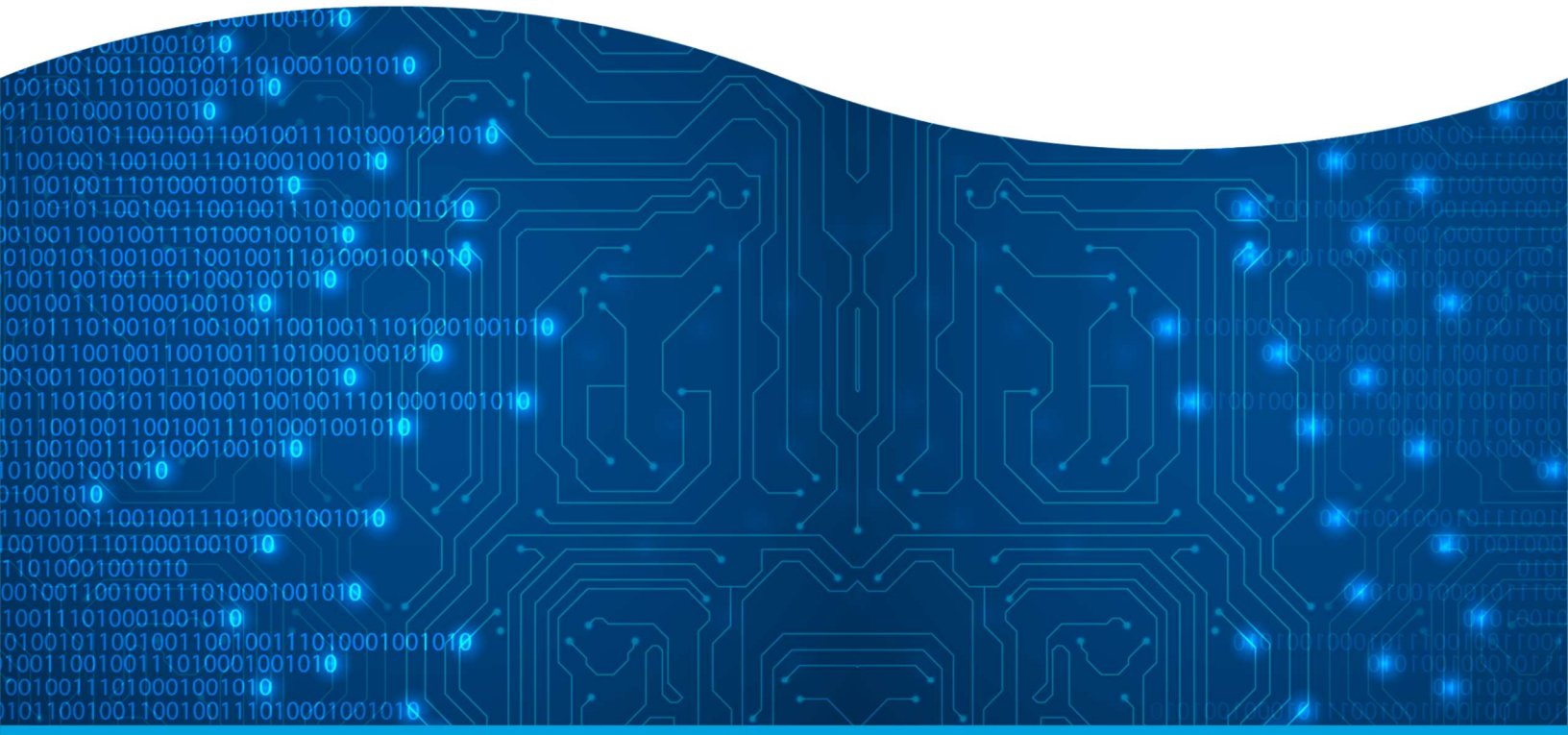
Consequence-driven
Cyber-informed
Engineering

Function-based Taxonomy Implementation



U.S. DEPARTMENT OF ENERGY
CYBERCORE integration center
Idaho National Laboratory INL

Function-based Taxonomy Implementation

Consequence-driven Cyber-informed Engineering

Jeffrey R. Gellner
Control Systems Engineer

David G. Kuipers
Control Systems Engineer

Nathan H. Johnson
Control Systems Cybersecurity Analyst

William W. Siwiec
Control Systems Engineer

Idaho National Laboratory
Cybercore Integration Center
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of National & Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Contents

Copyright

Purpose

Function-based taxonomies are relational mapping tools used to clearly illustrate how an organization delivers Critical Functions by using various people, processes, technologies, information, and infrastructure (PPTII). Critical Functions are the actions or activities that make up an organization's primary purpose. Enabling Functions are the combination of PPTII used by that organization to deliver their Critical Functions.

Taxonomies provide quick, visual depictions of these functions and their numerous relationships more efficiently than a written or verbal description. As available information increases, the taxonomy further enhances an organization's capabilities for identification and enumeration of relationships between their Critical Function delivery, the PPTII involved, and contextual understanding of any key artifacts related to the design and implementation.

A function-based taxonomy further provides a framework to categorize information and the related artifacts that document the organization's unique implementation of PPTII for function delivery. The ideal state of a function-based taxonomy is to organize the existing knowledge an organization has for their numerous systems, policies, people, procedures, configurations, and other factors. A well-organized taxonomy helps organizations effectively leverage their knowledge to clearly identify dependencies and connections that exist within their Critical Function delivery.

> ***Data Protection Warning**: The information contained within a functional taxonomy could likely provide an adversary with a highly-concentrated, valuable set of data. To avoid helping an adversary conduct sabotage efforts against Critical Functions, these taxonomies (and their associated artifacts) must be protected by restricting access and taking other security measures.*

Focus First

From a use-case perspective, a very high-level function-based taxonomy can be used to support an initial function analysis for an organization. However, if a more accurate depiction of the organization's function delivery is needed, this is best developed after a narrowed focus is determined.[1]

Prior to mapping out a function-based taxonomy, some boundary conditions[2] are used to narrow the areas of focus and ensure the taxonomy does not become filled with unrelated or non-essential details. After specific functions and portions of the organization are identified, details learned during interviews, and information gleaned from documents, can clearly inform how a function is performed.

[1] In general, a function-based taxonomy helps illustrate how a specific function is delivered. For CCE engagements, this process best occurs during Phase 2 (System of Systems Analysis) and is further refined during Phase 3 (Consequence Prioritization).

[2] For general application, boundary conditions are simple statements used to identify a specific function of interest and include or exclude any portions of an organization (such exclusions are usually made for logistical reasons). When used in a CCE setting, boundary conditions are developed during Phase 1 to clearly spell out the objective an adversary wishes to accomplish against an organization, with organization-specific thresholds. Boundary conditions also detail the scope of the engagement by listing identified areas of focus as well as any physical or logical restrictions placed on the CCE engagement.

