberty of expanding the use of the term ***Attack Surface*** to include the potential for Cyber-Physical Systems component failure, malicious agent or unintended system element interaction as they all represent potential paths of harm to human beneficiaries.
- ***Agree relevant threat catalog*** – Just because there is potential for harm does not mean the impact is significant enough to warrant concern or action by a stakeholder. Therefore, a list of the specific "bad outcomes" (threats), which matter to a stakeholder community should be created. This list of "bad outcomes" can then be used to prioritize the treatment of relevant risks.
- ***Articulate control affinities, countermeasures and fail safes*** – Once we have a stakeholder specific threat catalog we can then look for ways to treat risk through the use of controls. Controls can come in many forms; processes, procedures, countermeasure and fail safes. Residual risk to beneficiaries that cannot be treated by controls can be addressed with trust.
- ***Plan for life-cycle management*** – Cyber-Physical Systems often have complicated eco-systems that span stakeholder communities and exist for extended periods of time. Therefore it is imperative, that stakeholders re-assess ***Attack Surfaces***, update ***Threat Catalogs*** and evolve controls periodically or when significant elements change to maintain risk reward equilibrium.

Consider the pharmaceutical industry and the way in which the Food and Drug Administration (FDA) regulates it. New medicines are modeled, clinical trials are conducted and data is analyzed. The benefits of the medicine are compared against the potential side effects. Once approved, the medicine's quality must be measured, managed and attestable. This allows for continuous improvement based on empirical data and accepts that no system is full-proof or without risk.

Generally speaking, the more complex the system the larger the ***Attack Surface***. "Complexity Kills" takes on a whole new meaning in the world of Cyber-Physical Systems. Reducing the complexity of a system should be the first consideration when treating residual risk.

[2] This term could also be referred to as "failure surface".

## Cyber-Physical Systems Primitives

Before we can articulate what reasonable looks like, we must have a common way to communicate across stakeholder communities, regardless of native domain. There are currently several existing and emerging efforts to create frameworks, taxonomies and reference architectures to model and address the challenges of Cyber-Physical Systems. Industrial Internet, NIST and IAmTheCalvary are some groups worth investigating. NIST has an especially useful diagram for visualizing generic Cyber-Physical Systems' elements (Figure 2).

