

2022
Annual **INCOSE**
international workshop
HYBRID EVENT
Torrance, CA, USA
Jan 29 - Feb 1, 2022

Premier Systems Engineering Workshop

CIPR Working Group (WG) SysML Model & Functional Analysis of Department of Homeland Security (DHS) National Critical Functions (NCF)

- Tony Adebonojo (Team Lead)
 - CSEP/CISSP
 - January 29th 2022
-



www.incose.org/iw2022/



Agenda



- **Goal of Presentation**
- **DHS Model Team & Project Context**
- **DHS SysML Model Project Goals/Status**
- **References Used**
- **SysML Model of Food and Agriculture Sector**
- **What are National Critical Functions (NCFs)**
- **Definitions of Top Level NCFs**
- **NCF “Examples”**
- **National Critical Functions (NCF) to SSP Data Relationship**
- **NCF Model Development Navigation Page**
- **Connect NCF Decomposition**
- **DHS 16 Critical Infrastructure Sectors Taxonomy**
- **Result of Functional Analysis on Core Network NCF**
- **NCF Functional Analysis to SE “Design” Synthesis**
- **Value of IDT to Engineering Analysis**
- **Sunday Jan 30th CIPR WG Agenda**
- **Future Efforts**
- **Backup Slides**





Goal of Presentation

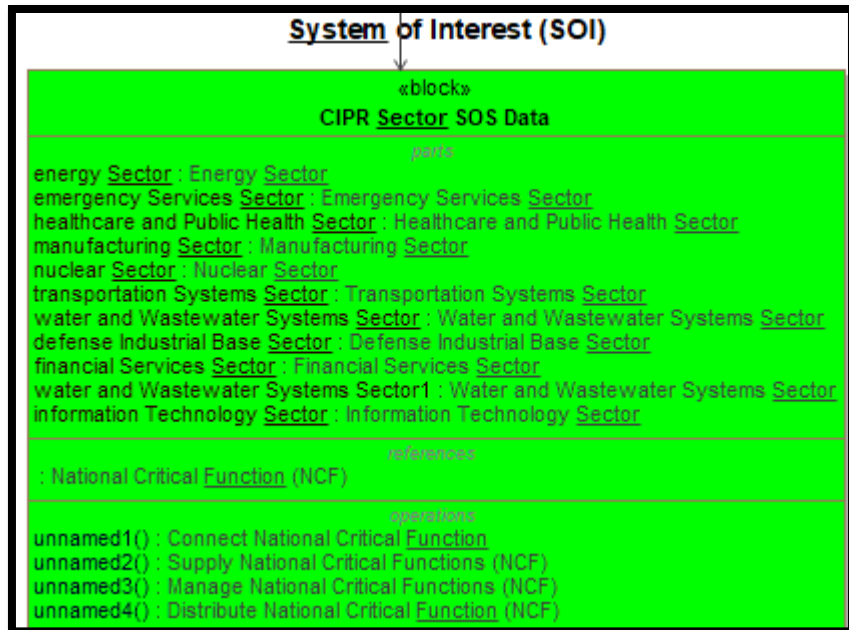
- Show how we have used Cameo Enterprise Architect (CEA) to perform **Functional Analysis** on DHS supplied National Critical Functions (NCFs) as an innovative use of MBSE Tools
- Talk about impact of this work and next steps
- Invite your assistance in this effort

DHS Model Team & Project Context



INCOSE DHS Model Team

Tony Adebonojo (Team Leader)
Dan Eisenberg (WG Chair)
Kirk Moen (Lead SE Multiple Projects)
Ken Heck (Retired Boeing)
John Juhasz (Telepath, Inc)
Howard Lykins (Resilient Hospitals Team Lead)
Dr. Vijay Thukral (Cientive Group)



• DHS 16 Sectors

1. Chemical Sector
2. Commercial facilities Sector
3. Critical manufacturing
4. Dams Sector
5. Defense Industrial base
6. Emergency Services Sector
7. Energy Sector
8. Financial Services Sector
9. Food & Agriculture Sector
10. Government Facilities Sector
11. Health Care & Public Health Sector
12. Information Technology Sector
13. Nuclear Sector
14. Telecommunications Sector
15. Transportation Sector
16. Water and Wastewater Sector





References Used

- [DHS 2015/2016 Sector Specific Plans \(SSPs\) x 16](#)
 - Chemical Sector, Commercial Facilities Sector, Critical Manufacturing
 - Dams Sector, Defense Industrial Base (DIB)
 - Emergency Services Sector, Energy Sector, Financial Services Sector
 - Food & Agriculture Sector, Government Facilities Sector
 - Health Care & Public Health Sector, Information Technology Sector
 - Nuclear Sector, Telecommunications Sector, Transportation Sector, Water and Wastewater Sector
- [National Infrastructure Protection Plan \(NIPP\) 2013](#)
- [Presidential Policy Directive 21 \(PPD-21\) \(2013\)](#)
- [National Critical Functions - Status Update to Critical Infrastructure Community on NCFs July 2020](#)
- [National Critical Functions - Status Update to Critical Infrastructure Community on NCFs Dec 2021](#)
- <https://www.cisa.gov/cisa/infrastructure-data-taxonomy>
 - For Infrastructure Data Taxonomy (IDT)