Mapping Software

Specialized visualization applications like MindManager[3] are effective tools that help capture hierarchical organization and relationship mappings between objects. If such specialized applications are not available, taxonomy mapping can be accomplished using a spreadsheet program, such as Microsoft Excel. Using these tools, parts of the taxonomy can link to documents or files, allowing users to quickly track artifacts and see how they tie to different elements within the taxonomy. This improves data organization, referencing, and retrieval. Importantly, the key is not the software used, but the application of consistent and repeatable naming conventions, tagging systems, and regular updates to ensure the function-based taxonomy remains accurate and relevant.

Approach

A targeted and repeatable approach for creating function-based taxonomies is presented below. These methods are the result of experience gained during previous taxonomy mapping efforts by several individuals. A function-based taxonomy always begins by identifying the root element and then branches logically in both directions.

Organization Box and Function-based Split

Function-based taxonomies place an organization's name at the root level of the structure to create an "Organization Box" (see Figure 1). Each element added to the mapping structure from this point will indicate a Critical Function (on the right-hand side) or an Enabling Function (on the left-hand side) for this organization. The organization named in the center of the function-based taxonomy could represent an overarching company (e.g., X Power Company), or the taxonomy can be tailored to a specific sub-organization within that larger company (e.g., the Infrastructure Department for X Power Transmission).

> ***Critical Functions*** *are the actions or activities that make up an organization's mission or primary purpose. Located on the right-hand side of a functional taxonomy.*
>
> ***Enabling Functions*** *describe the people, processes, technologies, information, and infrastructure an organization uses to both logically and physically deliver their Critical Functions. Located on the left-hand side of a functional taxonomy.*

The function-based taxonomy is immediately divided into two halves. Taxonomy elements on the right-hand side show the different branches of Critical Functions performed by the organization and describe actions or activities that make up that organization's primary mission or purpose. Importantly, these Critical Functions do not refer to specific groups, people, devices, or technologies. As an example, one Critical Function for many power utilities is "power transmission." Another example may be "power distribution." For manufacturing companies, one Critical Function would typically include "product creation."

[3] Visit https://www.mindmanager.com/en/product/mindmanager/ to learn more about MindManager's mind mapping software.

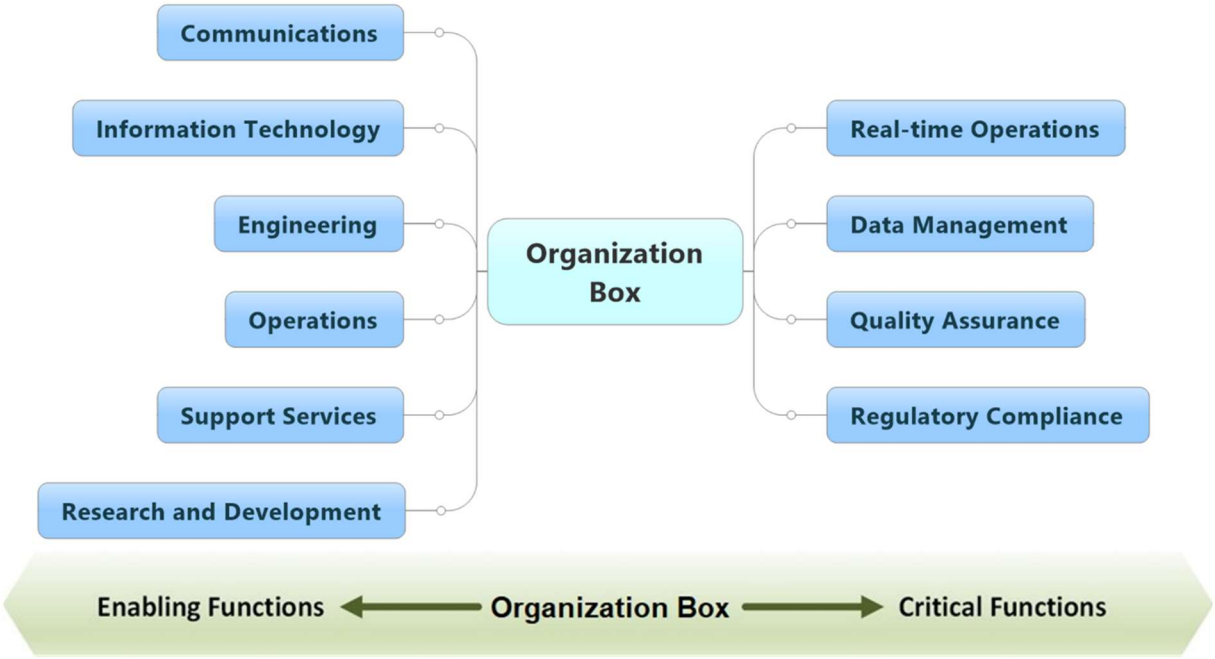


Figure 1: Basic taxonomy structure, with examples of Critical Functions and Enabling Functions

Elements on the left-hand side branch out to depict Enabling Functions. Enabling Functions describe all of the PPTII the organization implements to physically and logically deliver their Critical Functions. Some examples of Enabling Functions for power utilities that deliver electricity may include the physical power lines, step-up transformers, connected protection devices, and existing communications infrastructure. These Enabling Functions work together to ensure that the Critical Function of "power delivery" is accomplished. For manufacturing companies, the processes used in assembly lines, engineering designs, production employees, source materials, production tools, and even the electricity powering the facility are examples of Enabling Functions used to deliver their Critical Function of "product creation."

> ***Functional Grouping Conventions****: The approach presented in this paper supplies a universally applicable method for breaking down an organization. Organizational titles for labor, efforts, and activities will vary significantly across multiple sectors. As elements are added to the structure, they should clearly represent and document an organization's specific structure.*
>
> ***Adaptation:*** *For some sectors, these general taxonomy development principles may need to be arranged under different functional groupings, and in some cases organization-specific or sector-specific naming conventions will be more appropriate.*
>
> ***Terminology****: Some terminology used in this document is selected to convey specific functionality or to describe an object specifically related to functional taxonomy development. Some word choices may not universally apply for all practitioners (e.g., engineers, technicians, operators). During the creation of a sector-specific functional taxonomy, appropriate sector-specific terms should be used to avoid confusion.*

Critical Functions Mapping

Levels in Critical Function Structure - Overview

The right-hand side of a function-based taxonomy is comprised of hierarchically arranged Critical Function branches (see Figure 2). To map these, each Critical Function begins on the right side of the Organization Box and expands as Process Area Functions and critical subfunctions are identified. Keeping the root Organization Box at the center, we will numerically label the Critical Function levels of hierarchy, which become increasingly detailed and specific within a function. The position of the Organization Box is always considered the root level.