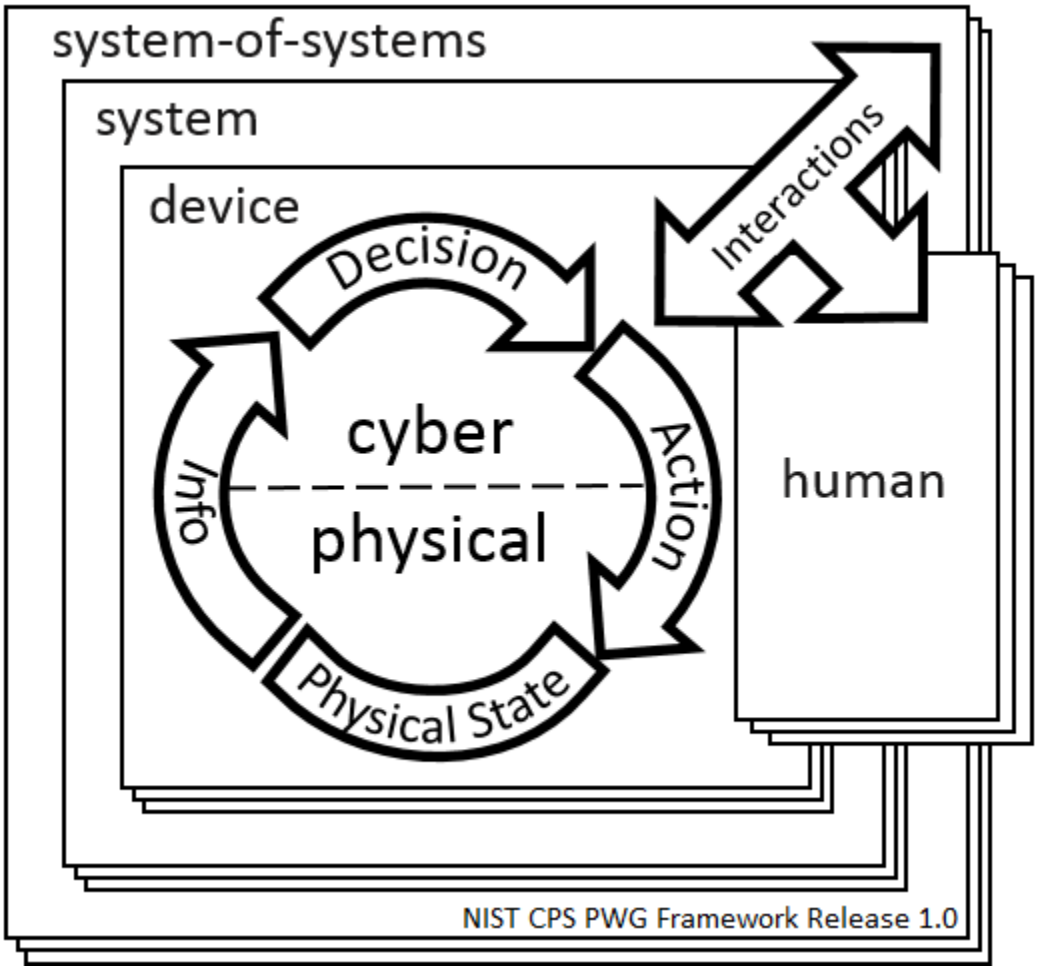



Figure 2

While these groups are accomplishing admirable work, their approaches provide limited practical application in the field. That is why I have developed a way to describe system components and an associated taxonomy that can provide immediate tangible value and is designed to easily map to the myriad of emerging standards. The highest order of Cyber-Physical Systems abstraction is called a Primary Cyber-Physical Systems Primitive. There are 7 Primary Cyber-Physical Systems Primitives in my methodology. They are the highest order of abstraction and can be used to model any Cyber-Physical System element.


The human element of the Cyber-Physical Systems is the primary motivation for this paper. Cyber-Physical Systems exist to support some human need or desire. Humans can be represented as a single individual, a population or role. Humans can be a beneficiary, an operator and/or a threat agent. Beneficiaries are always humans.


A “self-operating” machine or self-contained system element with some ability to change state. What NIST refers to as a ***device***.


How an automaton measures or “perceives” the physical domain. Sensors provide Information to the device or system element.


Method and ability for system elements to exchange information, often about state.


The system element (*Cyber* or *Physical*) that initiates state change in another system element.


The actual physical mechanism that enables the *Effector* to execute an action in the physical domain.


An operator is a type of actor that can control an *Effector* within Cyber-Physical Systems. Operators [3]can be human (benevolent, neutral or malicious), automata or software constructs.

## Modeling and Assessment

I propose a top down modeling approach to describe the relevant system elements using the primitives previously introduced. Primary Cyber-Physical Systems Primitives can be used to describe system elements in the form of objects. Objects, represented by Primary Primitives, have characteristics, which are expressed by Secondary Cyber-Physical Systems Primitives. Objects interact with other objects at touch points and are governed by the rules of the combined domains. Using the abstraction layers provided by primitives, we can support practical modeling and assessment practices, while converting them to objects with characteristics, would allow automation of those exercises at scale.

It is not the intent of this paper to provide an exhaustive or overly prescriptive assessment process. Rather, my objective is to use the Cyber-Physical Systems primitives to model the ***Attack Surface*** of any Cyber-Physical System. Then create the relevant ***Threat Catalog*** and develop tools for effective risk assessment and pragmatic risk treatment.

I will leverage the cyber modeling and assessment methodology as described in my Simulating Cyber Operations paper, utilizing the nine primitives created to represent any relevant cyber element (see appendix B). For purposes of this paper, Cyber-Physical Systems must have at least 1 of each of these primitives to be considered a modeling candidate:

- Single Function Automaton
- Communication
- Effector
- Actuator
- Sensor
- Beneficiary

[3] An external system *Effector* like "nature" should also be considered.