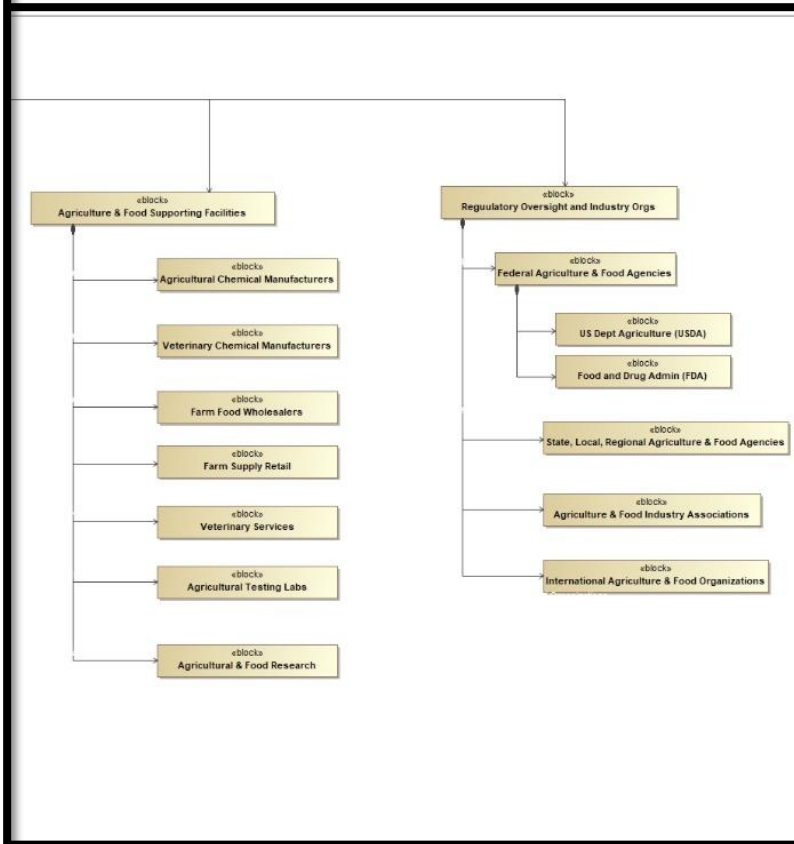
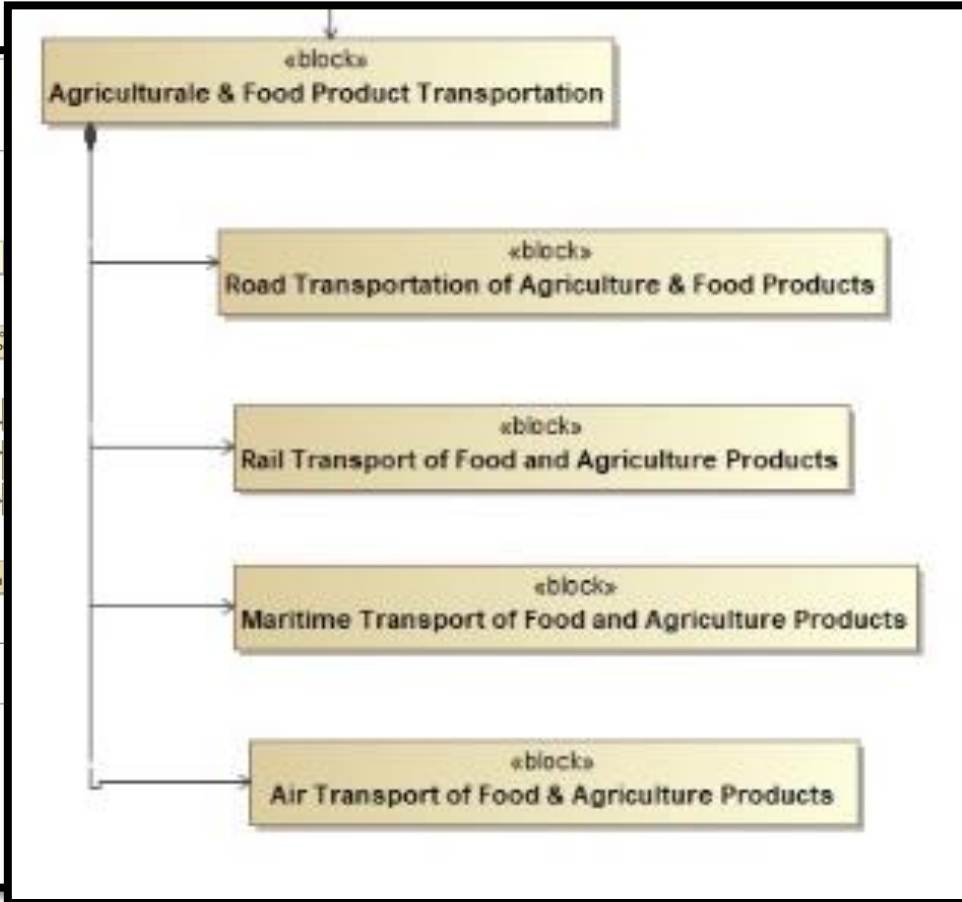
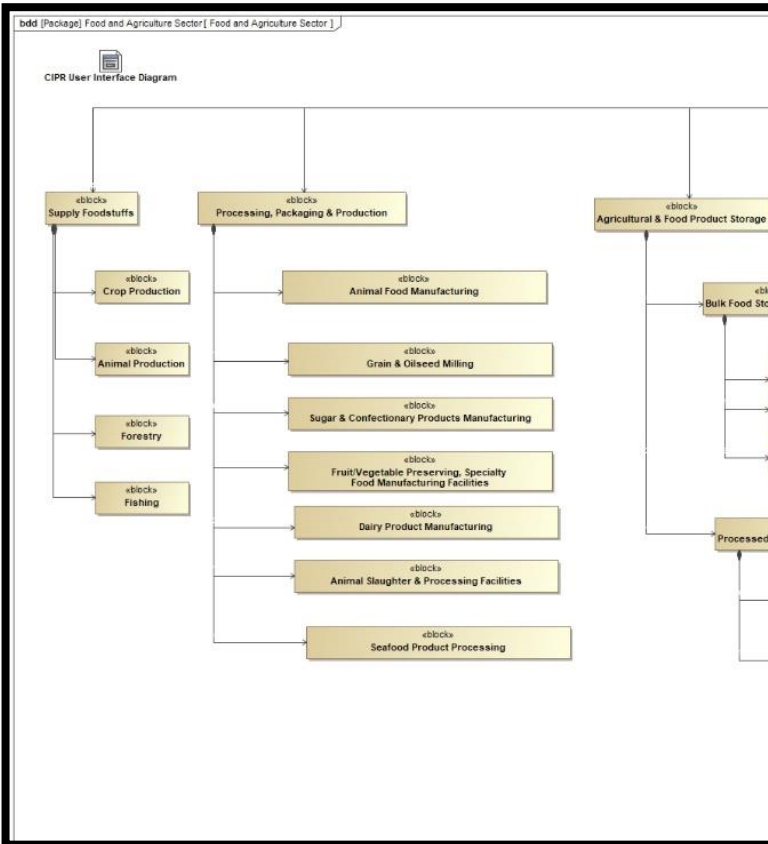
DHS SysML Model Project Goals/Status



- ▶ **Goal 1: Integrated Block Diagram of all 16 sectors (Done)**
 - ▶ Document integrated model down to level in Sector Specific Plans (SSPs)
 - ▶ "Types" allow for further analysis (stadiums as example to facilitate risk identification and interdependencies)
- ▶ **Goal 2: Sector Interdependencies (Mid Year Demo)**
 - ▶ Lifeline functions and "common" interdependencies already documented in SSPs
- ▶ **Goal 3: Sector Risks (Diagram Started)**
 - ▶ Tree diagram of all risks types created in model and linked to each element of 16 sectors that they impact
- ▶ **Goal 4: National Critical Functions (NCF) (Example Decomposed Oct 2021)**
 - ▶ Capture and decompose all NCFs (TBD)
- ▶ **Goal 5: Publish Model Results to HTML website (Demo Available)**
- **NB: Discovery of Infrastructure Data Taxonomy (IDT) led to meetings with DHS (Nov 21)**