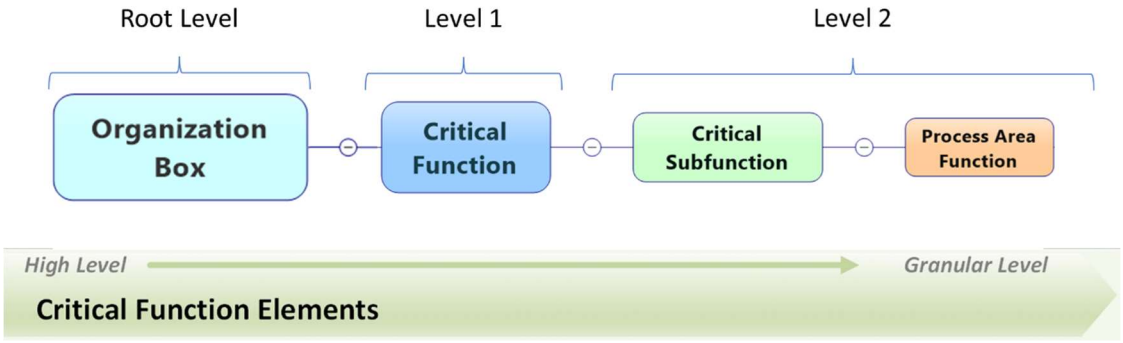


Figure 2: Hierarchy of Critical Function Elements

Level 1 elements are positioned immediately right of the Organization Box. These Level 1 elements represent the organization's primary and distinct functions and should all be Critical Functions. These refer to high-level actions or activities the organization performs. Although Level 1 Critical Functions may be unique to each organization, they should be similar among organizations within a given subsector. For example, local electric utilities would all likely share similar Critical Functions at Level 1.

> ***Level 1 Elements for Critical Functions*** *refer to high-level actions or activities the organization performs and should all directly relate to an organization's mission or primary purpose.*

Level 2 elements describe more detailed actions and activities as the hierarchy is enumerated. They are positioned further from the Organization Box and include the following mid-level elements: "Critical Subfunctions" and "Process Area Functions." These elements provide gradual transition from high-level business functions to specific operational functions, all tied back to the Critical Function they support at Level 1. There is no set number of elements to identify.

> ***Level 2 Elements for Critical Functions****:*
>
> ***Critical Subfunctions*** *describe the major actions that must take place within a primary Critical Function.*
>
> ***Process Area Functions*** *identify the key areas where the actions for each Critical Subfunction take place.*

If desired, Critical Functions can be broken down further into very granular elements using this relational hierarchy. Eventually, each branch can terminate with a very specific action or activity that cannot be

reduced any further. According to the taxonomy framework, these would be considered final, Level 3 elements. However, in most applications, function-based taxonomies do not need to be extended further than the Process Area Functions in Level 2.

The level of detail required will be determined by identifying what matters to the organization (e.g., What functions are we trying to learn about? What functions are we trying to protect?).

> ***Helpful Tip:*** *Always use an action phrase to describe each element on the right-hand side of the taxonomy. This ensures a function-based focus and avoids accidentally including PPTII elements.*

Relationships Between Functions

Relationships may be indicated on a function-based taxonomy to tie two elements together to identify interdependencies or interactions between elements that reside on separate branches of the mapping. Lines used to demonstrate such relationships should be different from the standard branching lines and include a label to provide clarity.

Enabling Functions Mapping

Levels in Enabling Function Structure - Overview

Enabling Functions describe the deployment of an organization's PPTII. This collection of people, processes, technologies, information, and infrastructure work together to deliver Critical Functions. These elements clearly show how the organization conducts various Critical Subfunctions and Process Area Functions. The Enabling Function mapping occurs on the left-hand side of the Organization element.

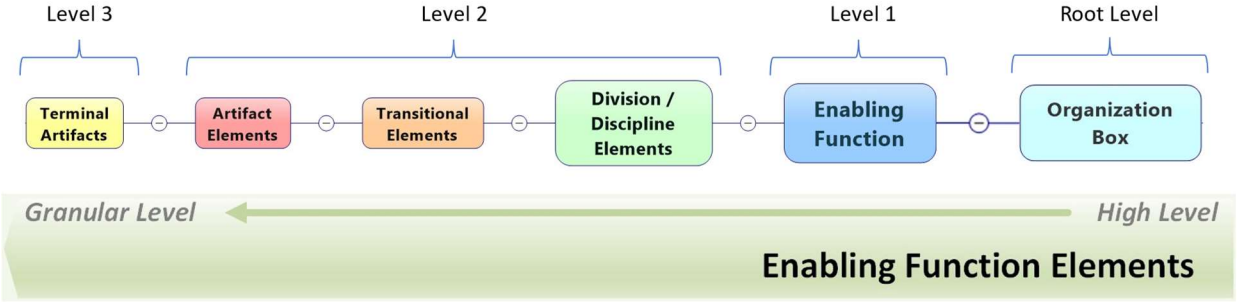


Figure 3: Hierarchy of Enabling Function Elements

The Level 1 Enabling Function elements, positioned closest to the root Organization Box, identify foundational groupings that exist within the organization. These high-level elements often mirror the major sections of an org chart and describe clear and fundamental divisions of expertise and labor.

> ***Level 1 Elements for Enabling Functions*** *describe an organization's major divisions of labor and activity. These are similar to the major categories found on an org chart.*

The Level 2 mid-level elements are used to capture the complexity inherent to modern business execution. These elements break down the Enabling Functions into three groups. Moving from higher to lower levels (right to left) we have "Division / Discipline Elements," "Transitional Elements," and

"Artifact Elements." There is no set number of Level 2 elements needed to describe each branch of the Enabling Function mapping, but it often requires a branch comprised of several elements.

Example Division / Discipline Elements

These elements are used to specify an organization's division of labor, expertise, and infrastructure into more specialized skillsets and refined areas of focus for delivery of the Enabling Functions. The following ideas are provided to help avoid missing some less-obvious Division / Discipline elements. These are particularly useful when performing a very thorough mapping of Enabling Functions.

Policy and Procedure

Policies and procedures are often a cornerstone for any design and operations activities within an Enabling Function. For example, Level 1 elements such as Communications, Information Technology, and Engineering are typically implemented with support services that include policies and procedures. Including elements to describe how policies drive certain activities helps to depict administrative controls that impact the functions being analyzed.

Design

Communications, Information Technology, and Engineering will typically include a design component that optimizes delivery of its Level 1 Enabling Function for the organization. For example, Level 1 elements like Operations or Support Services are unlikely to have design divisions internally, but rely on internal capabilities or require an external subcontractor for any infrastructure or system design needs.

Production

The higher-level *Operations* Enabling Function is typically delivered by a Division / Discipline group focused on production. Operations is where the "rubber meets the road" for the organization, and operations as a function supports production both directly and indirectly through Communications, Information Technology, and Engineering. Such groups provide associated specialized skillsets and, thus, indirectly support production, often represented on different branches of the taxonomy.

Information Technology and Cybersecurity

Information Technology (IT) groups often require a Division / Discipline element for cybersecurity. **Note:** Distinguishing between IT and OT cybersecurity teams is important if the organization divides their workforce into distinct departments, particularly if they reside in different Level 1 elements.

Support Services

Support services provide Enabling Functions for all businesses but is not directly involved in designing, operating, or maintaining infrastructure and PPTII for the delivery of Critical Functions. These include suborganizations responsible for marketing, financial, legal, compliance, administrative, testing, environmental, etc.

Please Note that in a detailed mapping, Support Services warrant special consideration and effort to enumerate for the subject organization. It is important to consider how the organization conducts supply chain activities (e.g., purchasing, delivery, receipt, storage) and contracts with third parties to understand external factors and dependencies.