**Note:** All beneficiaries are considered to be human actors.

## Danger Drivers and Confidence Characteristics

One of the goals of any Cyber-Physical Systems should be to achieve risk reward equilibrium. Since we are concerned with harming the beneficiary, it is important to understand the Cyber-Physical Systems elements that expand the ***Attack Surface*** or otherwise increases the possibility of harm. I propose the use of ***Danger Drivers***, which are Secondary Cyber-Physical Systems Primitives that can be used to model those Cyber-Physical Systems characteristics that increase risk. Below is the list of initial Secondary Cyber-Physical Systems Primitives:


Multiple automatons, often grouped together to create a system of systems with multiple functions and capabilities.


The ability of a system element to act as an *Effector* in relationship to other system elements, impacting beneficiaries across multiple domains.


The ability to project (direct & control) force in the physical domain.


The measurement of the degrees of freedom afforded Cyber-Physical Systems, a system element or individual actuator.


The maximum theoretical threshold of a Cyber-Physical Systems capability that can be measured.


The measurement of discretion afforded to system operators.


Often referred to as passwords, they are a common technique to increase confidentiality and integrity of some Cyber-Physical Systems elements.


The ability to control a Cyber-Physical Systems' geospatial position by means of actuators.


Weapons are offensive actuators designed to impact humans in a negative way.

We also want to catalog the Cyber-Physical Systems elements that increase or establish trust and control. I propose the use of Secondary Cyber-Physical Systems Primitives called ***Confidence Characteristics***.


Describes the level of autonomy available to a system, process or operator.


The ability to return to a known state or otherwise persevere state.


Measures the historical performance, statistical baseline, governance effectiveness and overall body of work around the specific Cyber-Physical Systems industry, sector, science and practice.


Controls, that when applied, have a high affinity for mitigating specific threats.


A special type of control that can be employed to increase *Confidence*. They can be deployed in the *Cyber* or *Physical* domain and can be autonomous, semi-autonomous or manual.

The level of clarity and understanding of Cyber-Physical Systems elements and their purpose, including beneficiaries and other stakeholder interests.


The level of subjective probability with which an agent assesses that another agent or group of agents will perform a particular action as prescribed.


This is a process or scheme that allows a high degree of confidence in transactions that does not require trust or shared secrets.


Refers to the level of insight into Cyber-Physical Systems system elements, including capabilities, integrity, state and operational status.


The level of protection afforded human beneficiaries' expectations of freedom from damaging publicity, public scrutiny, secret surveillance, or unauthorized disclosure of one's personal data or information.

By introducing these primitives to our Cyber-Physical Systems modeling and assessment practice we can start to identify a view to residual risk and control gaps. This can be a very subjective exercise and sometimes requires the use of fuzzy logic and rationalization supported by a deep understanding of the organization's ***Confidence Characteristics***, risk appetite, culture, sector norms, regulatory climate, governance maturity, operating model, etc. For our purposes we will assume an organization will have at least a basic understanding of the elements that impact overall *Confidence* in their Cyber-Physical Systems.

The two most practical applications of this approach are the treatment of residual risk and the relative comparison of two or more Cyber-Physical Systems or Cyber-Physical Systems elements. In order to do this, we employ the Rapid Risk Assessment approach to identifying the relevant risk, then treat with a combination of trust and control to develop the level of *Confidence* needed to operate the Cyber-Physical Systems in question.

### Attack Surface, Attack Vectors and Threat Catalog

Now that we have a way to describe the relevant Cyber-Physical Systems elements and model their relation to each other across domains, we can focus on articulating the ***Attack Surface***, identifying ***Attack Vectors*** and building a ***Threat Catalog***.

Depending on the maturity of the stakeholder's practices, this exercise can be as easy as merging risk registers or could require formal assessment. It should be assumed that Cyber-Physical Systems have all of the attack surface of their individual system elements, plus additional attack surface created at the intersections of Cyber-Physical Systems elements. These intersections can be thought of as touch points between automata.

Touch points offer control opportunities but also create new ***Attack Vectors***. ***Attack Vectors*** are all the pathways threat agents can take to affect an asset's state. The more control points that exist between a threat agent and its target, the more theoretical mitigation options available. This is an important consideration when evaluating control affinities, risk treatment and the relative value of automation versus discretion.

Creating the threat catalog requires a view to the assets that are relevant. Generally speaking, assets can be people, data, things or capabilities. The goal of a practical ***Threat Catalog*** is not to define every possible threat but the relevant threats to the assets in question.