SysML Model of Food and Agriculture Sector



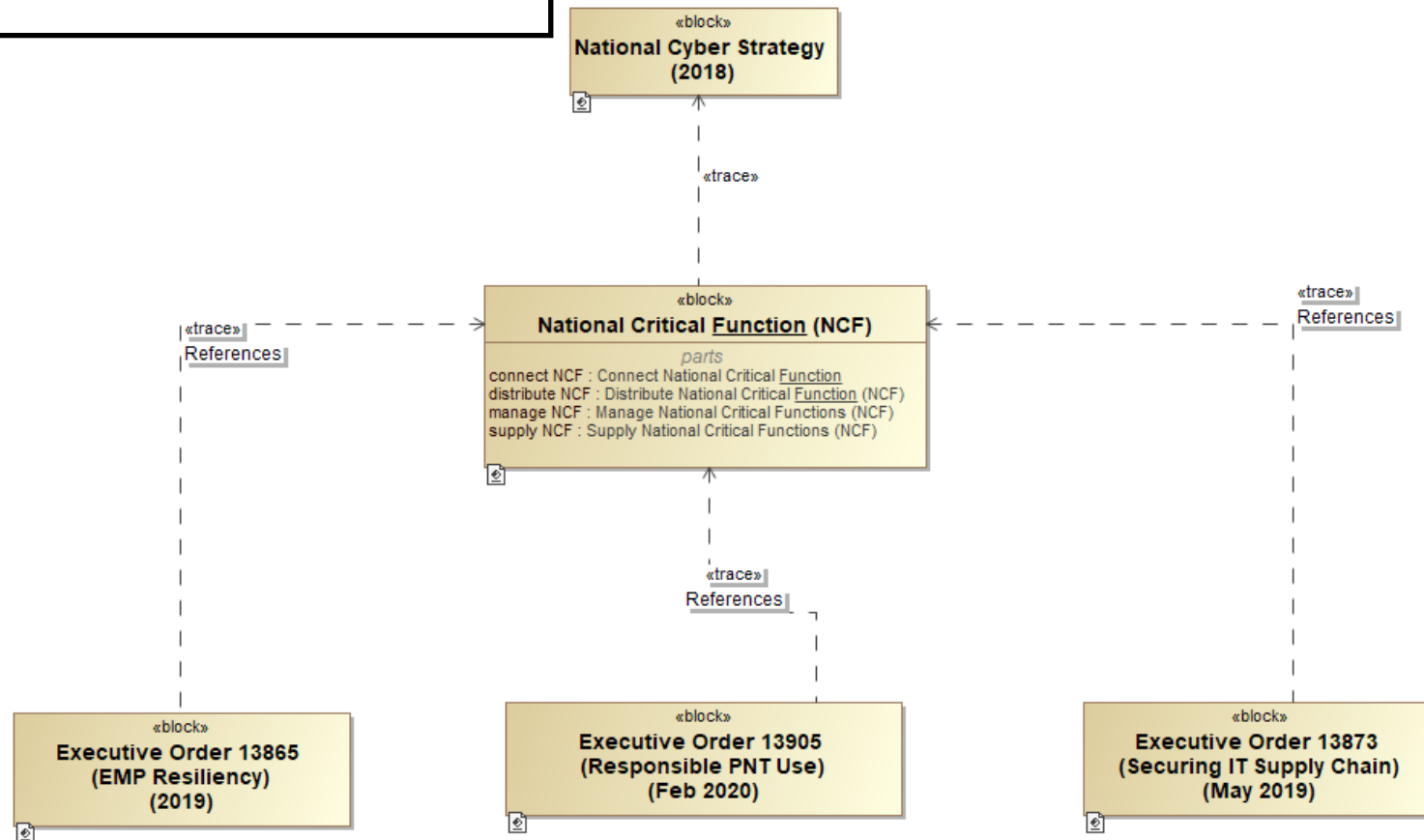
What are National Critical Functions (NCFs)?



National Critical Functions (NCFs) are functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Source: July 2021 Update to CI Community on NCFs

55 NCFs – They are National, Regional, Local And Hybrid in Nature



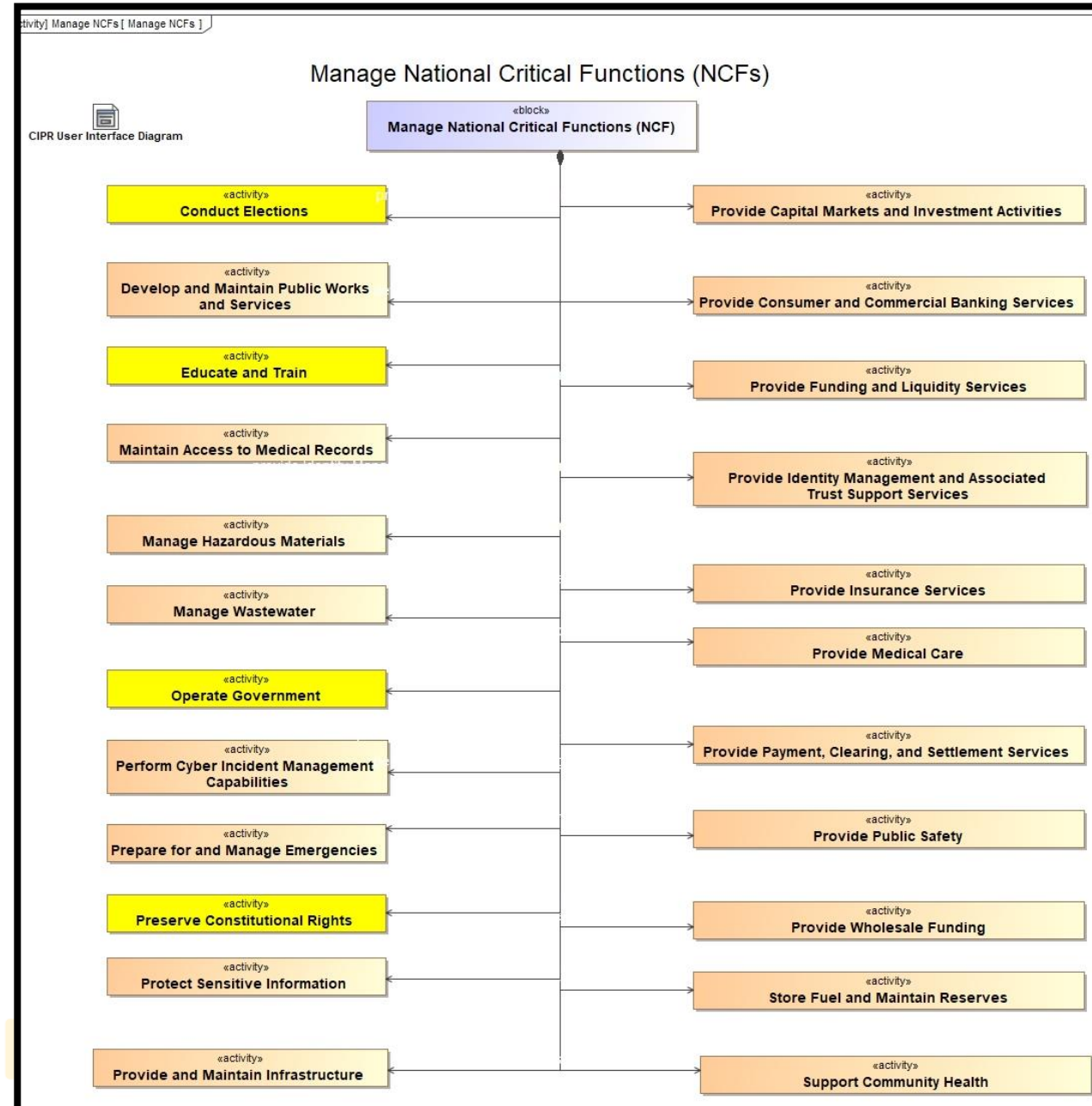
Definition of Top Level NCFs

Connect (9) Connection Technologies that enable critical communications and capabilities to send and receive data (e.g., internet connectivity)

Distribution (9) Distribution Methods that allow the movement of goods, people, and utilities inside and outside the United States (e.g., electricity distribution or cargo transportation)

Management (24) Management Processes that ensure our national security and public health and safety (e.g., management of hazardous material or national emergencies)

Supply (13) Supply of materials, goods and services that secure our economy (e.g., clean water, housing, and research and development)



NCF “Examples”