Research and Development Plus Exploration

Some organizations need to integrate Research and Development plus Exploration when enumerating their Enabling Functions at lower, more granular taxonomy levels. These are largely sector or business specific with varying degrees of relevance or dependencies shared among the major Level 1 elements.

Such Level 2 elements allow the function-based taxonomy to bridge the larger, more foundational elements positioned closer to the Organization Box with those providing relevant infrastructure (e.g., communications networks), applied technologies (e.g., control systems, devices, etc.), specific processes (e.g., emergency shutdown procedures), and key people (e.g., vendor contacts).

> ***Level 2 Elements for Enabling Functions:***
>
> ***Division / Discipline Elements*** *describe an organization's division of labor and infrastructure into more specialized skillsets and refined areas of focus for delivery of the Enabling Functions.*
>
> ***Transitional Elements*** *describe the people, processes, technologies, information, and infrastructure an organization uses to both logically and physically deliver the Critical Functions. Located on the left-hand side of a functional taxonomy.*
>
> ***Artifact Elements*** *describe component elements of the systems they belong to, including specific hardware, software, and sub-processes that are part of a transitional element and retain their own unique functionality.*

Finally, on the very end of each branch of the taxonomy mapping reside Level 3 elements, or "Terminal Artifact Elements." Level 3 elements are unique because they identify specific artifact types that describe the artifact they branch from (e.g., Configuration Files, Specifications, or Operator Contact Information). These Level 3 Terminal Function elements typically only span a single level, but a single Artifact Element will often have multiple Level 3 elements. For example, a device or component within a fire suppression system (the Level 2 Artifact Element) may have a technical manual, an operator's guide, a maintenance schedule, and an inspection log that all reside on the function-based taxonomy as Level 3 elements that provide context and information about that artifact.

> ***Level 3 Terminal Elements for Enabling Functions*** *identify specific artifact types that describe specifications, installation details, specific configurations, maintenance requirements, or standard operations of the Artifact Elements they branch from. Located on the very end of each branch.*

Taxonomy Example: Water Treatment Organization

To help illustrate the basic application of this function-based taxonomy framework, the following sections will explore the Critical and Enabling Functions for a water treatment organization. Each pertinent level of the example taxonomy will be described and diagramed. Please note, this example is not exhaustive.

Water Treatment Organization: Critical Function Structure

Level 1 Critical Function Elements

In our example, the water treatment organization's Critical Functions are identified as: *Water Treatment, Water Sourcing, Water Distribution*, and *Reporting & Regulatory Actions*. Level 1 Critical Function elements describe the primary distinct critical business functions for the organization. Each Critical Function is then added as a Level 1 taxonomy diagram element (see Figure 4).

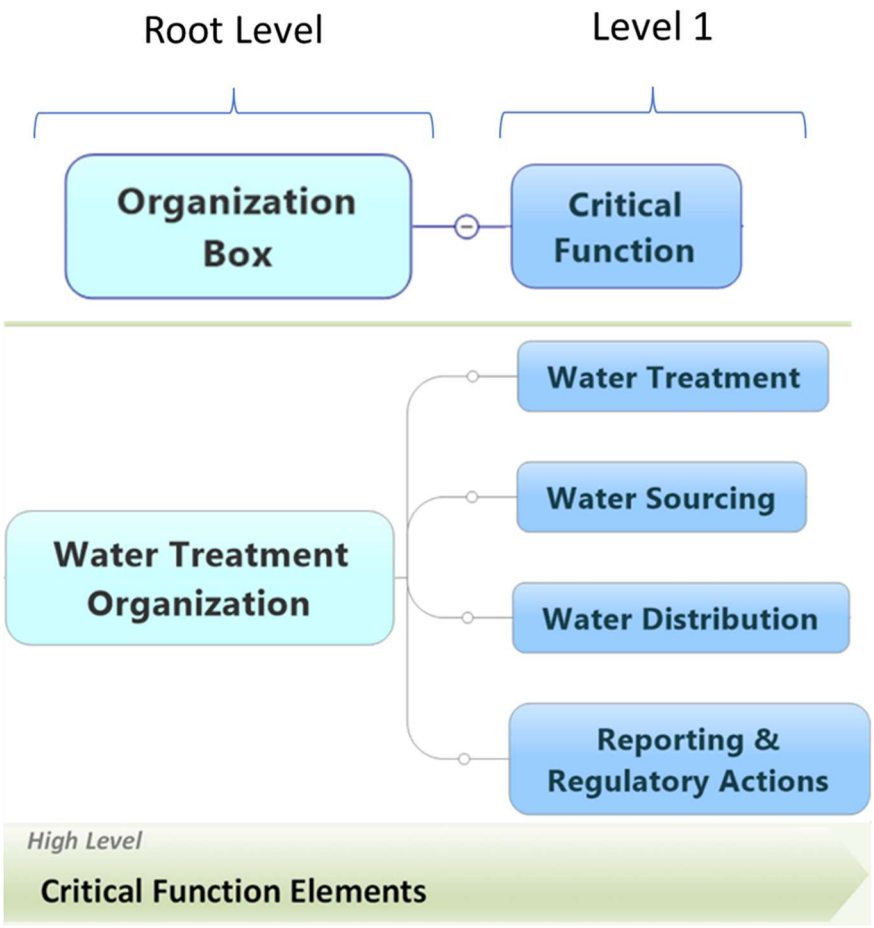


Figure 4: Example Level 1 Critical Function Elements

This representation provides an overarching example of several water treatment organization functions. However, when developing a taxonomy for a specific purpose, only those branches of Critical Functions of interest need to be explored in detail when mapping a function-based taxonomy. For example, if a study were to focus on the presence of chemicals in drinking water, the function-based taxonomy may only need to explore *Water Treatment*.

Level 2 Critical Function Elements

For this water treatment organization example, the mid-level Critical Function elements help describe more detailed functions that comprise each of the Level 1 elements. These include elements describing Critical Subfunctions and Process Area Functions. Our example has exactly two Level 2 elements per branch, but it is important to note that mid-level element section of the taxonomy mapping structure can have differing numbers of elements. Importance is placed on accurately reflecting the complexity of actions and activities that produce the Level 1 Critical Functions.

Critical Subfunctions

Critical Subfunctions describe the major processes that exist within a primary Critical Function. In the simplified example below, the Level 1 Critical Function of *Water Sourcing* has a critical subfunction of *Water Transport*. This critical subfunction describes the process system function responsible for the source water delivery systems. In comparison, the Level 1 element titled *Water Treatment* has two critical subfunctions that branch from it: *Solids Removal* and *Chemical Injection* (see Figure 5).