## Danger Index

With these tools in hand we can now start to address the ***Danger Drivers*** by building up ***Confidence Characteristics***. The practical objective is to use existing governance and decision support tools for modeling the holistic system of systems in a common and repeatable way.

To that end, we will use field proven risk assessment and treatment tools[4]. I use Rapid Risk Assessment (RRA) and Trust Enhanced Risk Management (TERM) tools in my practice. The Cyber-Physical Systems specific assessment process is used to create a ***Danger Index***. Its purpose is to quickly profile two or more Cyber-Physical Systems and identify relative danger drivers and risk rankings against defined threat catalogs. We can then apply controls, countermeasures and fail safes across domains as appropriate. When we cannot or choose not to mitigate risk we will supplement with documented trust.

[4] It is beyond the scope of this paper to discuss those tools in detail. It is assumed that reader has these or similar capabilities.

To demonstrate this approach[5] I have modeled and assessed three different modes of transportation (planes, trains and automobiles) using seven Secondary Cyber-Physical Systems Primitives as Assessment Elements. My objective will be to determine which system is more or less dangerous (harmful to humans) compared to the other systems. Assessment Element selection criteria is not overly prescriptive but flexible and somewhat subjective based on the objective of the exercise.

The first step is to populate the individual Assessment Elements details for each mode of transportation, remembering that this is a high-level first pass. Any subjective components should be represented by the most appropriate unit of measurement across a normalized "spectrum"; low end, middle range and high end. I have done this below (Tables 1, 2 and 3).

| **Assessment Elements** | **Planes** |
|---|---|
| **Number of Critical System Elements** | 5 -Fuselage, wings, empennage (tail structures), power plant (propulsion system) and the undercarriage |
| **Attack Surface** | Medium |
| **Level of Autonomy** | Medium |
| **Privacy** | Low |
| **Maturity** | 1915, Regulated, Global Standards |
| **Countermeasures** | Many |
| **Fail Safes** | Protocol & Physical Override |

Table 1

| **Assessment Elements** | **Trains** |
|---|---|
| **Number of Critical System Elements** | 8 - OBC (On Board Computer), wheel rail, points & crossings, coupler, cow catcher, bearings, brakes and power plant |
| **Attack Surface** | Large |
| **Level of Autonomy** | Low |
| **Privacy** | Medium |
| **Maturity** | Mid-16th Century (1550), Regulated, Global Standards |
| **Countermeasures** | Some |
| **Fail Safes** | Protocol & Physical Override |

Table 2

[5] It should be noted that a more practical application of this approach would be to compare 2 or more Cyber-Physical Systems of the same class. (e.g. different makes/models of automobiles).

| Assessment Elements | Automobiles |
|---|---|
| **Number of Critical System Elements** | 9 -Cooling, fuel supply, steering, suspension, electrical, transmission, exhaust, gasoline engine and braking system |
| **Attack Surface** | Large |
| **Level of Autonomy** | High |
| **Privacy** | High |
| **Maturity** | 1672, Regulated, Global Standards |
| **Countermeasures** | Few |
| **Fail Safes** | Physical Override |

Table 3

The next step is to bring the individual tables together to form the ***Danger Index***, which will allow us to view the Assessment Elements in a matrix format, making comparison of the various ***Danger Drivers*** and ***Confidence Characteristics*** easier.

# Danger Index

| Assessment Elements[6] | Planes | Trains | Automobiles |
|---|---|---|---|
| **Critical System Elements** | 5 | 8 | 9 |
| **Attack Surface** | M | L | L |
| **Level of Autonomy** | M | L | H |
| **Privacy** | L | M | H |
| **Maturity** | M | M | M |
| **Countermeasures** | M | S | F |
| **Fail Safes** | 2 | 2 | 1 |

Table 4

The ***Danger Index*** highlights key Cyber-Physical Systems element differences between various Cyber-Physical Systems. These differences can be modeled in more detail by adding additional Secondary Cyber-Physical Systems Primitives or by expanding Cyber-Physical Systems element characteristics, enabling better decision support capabilities.

The more Assessment Elements available the more detailed the model that can be created. However, there is a tradeoff between the level of fidelity (model detail) and the time to provide a decision support

[6] This is not an exhaustive list of assessment elements. Any secondary primitives can be used to perform a relative danger assessment of Cyber-Physical Systems elements.

capability (rapid assessment). The more quality data available the better the models we can build but it may take longer to realize the assessment benefits.