	Function	Definition	SSP Equivalent
Connect	1 Operate Core Network	Maintain and operate communications backbone infrastructure for voice, video, and data transmission that connects to users through broadcasting, cable, satellite, wireless, and wireline access networks	Telecommunications SSP Commercial Facilities SSP
	2 Provide Cable Access Network Services	Provide access to communications backbone infrastructure through fiber and coaxial cable network, supplying analog and digital video programming services, digital telephone service, and high-speed broadband services	Telecommunications SSP
	3 Provide Internet Based Content, Information, and Communication Services	Produce and provide technologies, services, and infrastructure that deliver key content, information, and communications capabilities via the Internet	Telecommunications SSP Information Technology SSP
Connect	4 Provide Internet Routing, Access, and Connection Services	Provide and operate exchange and routing infrastructure, points of presence, peering points, local access services, and capabilities that enable end users to send and receive information via the Internet	Telecommunications SSP Information Technology SSP
	5 Provide Positioning, Navigation, and Timing Services	Operate and maintain public and private capabilities which enable users to determine location, orientation and time	Telecommunications SSP

NCF Example Decomposition to Follow



NCF - SSP – Infrastructure Data Taxonomy (IDT) Relationships

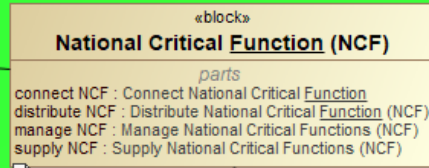


bdd [Package] NCF SSP and IDT Relationship [NCF SSP and IDT Relationship BDD]

National Critical Functions (NCF) to Sector Specific Plan (SSP) Relationship

INCOSE DHS SysML Model Contents

DHS Macro level analysis: 5G, Position, Navigation & Timing, etc



Map NCFs to SSP Data (TBD in Model)

1..*

CIPR Sector SOS Data

```

    «block»
    CIPR Sector SOS Data
    parts
    energy Sector : Energy Sector
    emergency Services Sector : Emergency Services Sector
    healthcare and Public Health Sector : Healthcare and Public Health Sector
    manufacturing Sector : Manufacturing Sector
    nuclear Sector : Nuclear Sector
    transportation Systems Sector : Transportation Systems Sector
    water and Wastewater Systems Sector : Water and Wastewater Systems Sector
    defense Industrial Base Sector : Defense Industrial Base Sector
    financial Services Sector : Financial Services Sector
    water and Wastewater Systems Sector1 : Water and Wastewater Systems Sector
    information Technology Sector : Information Technology Sector
  
```

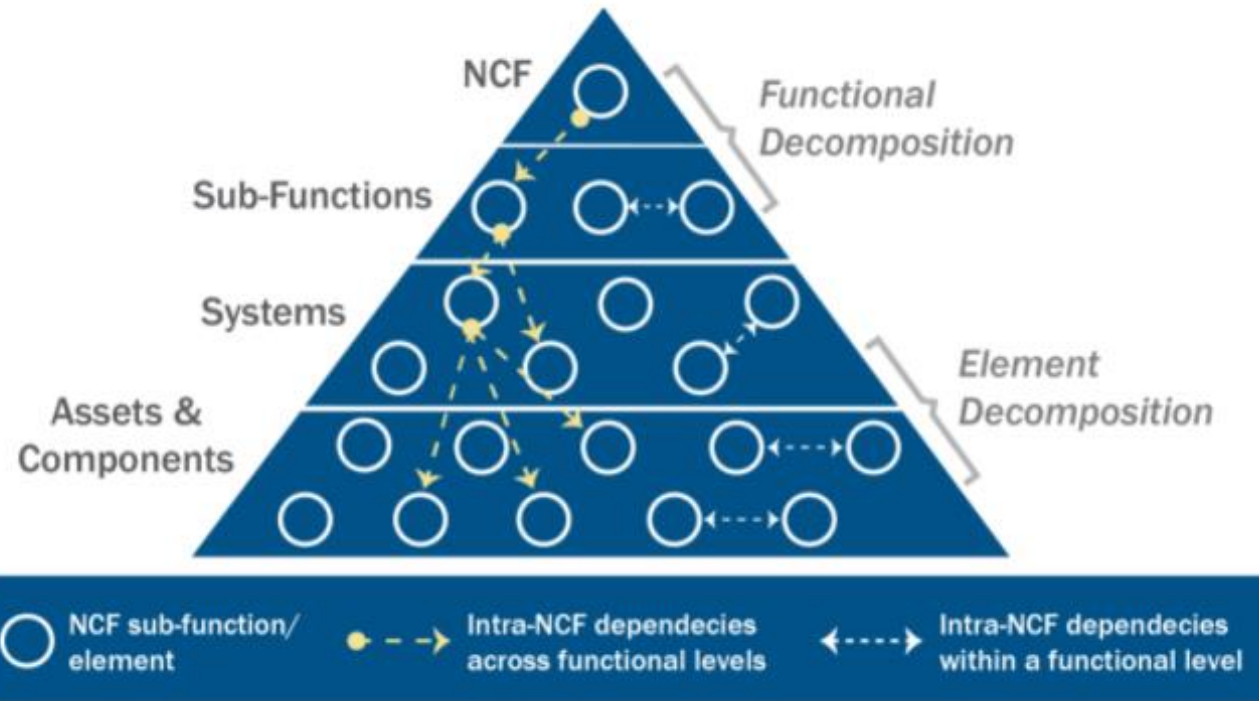
Trade Studies, market analysis, SCADA, ICS Protocols Dependency Relationships, (lifeline functions).

Validate

```

    «block»
    Infrastructure Data Taxonomy (IDT)
  
```

Import to SysML Model




NCF Model Development Navigation Page





package 00 Model User Interface Navigation Dashboard [Connect NCFs]


Diagram name	Connect NCFs
Author	14255
Creation date	10/30/21 9:28 AM
Modification date	10/31/21 4:47 PM
Last modified by	14255
Documentation	<p>This diagram is intended to be used as a presentation dashboard to quickly access different Views of the model's content specific to the presentation intent and scope.</p> <p>It is further intended to help relate System Engineering (SE) understanding and architecture/archetype to those who may not be familiar to SE that it help facilitates what one may wish to considered in one's MBSE Model as related to the SE Architecture of architecture/archetypes.</p> <p>In extreme simple terms, consider the WHAT, WHO, WHEN, HOW and help you determine/decide what model content and views would be necessary as it adds value in addressing your "needs"; conversely, it helps you help you determine/decide what model content and views is NOT necessary as it adds NO value as it does NOT address your "needs".</p>

Functional Architecture



 Connect NCF Orig



 Connect NCF high level



 Connect NCF Ken


 Functional Definitions


Logical Architecture



 National Critical Infrastructure


 Communications Sector



 Communications Sector Revised


Requirements Architecture


 Requirements Hierarchy



 Requirements

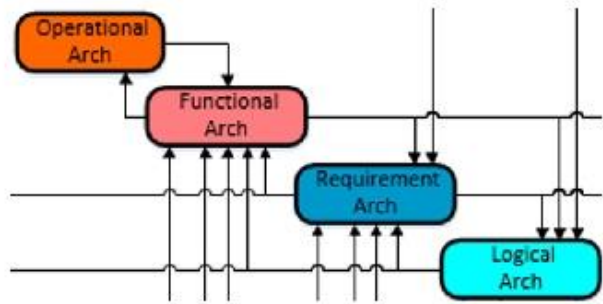
Integration


 Fn and Logical


 Communication Sector Integration

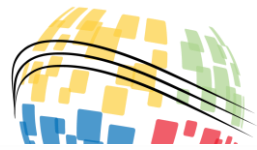
Actors (People, Organization, Departments, Groups, Companies, etc.)