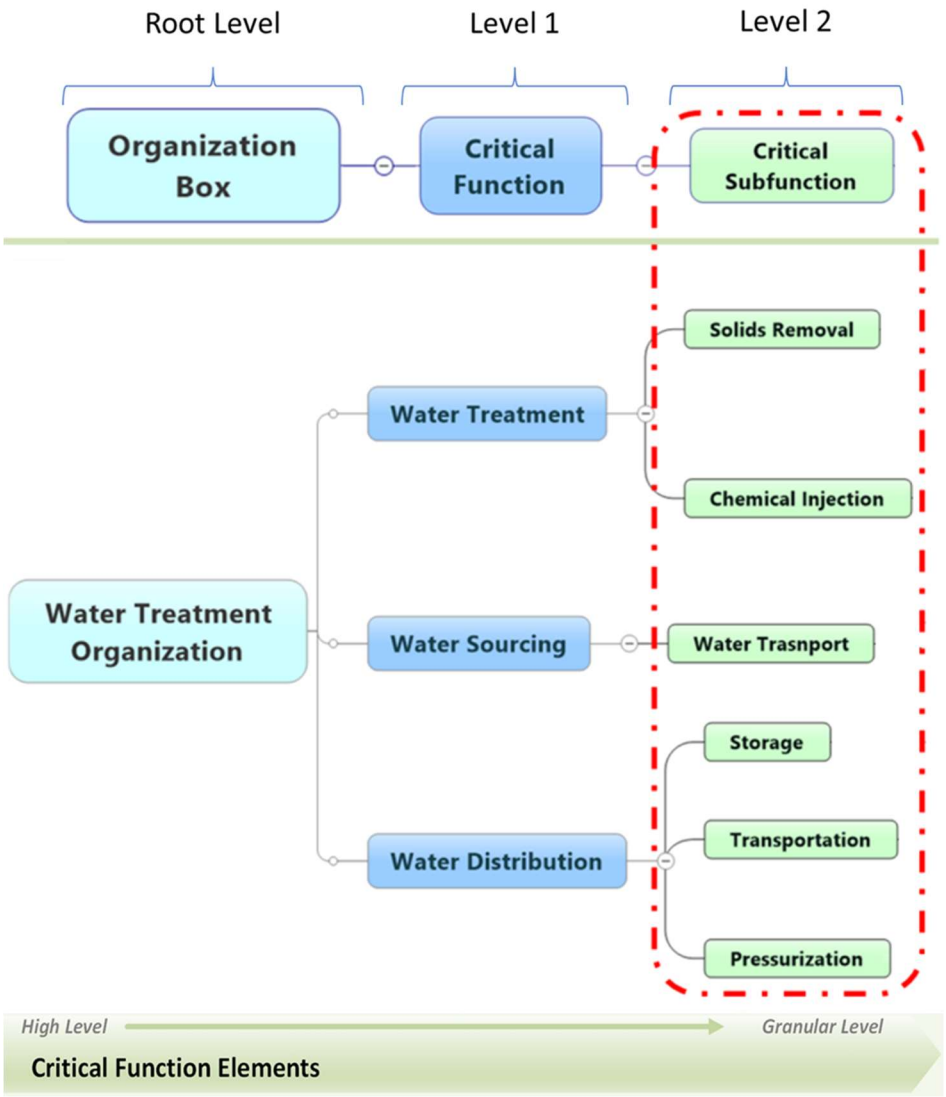


Figure 5: Critical Subfunctions of Example Water Treatment Organization

Process Area Function

Process Area Functions describe the key areas of each subfunction. The first example branch in Figure 6 defines Process Area Functions that support *Solids Removal* as *Holding*, *Coagulation / Flocculation*, and *Filtering*. In this simplified water treatment organization example, these actions allow the organization to pull unwanted solids from the sourced water, which constitute important activities that make up the organization's larger water treatment function.

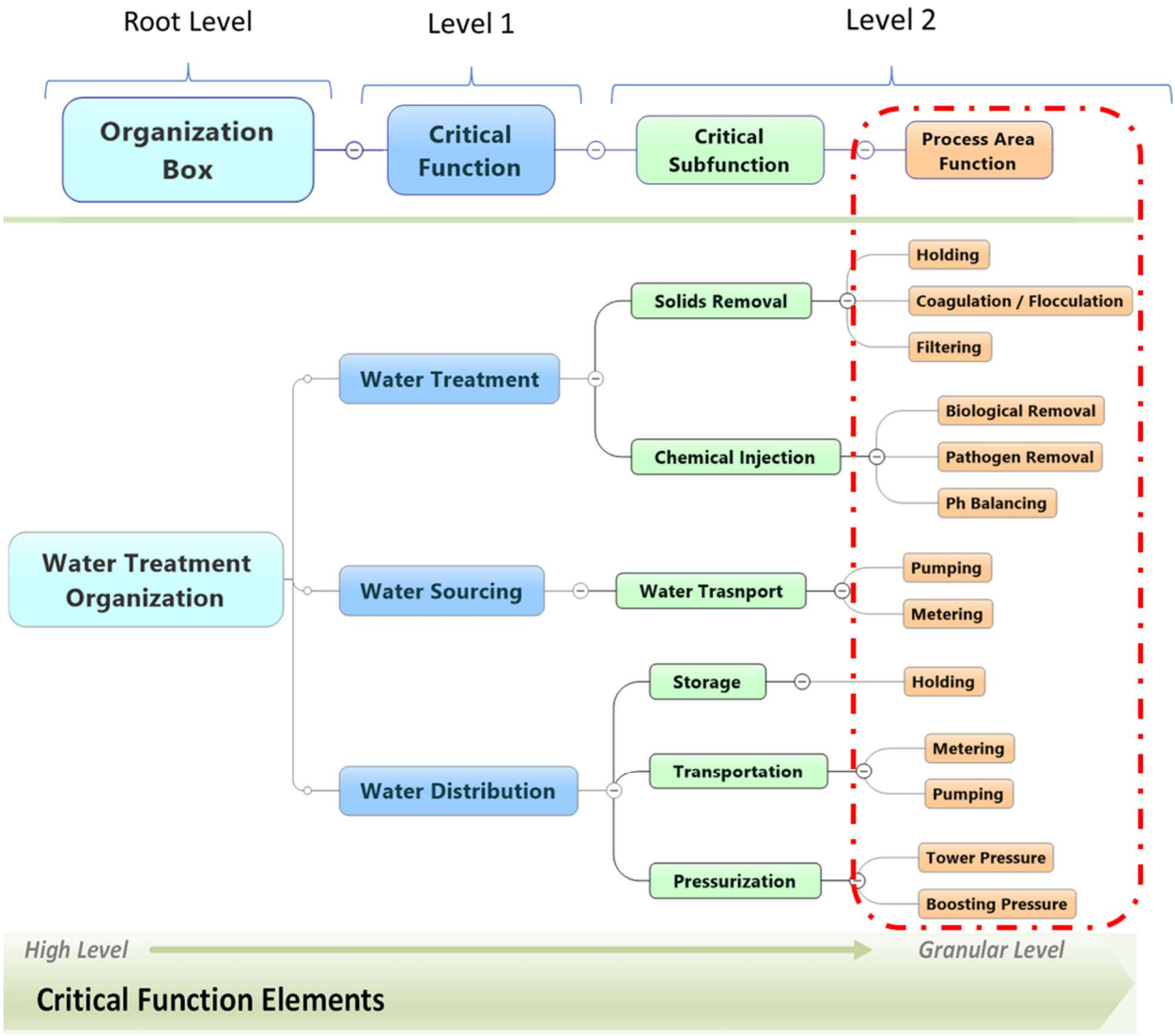


Figure 6: Process Area Functions of Example Water Treatment Organization

Lower Levels

In very specific cases, subfunctions to the Process Area Functions may be necessary. These follow the same pattern seen here. Each subfunction along a specific Critical Function branch should describe the actions and activities that are performed to achieve the preceding element. For our water treatment example, Process Area Functions are sufficient to describe the actions performed. Eventually, these actions and activities cannot be broken down further.