Using the example above, one quickly realizes that you cannot simply count the number of Critical Systems Elements to compare and contrast the various modes of transportation. While there are fewer "high-level" Critical Systems Elements associated with a Plane than an Automobile, operating a plane is much more complicated than driving an automobile. However, the complexity of the Plane's sub systems are only articulated at a lower level of detailed. Therefore, Critical System Elements is not a good Assessment Element choice for this exercise.

Further, with respect to determining which mode of transportation is safer relative to another other mode of transportation, we might be asking the wrong question. There is a wealth of actuary data maintained by insurance companies, government agencies and research organizations, which could provide statistically valid answers to that question. Traveling by train is safer than driving in your car but not as safe as air travel.

On the other hand, ***Level of Autonomy***, ***Countermeasures*** and ***Fail Safes*** are a bit more interesting and relevant to a different question. "Could human operators who have discretion or otherwise exercise control could be a ***Fail Safe*** for faulty sensor data, active threat agent action or malfunctioning autonomous systems?" or "Could that same discretion be a ***Danger Driver*** if the human operator can't react to some stimulus (state change) fast enough to execute the needed ***Countermeasure***?".

## A Call to Action

Whether you call it *The Internet of Things*, IT/OT, the Industrial Internet or Cyber-Physical Systems, the potential for catastrophic failure and unmitigatable surprise exists “When Worlds Collide!” and domains intersect. Lack of alignment between stakeholders and overlapping domains conspire to create dangerous systems. New risk models must be developed. It is reasonable to identify and treat the relevant risk.

Whenever these conditions exist, opportunities must be tempered with a conscious understanding of the relevant risk. To do this we must understand the Cyber-Physical Systems’ attack surface and create a stakeholder relevant ***Threat Catalog***. This approach allows for the enumeration of ***Attack Vectors*** and to model how independent Cyber-Physical Systems might interact with each other in ways that could cause harm to humans.

Using transportation systems as an example, we demonstrate a “human friendly” understanding of how to apply critical thinking and “what if” scenario planning for practical application of my approach.

- Planes -Air traffic control systems use a lot of sophisticated tracking, communication and autonomous warning systems to keep travelers safe. However, it is ultimately the "human" operators that make the key decisions. What does the introduction of autonomous and semi-autonomous drones mean to this ecosystem? How much discretion will the "human" operators be afforded?
- Trains –The impact of a train collision or derailment is dependent on many factors but it’s never good. Trains are big and heavy, often times carrying dangerous cargo. Trains operate on tracks that were deployed decades ago and maintained by different entities across thousands of miles. Are the cyber elements maintained in a similar fashion? When autonomous warning systems fail can operators make informed decisions or override system control agents?
- Automobiles -Every day human operators of vehicles must make decisions concerning accelerating, steering and stopping. Would autonomous or semi-autonomous vehicles apply the same logic? How would an autonomous vehicle apply discretion in the face of a "no win decision" - Hit the elderly person crossing the street or kill the driver?

The approach presented will allow practitioners, stakeholders and beneficiaries to quickly determine the level of confidence they should have in a given Cyber-Physical System and determine which Cyber-Physical Systems limit or do not afford any user discretion or control. This provides the basis for a pragmatic and consistent decision support capability, regardless of the Cyber-Physical System in question.

## About the author:

Bryan K. Fite is a committed security practitioner and entrepreneur, Bryan is currently an Account Chief Information Security Officer (CISO) at BT. Having spent over 25 years in mission-critical environments, Bryan is uniquely qualified to advise organizations on what works and what doesn't. Bryan has worked with organizations in every major vertical throughout the world and has established himself as a trusted advisor. "The challenges facing organizations today require a business reasonable approach to managing risk, trust and limited resources while protecting what matters."

Professional Highlights:

Host of the annual "Non-Con" Dayton Security Summit (http://day-con.org )

Founded Meshco™ Producers of PacketWars™ (http://packetwars.com )

Introduced Forensix™ computer forensics collection, analysis and visualization suite

Released AFIRM: Active Forensic Intelligent Response Method to the general public

Founded GETSecure™ a full service security practice; products, professional services, managed services and training.