 Communications Actors



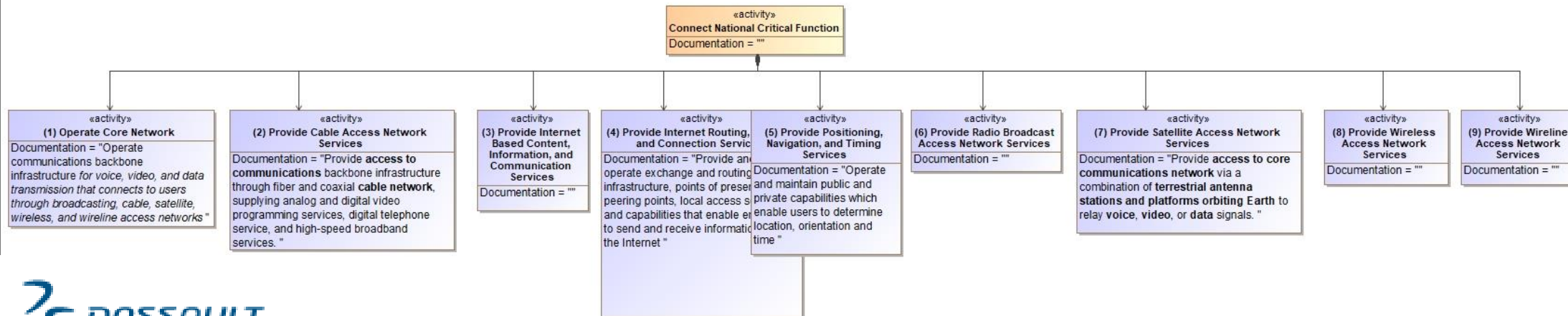
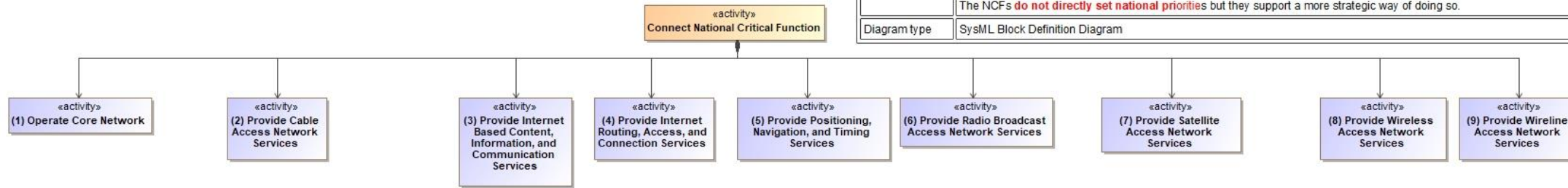


Connect NCF Decomposition



bdd [Package] Original [Connect NCF High Level]

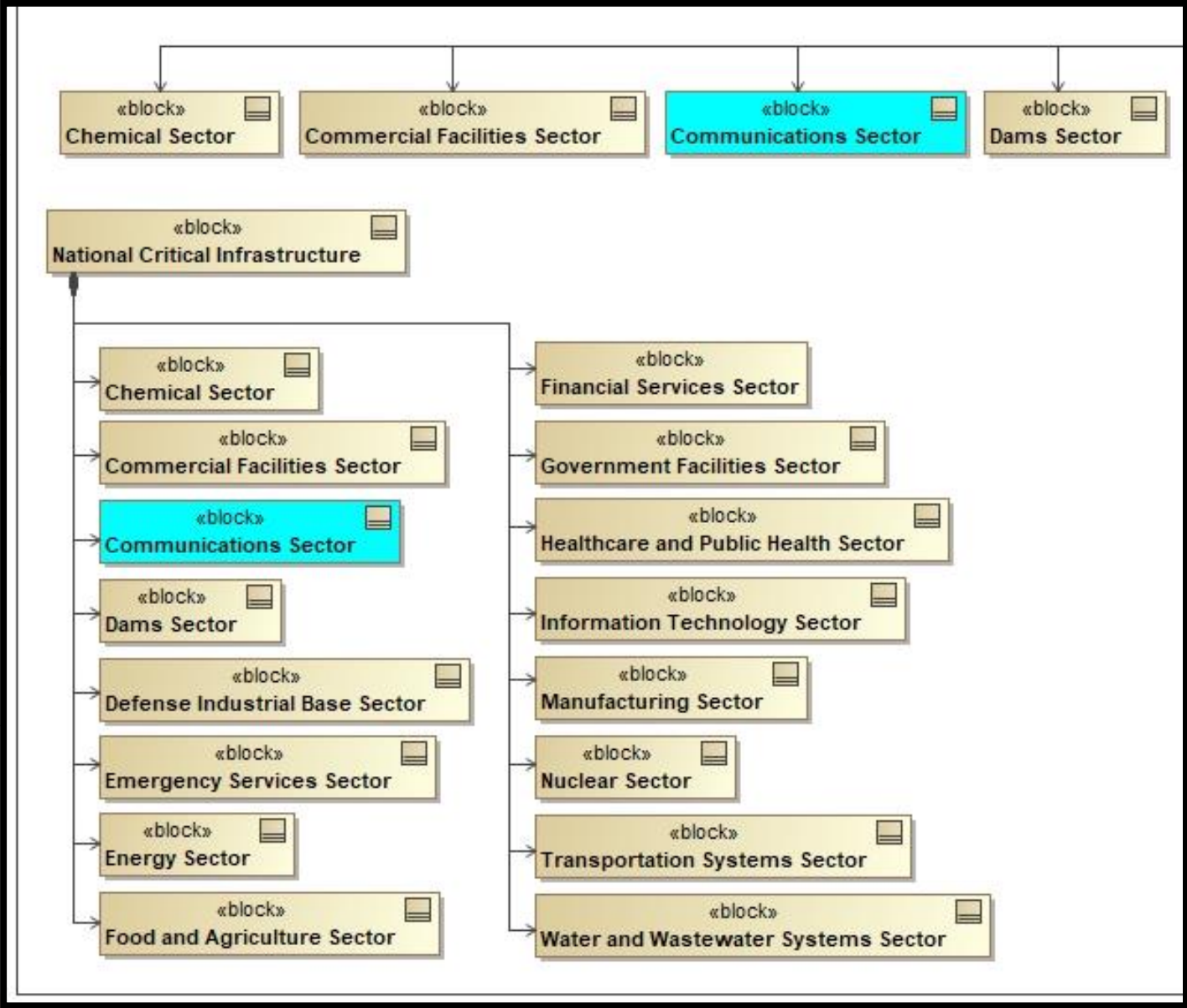
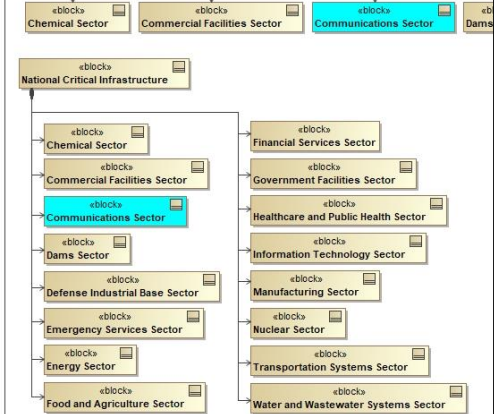
Diagram name	Connect NCF High Level
Author	tadebonojo
Creation date	12/28/21 10:54 PM
Modification date	1/21/22 3:26 PM
Last modified by	tadebonojo
Documentation	<p>The NCFs are a springboard for a wide range of risk management activity including:</p> <ol style="list-style-type: none"> 1. Supporting Infrastructure and Programmatic Prioritization 2. Conducting Detailed Operational and Risk Analysis 3. Informing Intelligence Collection Requirements 4. Supporting Incident Management Prioritization 5. Setting Priorities for Investments in Infrastructure Security and Resilience 6. Supporting National Security Decision Making 7. Enhancing the Efficacy of Continuity Efforts <p>A key component of CISA's strategy will be to use the National Critical Functions to conduct the activities listed above. It will be supported by continued doctrinal and policy evolution as well as close coordination CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY NATIONAL RISK MANAGEMENT CENTER across the interagency and the critical infrastructure community. Ultimately, the set of NCFs is a launching pad for executing a more advanced approach to cybersecurity and critical infrastructure security and resilience.</p> <p>The NCFs do not directly set national priorities but they support a more strategic way of doing so.</p>
Diagram type	SysML Block Definition Diagram