Water Treatment Organization: Enabling Function Structure

Level 1 Enabling Function Elements

As explained previously, Level 1 Enabling Function elements describe high-level divisions of expertise and labor within a business. These are foundational groupings within an organization and are usually easy to identify. The mapping shown in Figure 7 identifies three Level 1 Enabling Functions, *Engineering, Operations,* and *Maintenance,* that capture this example organization's foundational function groups. Mapping out Enabling Functions can become very complex. Our example is not exhaustive, but intentionally simplified to provide clear examples for each level.

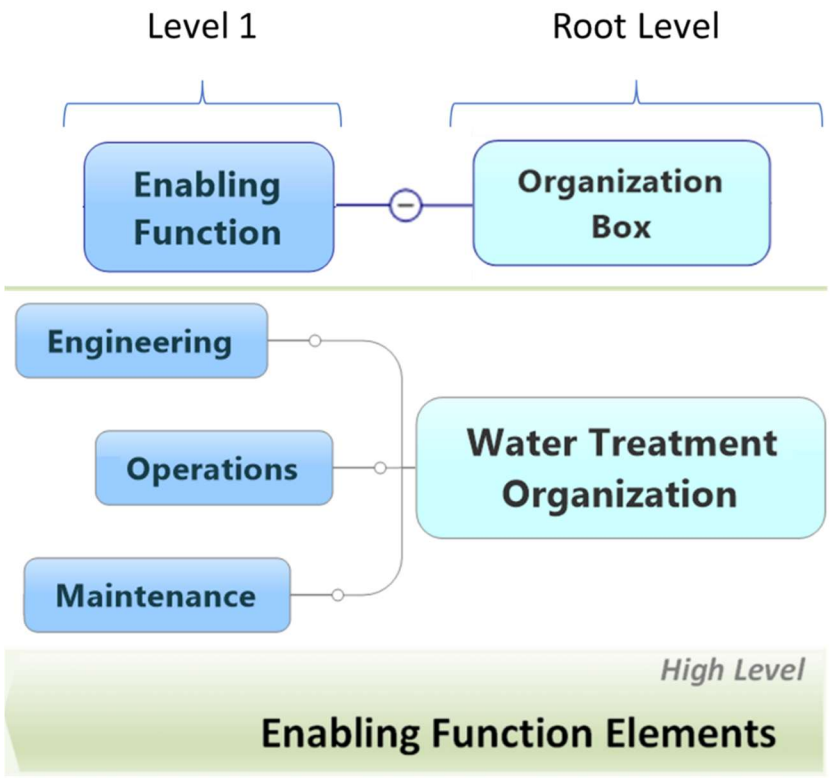


Figure 7: Example Level 1 Enabling Function Elements

The water treatment organization's *Engineering*, *Operations,* and *Maintenance* groups work together to perform the actions and activities mentioned previously. Each group represents a major division of labor and expertise within the notional water treatment organization, and thus their roles and responsibilities differ greatly. Recognizing this, we are prepared to move lower to the next level of Enabling Functions.

Level 2 Enabling Function Elements

As explained previously, the Level 2 elements on the left-hand side of the taxonomy divide into three groups within the taxonomical hierarchy. Positioned on the left-hand side of the Organization Box, these develop from higher to lower levels (right to left) as *Division / Discipline Elements*, *Transitional Elements*, and *Artifact Elements.*

Division / Discipline Elements

The first grouping in the Level 2 elements is *Division / Discipline.* These elements are used to specify an organization's division of labor, expertise, and infrastructure into more specialized skillsets and refined areas of focus for delivery of the Enabling Functions. For our example, we will briefly describe the specific lines of effort for *Engineering*, *Operations*, and *Maintenance* efforts.

Division / Discipline Elements: Automated Systems (Engineering)

The automation conducted at lower (more detailed) levels is performed by specific devices that were selected, programmed, and configured according to the efforts performed in the *Engineering* division called the *Automated Systems* division. The automation required to enable a water treatment organization's Critical Functions combines the needs for reliability, safety, and availability of equipment used to handle the necessary quantities of treated water.

Division / Discipline Elements: Design (Engineering)

The Engineering group's *Design* efforts relate to the functional design of facilities and the equipment used inside. As part of *Engineering*, their focus is largely centered on reliability and functionality to ensure the organization can deliver treated water for a long timeframe and without interruption.

Division / Discipline Elements: Control and Monitoring (Operations)

In our example, the Level 1 *Operations* element requires resources (people and equipment) specific to *Control and Monitoring*. SCADA operations, connected equipment, procedures used by operators to observe, and intervene, when necessary, all make up this sub-group of Operations.

Division / Discipline Elements: Laboratory Ops (Operations)

Laboratory Operations are distinct from the second item, but both are required for water treatment to occur. The environment, policies, equipment, and procedures used to ensure water is properly treated are all different from the *Control and Monitoring* division but prove to be equally essential for this organization to deliver their Critical Function.

Division / Discipline Elements: Calibration (Maintenance)

Calibration is required for the various instrumentation and must be regularly confirmed or adjusted. The *Maintenance* group in charge of calibrating will employ special tools to interact with various sensors and control elements, ensuring accuracy of key instrumentation and verifying them against predetermined specifications.

Division / Discipline Elements: Programming (Maintenance)

Ongoing *Programming* is performed and confirmed by *Maintenance* personnel according to the specifications provided to them by Engineering. Communication between these groups helps ensure that equipment functions and performs as specified.

Division / Discipline Elements: Repairs (Maintenance)

Equipment failures and end-of-life replacements may take place at irregular times. *Maintenance* personnel use procedures and specialized equipment to perform *Repairs* to systems that fail to deliver Critical Functions. *Repairs* range from simple tasks to highly-involved efforts to replace critical components, with a focus on minimizing downtime.

In Figure 8, these Level 2, Division / Discipline elements are shown within the example function-based taxonomy.