BFite@Meshco.com

Follow on Twitter @BryanFite

Appendix A: References

worldmeters Online Population meter (Online Service). Current World Population Online Service. Retrieved August 29, 2016 from http://www.worldometers.info/world-population/

Mario Morales, IDC report (NANOCHIP, V8/Issue 2/2013 ). FABS In the Internet of Things Era. Retrieved August 29, 2016 from https://www.eiseverywhere.com/file_uploads/27ceb1798b372d92a7fd66726e007473_Applied-2.pdf

mm1 White Paper, (Stuttgart, July 2015). Autonomous Driving: Cars in a moral dilemma? Retrieved August 29, 2016 from http://mm1.com/fileadmin/content/Whitepaper/mm1_White_Paper_Cars_in__Moral_Dilemma_7_2015_EN.pdf

NIST Cyber-Physical Systems (CPS) Public Working Group (NIST, May 2016). Cyber-Physical Systems PWG Cyber-Physical Systems (CPS) Framework release 1.0. Retrieved August 29, 2016 from https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/Cyber-Physical Systems_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf

Bryan K. Fite (SANS, February 11, 2014). Simulating Cyber Operations. Retrieved August 29, 2016 from https://www.sans.org/reading-room/whitepapers/bestprac/simulating-cyber-operations-cyber-security-training-framework-34510

Dictonary.Com Definition (Online Service). Privacy Definition. Retrieved August 29, 2016 from http://www.dictionary.com/browse/privacy

Enno Rey, presentation (ERNW, March 2010). Rapid Risk Assessment (RRA). Retrieved August 29, 2016 from https://www.troopers.de/media/filer_public/0e/b0/0eb0da2a-ab14-4dc4-b685-156b8348075c/troopers10_rapid_risk_assessment_enno_rey.pdf

Bryan K. Fite (BT, May 14, 2013). Trust Enhanced Risk Management (TERM), Retrieved August 29, 2016 from http://secure360.org/wp-content/uploads/2013/05/Risk-Matters-so-Does-Trust-Bryan-Fite.pdf

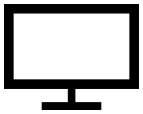
NASA Virtual SKIES (NASA, December 2010). Parts of an Airplane and Their Functions, Retrieved September 12, 2016 from http://virtualskies.arc.nasa.gov/aeronautics/4.html

Ir Jan de Beer Pr Eng (SlideShare, May 14, 2009). Locomotive Safety Critical Systems and Railway Safety Regulator. Retrieved September 12, 2016 from http://www.slideshare.net/sasre/locomotive-safety-critical-systems-and-railway-safety-regulator

Merriam-Webster (Online Service). Automobile Systems. Retrieved September 12, 2016 from http://www.visualdictionaryonline.com/transport-machinery/road-transport/automobile/automobile-systems.php

Alicia Lu, Bustle (May 14, 2015). Are Trains Safer Than Planes? Statistics Are Clear About Which Mode Of Transportation Is Safest. Retrieved on August 29, 2016 from http://www.bustle.com/articles/83287-are-trains-safer-than-planes-statistics-are-clear-about-which-mode-of-transportation-is-safest

The nine *Cyber Operations Simulation Primitives* are:

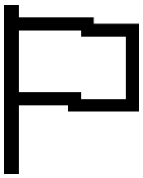
 ***Node***: Any Open System Interconnection (OSI) Layers 1 to 7 (International Organization for Standardization, 1996) connected element

 ***Network***: The communication path or paths between nodes, typically OSI Layers 1 to 3 (International Organization for Standardization, 1996)

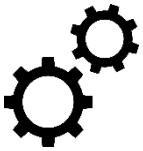
 ***Software***: An operating system, utility, application or service

 ***Artifact***: A file (text, audio, graphic or video) or credentials (account, username, password or key material)

 ***Constraint***: Shapes a simulation by limiting the actor's range of motion and sphere of influence

 ***Objective***: The relative goals of a simulation

 ***Actor***: A human participant in an active simulation

 ***Process***: The workflow associated with a pre-defined simulation element interaction

 ***Message***: Communicates information, data or instructions between simulation elements


BY NC SA