DHS 16 Critical Infrastructure Sectors



Diagram name	National Critical Infrastructure
Author	14255
Creation date	10/28/21 9:57 PM
Modification date	10/31/21 3:29 PM
Last modified by	14255
Documentation	This diagram is intent to represent the Logical (de)composition of the National Critical Infrastructure into its next lower-level child Logical sectors.

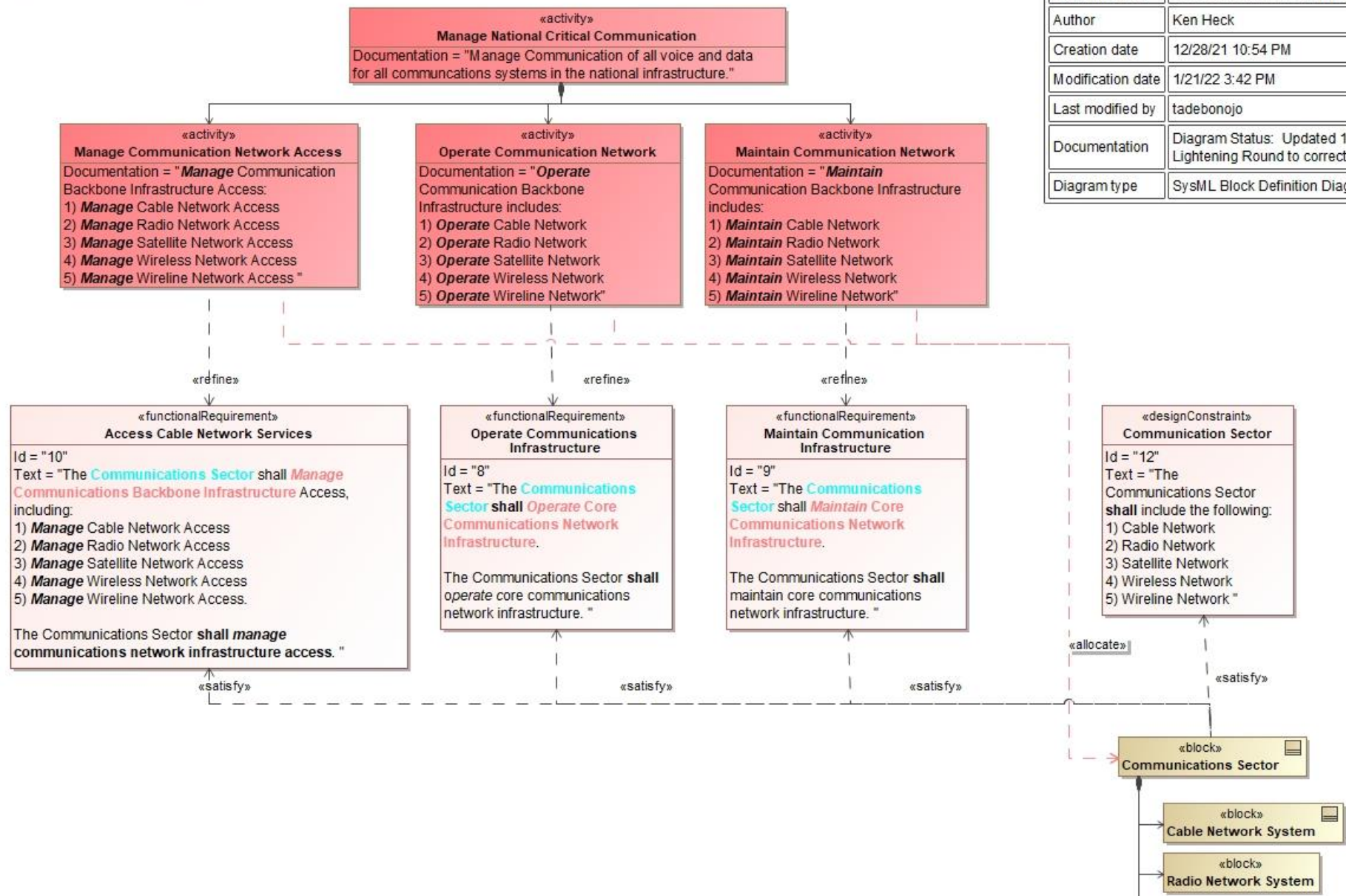


Functional Analysis on Core Network NCF



bdd [Package] 05 Integration View [Communication Sector Integration]

Diagram name	Communication Sector Integration
Author	Ken Heck
Creation date	12/28/21 10:54 PM
Modification date	1/21/22 3:42 PM
Last modified by	tadebonojo
Documentation	Diagram Status: Updated 1/21/22 for IW 2022 Lightning Round to correct stereotype
Diagram type	SysML Block Definition Diagram





NCF Functional Analysis to SE “Design” Synthesis

MBSE Functional Analysis “Product”



«functionalRequirement»
Access Cable Network Services

Id = "3"
Text = "The Communications Sector shall Manage Communications Backbone Infrastructure Access, including:
1) Manage Cable Network Access
2) Manage Radio Network Access
3) Manage Satellite Network Access
4) **Manage Wireless Network Access**
5) Manage Wireline Network Access.