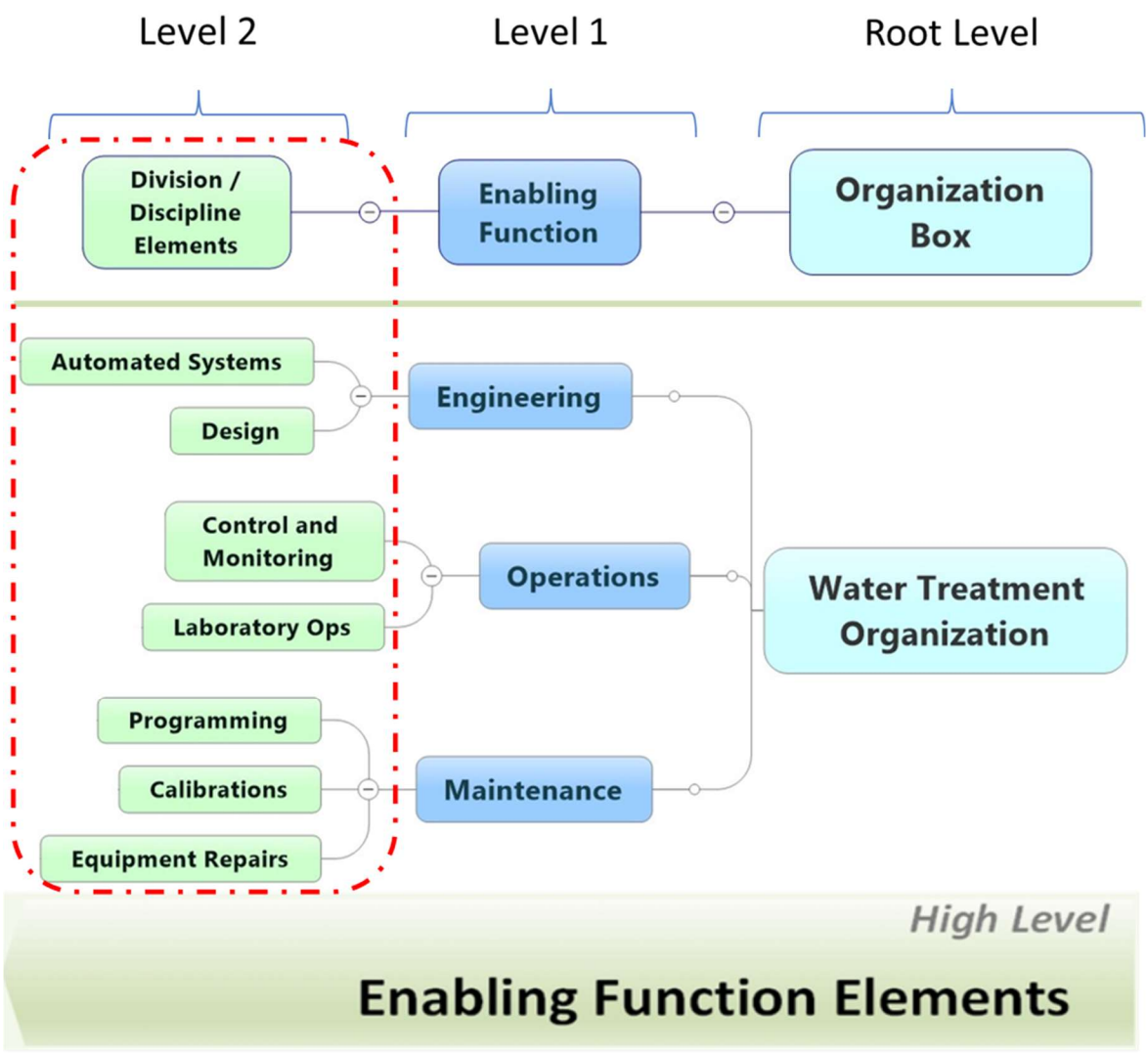


Figure 8: Level 2 Enabling Functions, Division / Discipline Elements

Transitional Elements and Artifact Elements

In the extension of Level 2 elements, a range of transitional and placeholder elements provide a logical and sequential grouping. For every taxonomy, such element types are represented uniquely for each subject organization's model and infrastructure. This often expands the taxonomy significantly. To reduce the visual complexity, our example water treatment organization's taxonomy will look at the Level 2 elements branching out from the *Engineering* Enabling Function.

Within the higher-level Enabling Function, *Engineering*, our example taxonomy shows two disciplines, *Automated Systems* and *Design*. Both Engineering groups share infrastructure Transitional Elements that represent the organization's various structure types (*Water Tower*, *Pump Station*, and *Treatment Plant*).

Although infrastructure-focused Transitional Elements are shown for both disciplines, they are not duplicative. From these elements, the two *Engineering* branches can expand out to the Artifact

Elements. These items (*PLCs*, *Wireless Communication Devices*, *Sensors*, *SCADA Platform*, etc.) must logically align with their respective disciplines. These more granular elements represent the physical devices and platforms that are then used to fulfill the group's functional needs within a particular station or plant type.

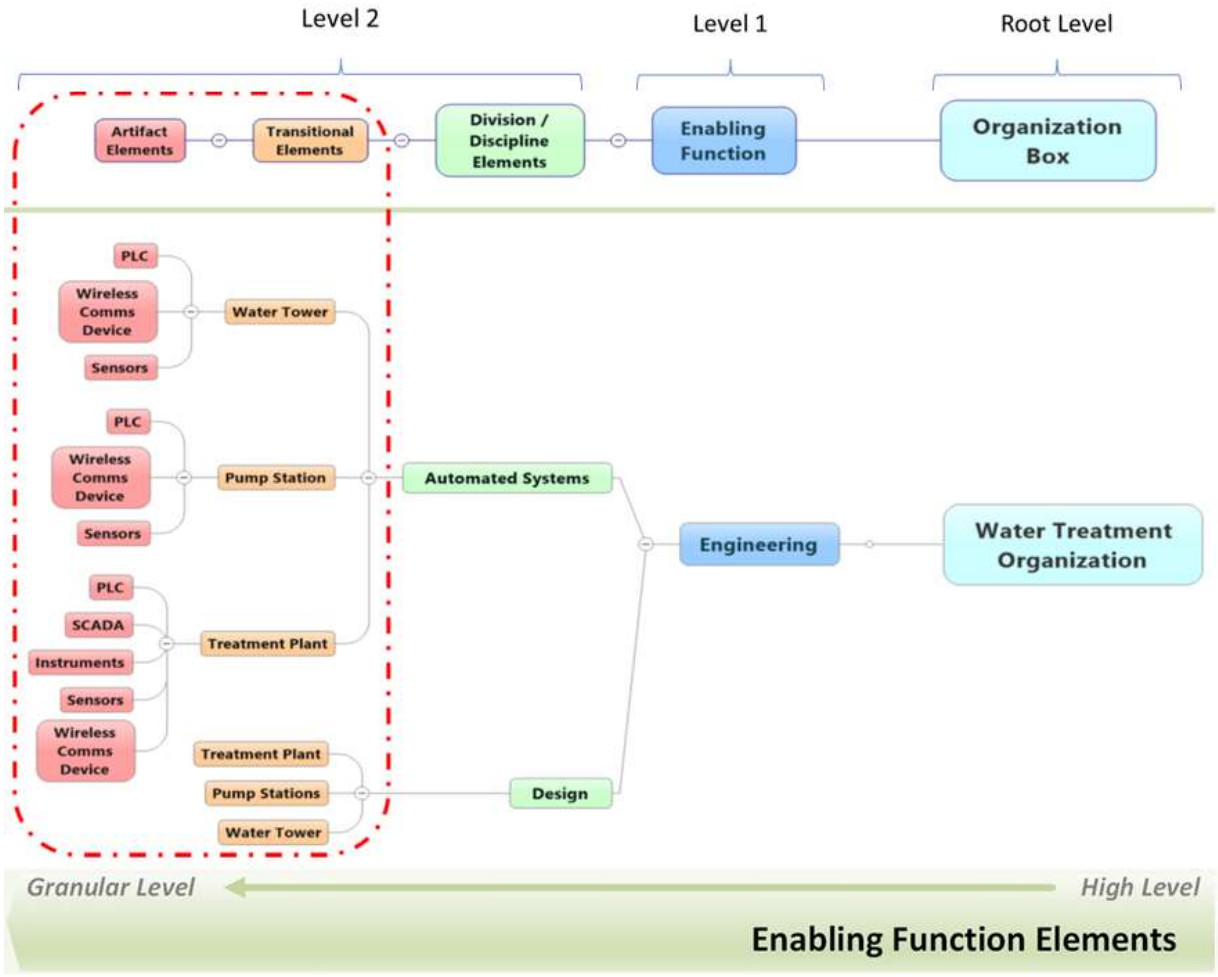


Figure 9: Level 2 Enabling Functions, Transitional Elements and Artifact Elements