The Communications Sector shall manage communications network infrastructure access. "

SE “Design Synthesis”
“Outputs”



People, Processes and Things or Systems that Provide for **Management of Satellite Network Access:**

- **Satellite Comm Ground Station (GS) (Asset or “System”) – Found in IDT !**
- **Satellite Telecomm Link (GS Component)**
- **Satellite Operations Center (Organization)**
- **Satellite Ground Station Antenna Dish (GS Component)**
- **Ground Station Software (GS “Component”)**
- **Satellite Operators (People)**
- **Standard Operating Proc (SOPs)**

IDT Excel Search



Name	Cell	Value
\$AWS3		Satellite Communication
\$AXS3		Satellite Communication
\$AYS3		Satellite Communication
\$AZS3		Satellite Communication
\$BAS3		Satellite Communication
\$BBS3		Satellite Communication
\$BCS3		Satellite Communication
\$BDS3		Satellite Communication
\$BES3		Satellite Communication
\$BFS3		Satellite Communication
\$BGS3		Satellite Communication
\$BHS3		Satellite Communication
\$BIS3		Satellite Communication
\$BJS3		Satellite Communication
\$BKS3		Satellite Communication
\$BLS3		Satellite Communication
\$BMS3		Satellite Communication
\$AYS4		Satellite Communications Ground Station
\$BFS4		Satellite Control Station
\$BGS4		Satellite Telecommunication Ground Link
\$BHS4		Communication Satellite
\$BIS4		Satellite Telecommunication Service Provider Facility
\$BMS4		Satellite Phone
\$BAS5		Satellite Operations Center
\$CS8		Establishments engaged in operating and maintaining s
\$AGS8		Establishments primarily engaged in operating, maintair
\$AWS8		Establishments primarily engaged in providing point-to-

“SE Design Synthesis” Process Maps NCF to “Assets” level entities in IDT



Sunday Jan 30th CIPR WG Agenda

1000 – 1200: CIPR Invited Speaker Panel New Approaches for Critical Infrastructure System Data and Models		
Time (US Pacific Time Zone)	Topic	Speaker
1000-1030	A Systems Engineering Approach to Understanding Critical Infrastructure Risk	Carmen Zapata, Senior Technical Advisor, US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)
1030-1100	Evaluating Cross-Sector Interdependencies with the All-Hazards Analysis (AHA) Methodology	Ryan Hruska, Chief Scientist, Infrastructure Analysis, Idaho National Laboratory (INL)
1100-1130	Cybersecurity Risk and Data Models for Critical Infrastructure Systems	Bob Hanson, Deputy Associate Program Leader, Defense Infrastructure, Lawrence Livermore National Laboratory (LLNL)
1130-1200	Q&A and Panel Discussion	Moderated, All Attendees

1300 – 1730: CIPR Workshop Model-based Systems Engineering for Critical Infrastructure Systems		
Time (US Pacific Time Zone)	Topic	Speaker
1300-1400	SysML-based Model of a COVID-19 Last Mile Vaccine Delivery System	Steve Sutton, CIPR WG Co-Chair + CIPR WG COVID-19 Modeling Team
1400-1500	Resilient Hospital Reference Model	John Juhasz, CIPR WG Co-Chair + CIPR WG Resilient Hospital Modeling Team
1500-1530	Break	
1530-1630	US DHS Critical Infrastructure Sector Modeling	Anthony Adebonojo, CIPR WG Co-Chair + DHS Modeling Team
1630-1730	Next Steps for the CIPR WG	Moderated, All Attendees

Session Call-In Information

Join Zoom Meeting

<https://incose-org.zoom.us/j/91326068478?pwd=SXpmdGVLV2NkVXdLUmRDakJXdk1qUT09>

Meeting ID: 913 2606 8478

Passcode: 268927

<https://www.incose.org/iw2022/event-schedule/>



Future Efforts

- Model sustainment efforts first part of this year
- Many opportunities/use cases driven by this modeling effort:
 - Engagement with DHS CISA on Infrastructure Data Taxonomy (IDT) update process
 - Glossary Use Case (Ingest and compare after Re Draft NIPP)
 - Engage with other INCOSE WG on CIPR related modeling efforts
 - Ingest IDT into the Model/Engage with CISA in Update of IDT
 - Validate BDDs using IDT
 - Trusted Advisor Services to DHS?
 - Potential opportunities related to Cyber in IDT (Cyber not represented in the IDT)

A logo for 'MBSE Lightning Round' featuring a yellow lightning bolt inside a yellow circle, with the text 'MBSE Lightning Round' in black.



Backup Slides

DHS Water “Supply” NCF Graphic



CYBER RISKS & RESOURCES FOR THE WATER AND WASTEWATER SYSTEMS SECTOR

The Water and Wastewater Systems Sector provides essential services that support the operation of all U.S. critical infrastructure. Water and wastewater facilities rely on information technology (IT) and operational technology (OT) systems to operate, and a compromise of these systems could lead to disruptions of service and significant cascading impacts throughout U.S. critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) developed this infographic to highlight potential cyber risks to the management of wastewater and provide available resources to support proper cybersecurity and resilience.

RISKS TO THE MANAGE WASTEWATER NATIONAL CRITICAL FUNCTION

Information Technology (IT) Systems

1 DATA

Malicious actors may attempt to access IT systems to steal sensitive data, disable network components, and move laterally within the network to access other more sensitive systems.

2 RANSOMWARE

Ransomware attacks can disrupt operations within a facility until systems are restored. While disruptions in office-based systems are most common, it is possible for ransomware to also infect connected Operational Technology (OT) systems, particularly if there is not adequate segmentation between IT and OT systems.

IT/OT Convergence

3 NETWORK SEGMENTATION

Malicious actors may use IT networks as a vector to target non-segmented OT networks and systems. Proper network segmentation is the most effective way to prevent cyber-attacks against OT networks.

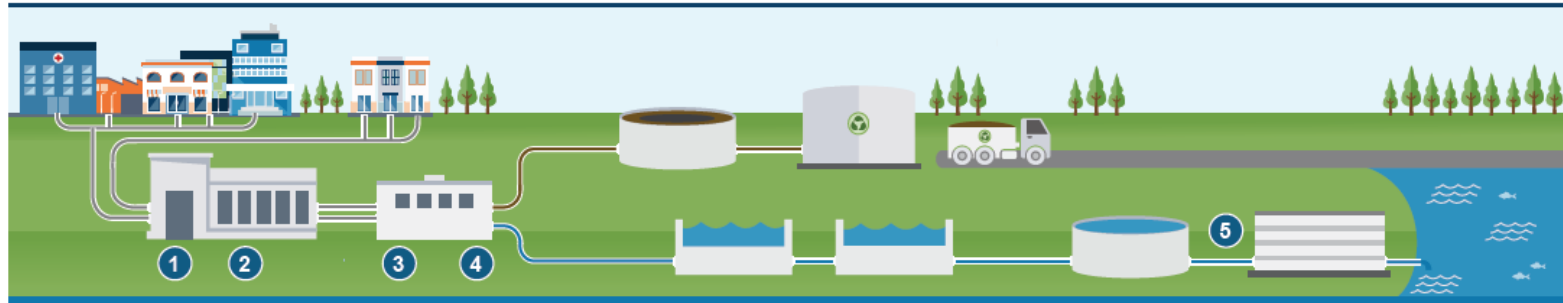
Operational Technology (OT)

4 NETWORK COMPLEXITY

Wastewater management OT networks may contain hundreds of diverse components that can be difficult to properly map and update. This complexity may lead to operators not having full visibility into their networks and may contribute to misconfigurations and continued usage of components that are not included in a utility's network mapping.

5 SYSTEM MAINTENANCE

Improperly maintained custom and Commercial off the Shelf (COTS) components, particularly those that have not been kept up to date on security patches or are operating beyond end-of-life, can leave OT systems vulnerable to attack. Managed Service Providers (MSP) may be used within critical infrastructure to support both IT and OT networks, and if compromised, could provide adversaries with remote access into customers' OT systems. A successful exploitation of an OT system can provide attackers with a direct means of manipulating systems that support the management of wastewater systems.



Data

1



Ransomware

2



Network Segmentation

3



Network Complexity

4



System Maintenance

5

IT SYSTEMS

Implementing cyber hygiene and best practices within IT networks can protect wastewater management systems from cyber attacks such as ransomware and data theft, and reduce the risk of lateral movement within systems or networks.