Level 3 Enabling Functions: Terminal Artifacts

In our water treatment organization, the Level 3 Terminal Artifacts reflect very specific artifact types: *Specifications*, *Technical Manuals*, *Configuration Files*, *Application Files*, etc. Level 3 Terminal Function elements are typically single level, but each Artifact Element will likely have multiple Terminal Artifacts to describe them. These are often documents, and reflect the unique implementation of its preceeding Artifact Element. By viewing Terminal Artifacts in the context of the various Enabling Function element levels, their role in delivery of a Critical Function is readily apparent.

In Figure 10, Terminal Artifacts are shown as they relate to a specific programmable logic controller (PLC), specific to a *Water Tower*, and would describe how the *PLC* is engineered to support automation for the water treatment organization.

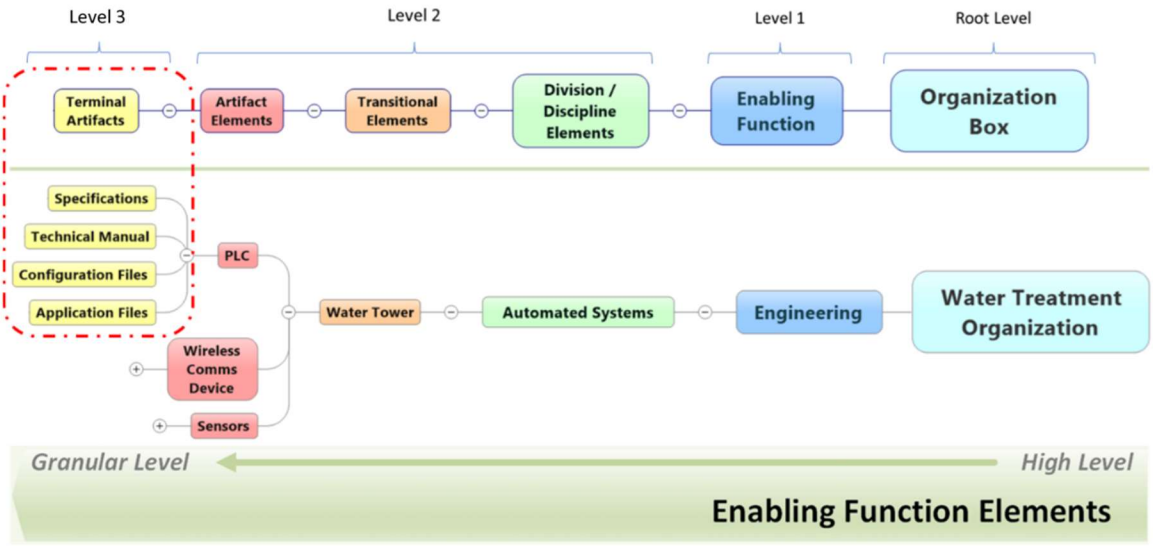


Figure 10: Level 3 Enabling Functions, Terminal Artifacts

Summary

Using a function-based taxonomy, any organization can explore their primary activities and actions to see how they are delivered in a visual and concrete manner. By methodically connecting elements together and displaying them in a heirarchical framework, an organization's Enabling Functions can be studied and better understood. This allows for more productive collaboration and better insight when discussing the importance of various artifacts, how they are used to deliver, produce, and ensure the organization's Critical Functions.

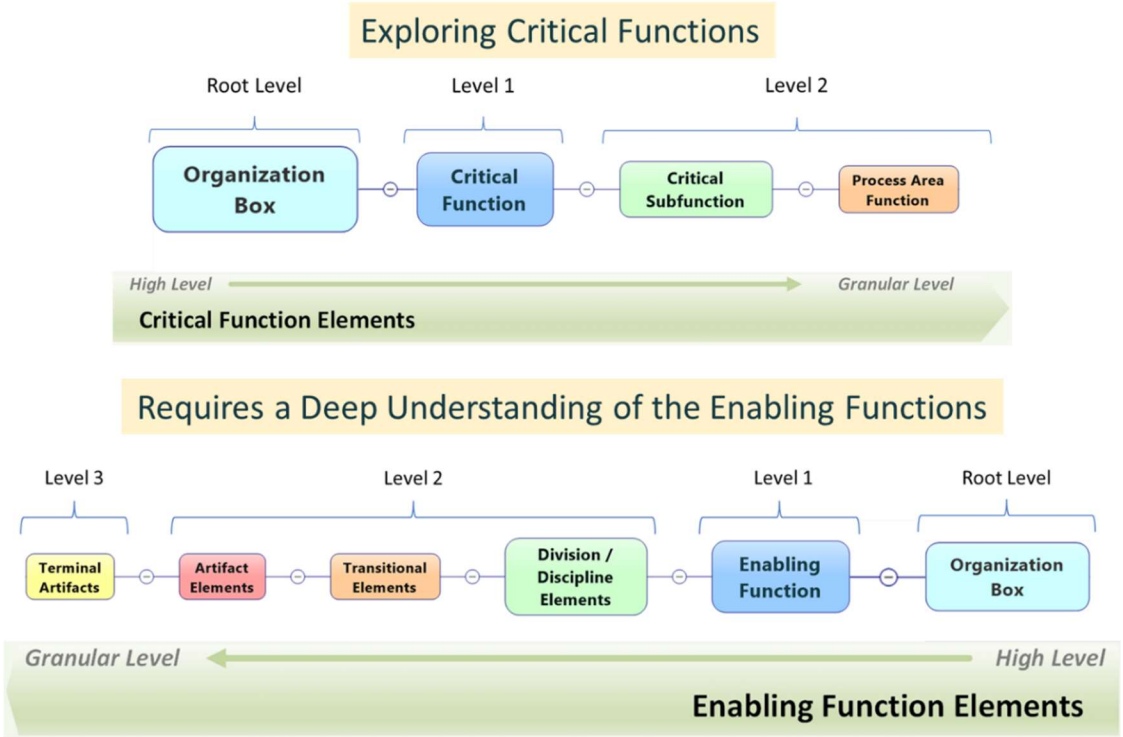


Figure 11: Function-based Taxonomy Summary