IT/OT CONVERGENCE

Properly segmenting IT/OT systems, and ensuring that no part of OT systems connect directly to the internet, can greatly reduce the possibility of a successful attack upon ICS/SCADA systems that support the manage wastewater function.

OT SYSTEMS

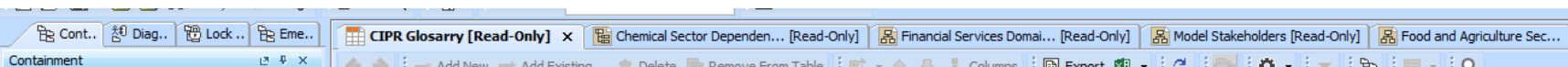
System owners should ensure that OT systems that help wastewater systems control valves and pumps and monitoring are properly protected through patching and proper network mapping. Human machine interfaces, through which operators typically control OT systems, should be a priority for securing.

RESOURCES

AVAILABLE RESOURCES INCLUDE: CISA's [Cyber Resource Hub](#) provides a range of free, immediately available cybersecurity resources. CISA's [Cyber Essentials Toolkit](#) for non-technical leadership. [Securing Networking Devices](#) provides guidance on Segmenting and Segregating Networks. [Stopransomware.gov](#) contains best practices for preventing or responding to ransomware. The [Industrial Control Systems Joint Working Group \(ICS-JWG\)](#) has links to trainings and resources related to the securing and safe operation of ICS systems. CISA also provides no-cost [cybersecurity assessments](#). The [WaterISAC](#) provides wastewater managers with cyber hygiene and water security resources. The [AWWA's Security Guidance and Tool](#) supports the sector in implementing the NIST Cybersecurity Framework and use of Cybersecurity Guidance and Assessment Tool.



Model Glossary – Sourced from NIPP 2013



		Partnering for <u>Critical Infrastructure Security and Resilience</u>)
8	Critical Infrastructure Cross-Sector Council.	Private <u>sector</u> council that comprises the chairs and vice chairs of the SCCs. This council coordinates cross- <u>sector</u> issues, initiatives, and interdependencies to support <u>critical infrastructure</u> security and <u>resilience</u> . (Source: Adapted from the 2009 NIPP)
9	Critical Infrastructure Information (CII).	Information that is not customarily in the public domain and is related to the security of <u>critical infrastructure</u> or protected systems. CII consists of records and information concerning any of the following: <ul style="list-style-type: none"> • Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of <u>critical infrastructure</u> or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law; harms the interstate commerce of the United States; or threatens public health or safety. • The ability of any <u>critical infrastructure</u> or protected <u>system</u> to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the <u>vulnerability</u> of <u>critical infrastructure</u> or a protected <u>system</u>, including security testing, <u>risk</u> evaluation, <u>risk</u> management planning, or <u>risk</u> audit. • Any planned or past operational problem or solution regarding <u>critical infrastructure</u> or protected systems, including repair, <u>recovery</u>, insurance, or continuity, to the extent that it is related to such interference, compromise, or incapacitation. (Source: CII Act of 2002, 6 U.S.C. § 131)
10	Critical Infrastructure Owners and Operators.	Those entities responsible for day-to-day operation and investment of a particular <u>critical infrastructure</u> entity. (Source: Adapted from the 2009 NIPP)
11	Critical Infrastructure Partner.	Those Federal and SLTT governmental entities, public and private <u>sector</u> owners and operators and representative organizations, <u>regional</u> organizations and coalitions, academic and professional entities, and certain not-for-profit and private volunteer organizations that share responsibility for securing and strengthening the <u>resilience</u> of the Nation's <u>critical infrastructure</u> . (Source: Adapted from the 2009 NIPP)

National Cybersecurity and Commu	14	Cyber System.	Any combination of facilities, equipment, personnel, procedures, and communications integrated to provide cyber services; examples include business systems, <u>control systems</u> , and access <u>control systems</u> . (Source: 2009 NIPP)
National Infrastructure Coordinatin			The <u>prevention</u> of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes <u>protection</u> and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and <u>control systems</u> . (Source: 2009 NIPP)
National Operations Center.			The one-directional reliance of an <u>asset</u> , <u>system</u> , <u>network</u> , or collection thereof—within or across sectors—on an input, interaction, or other requirement from other sources in order to <u>function</u> properly. (Source 2009 NIPP)
			The primary, but not exclusive, Federal coordinating structures for building, sustaining, and delivering the <u>response</u> core capabilities. ESFs are vital for responding to Stafford Act incidents but also may be used for other incidents. (Source: National Response Framework, 2013)



Core Network NCF to Telecomm Sector Allocation Matrix



Legend		L1 Communications Sector Revised																								
Allocate		Cable Network System					Radio Network System					Satellite Network System					Wireless Network System					Wireline Network System				
		Cable Network System	TBD Subsystems	Broadcast Component Types	Cable Component Types	TBD Application Types	AM Subsystems	TBD Component Types	FM Subsystems	TBD Component Types	HF Subsystems	TBD Component Types	UHF Subsystems	TBD Component Types	VHF Subsystems	TBD Component Types	Satellite Network System	Satellite Subsystems	Satellite Types	TBD Component Types	Wireless Network System	TBD Subsystems	TBD Component Types	Wireline Network System	TBD Subsystems	TBD Component Types
Revised		7	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	
Manage National Critical Communication(context Communications Sector)	1	Allocate																								
Maintain Communication Network(context Communications Sector)	1	Allocate																								
Maintain Cable Network(context Communications Sector)	5	Allocate	Allocate	Allocate	Allocate	Allocate																				
Maintain Radio Network(context Communications Sector)	11						Allocate	Allocate	Allocate	Allocate	Allocate	Allocate	Allocate	Allocate	Allocate	Allocate										
Maintain Satellite Network(context Communications Sector)	4															Allocate	Allocate	Allocate	Allocate							
Maintain Wireless Network(context Communications Sector)	3																			Allocate	Allocate	Allocate				
Maintain Wireline Network(context Communications Sector)	3																						Allocate	Allocate	Allocate	
Manage Communication Network Access(context Communications Sector)	1	Allocate																								
Manage Cable Network Access(context Communications Sector)	5	Allocate	Allocate	Allocate	Allocate	Allocate																				
Manage Radio Network Access(context Communications Sector)	11						Allocate	Allocate	Allocate	Allocate	Allocate	Allocate	Allocate	Allocate	Allocate	Allocate										
Manage Satellite Network Access(context Communications Sector)	4															Allocate	Allocate	Allocate	Allocate							
Manage Wireless Network Access(context Communications Sector)	3																			Allocate	Allocate	Allocate				
Manage Wireline Network Access(context Communications Sector)	3																						Allocate	Allocate	Allocate	
Operate Communication Network(context Communications Sector)	1	Allocate																								
Operate Cable Network(context Communications Sector)	5	Allocate	Allocate	Allocate	Allocate	Allocate																				
Operate Radio Network(context Communications Sector)	11						Allocate	Allocate	Allocate	Allocate	Allocate	Allocate	Allocate	Allocate	Allocate	Allocate										
Operate Satellite Network(context Communications Sector)	4															Allocate	Allocate	Allocate	Allocate							
Operate Wireless Network(context Communications Sector)	3																			Allocate	Allocate	Allocate				
Operate Wireline Network(context Communications Sector)	3																						Allocate	Allocate	Allocate	