

# **Boundary-Based Approach to Chain of Custody**

**Daniel Krementz, *Savannah River National Laboratory***

**Ian Hayes, *Atomic Weapons Establishment, UK***

**Joshua Cunningham, *Consolidated Nuclear Security, LLC***

**Joshua Flach, *NNSA Packaging and Transportation Division***

**Richard Headley, *Pacific Northwest National Laboratory***

**William Johnson, *Savannah River National Laboratory***

**Matt MacDougall, *Pacific Northwest National Laboratory***

**HaliAnne McGee-Hilbert, *Pacific Northwest National Laboratory***

**Kate McIntosh, *Los Alamos National Laboratory***

**Karen Ventura, *currently The Aerospace Corporation, contributions while employed at the Pantex Plant***

**Ben Stanley, *Atomic Weapons Establishment, UK***

## **Abstract**

A boundary-based approach to the implementation of a Chain of Custody (CoC) system to the weapons dismantlement lifecycle has been developed over the past few years. The boundary-based approach uses a prescribed methodology to frame the dismantlement verification problem that results in a description of dismantlement processes and CoC measures in a graphical flowchart form. This approach has potential to be a tool in future arms control agreements to:

1. Describe dismantlement activities and associated CoC measures to treaty negotiators in a condensed graphical format to aid in making more informed decisions during treaty negotiations.
2. Aid in the identification of processes where CoC measures are needed and the types of CoC technologies/approaches that should be used for improved confidence in the treaty verification regime.
3. Provide a visual aid to describe the dismantlement steps and associated CoC measures to host and inspector teams during treaty verification visits.

## **Introduction**

Over the past few years work has been carried out to on the development of systematic approaches to treaty verification that are intended to help prepare states for future arms control agreements. The Boundary-Based Approach to CoC will be a graphical tool that could be helpful in both the treaty negotiation and implementation processes. This paper describes development of this Boundary-Based Approach to the implementation of a CoC system within the weapons dismantlement lifecycle. The weapons dismantlement lifecycle is defined by the International Partnership for Nuclear Disarmament Verification (IPNDV) 14 steps, [https://www.ipndv.org/wp-content/uploads/2017/11/IPNDV\\_14-steps-diagram-Final.pdf](https://www.ipndv.org/wp-content/uploads/2017/11/IPNDV_14-steps-diagram-Final.pdf), however here we focus on steps 6-10 of the IPNDV Basic Dismantlement Scenario as the key areas of interest. The intent of this approach is to improve the process of identifying CoC system requirements by highlighting the aim of the CoC system and characterizing potential routes to exploit the system. Establishing

clear CoC system requirements allows for streamlined selection and application of CoC measures designed for use under an arms control agreement. The work described is intended to generate ideas and is not representative of any government positions.

## **Background**

A CoC system is designed to supplement inspection activities, providing a means to detect undeclared access, or movement of a Treaty Accountable Item (TAI). The aim of a CoC system is to detect attempts to divert or counterfeit a TAI or detect misuse of facilities or processes relevant to the treaty. CoC poses a variety of challenges and may rely heavily on technology for successful execution.

This boundary-based approach builds on a dismantlement analysis for treaty accountable items, which outlined the notionally permitted processes expected on a TAI, including moving the TAI from one location to another, changing the container that the TAI is transported/stored in, removal of non-nuclear (NN) components from the TAI, and separation of special nuclear material (SNM) from high explosives (HE). These permitted activities allowed for the definition of 3 basic processing categories. The first is Static Processes, which refers to situations in which there are no changes to the location, container, or components of the TAI. The second category is a Transit Process where the TAI container and components do not change, however it is moved from one distinct location to another. The final category is a Dynamic Process in which changes are made to the TAI, its containment, or both, within a defined location.

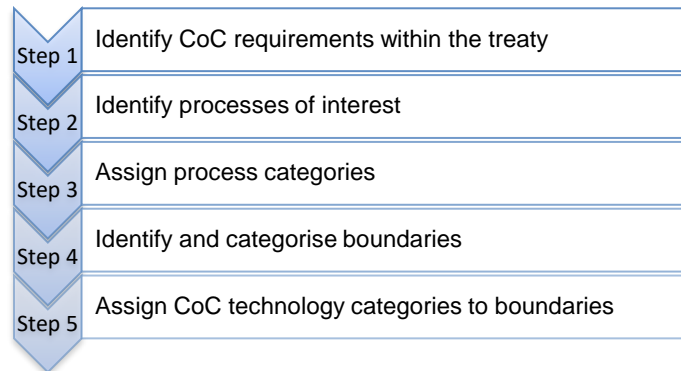
The purpose of a boundary in CoC is to identify, encompass, or restrict access to a location or item of interest. This allows a CoC measure to be implemented to form a layer of protection around a facility, process, or item of interest. Facilities, items, or processes may be surrounded by a single boundary or by multiple boundaries for layered CoC measures depending on the system requirements. The aim of the boundaries is to facilitate identification of undeclared items or processes and to make diversion, substitution or counterfeiting of declared items difficult to achieve and easier to detect.

The boundary-based approach to CoC is a method for simplifying the implementation or evaluation of a CoC system by systematically deconstructing a given system into individual categorized processes, recognizing and crediting the inherent boundaries where possible, and implementing CoC measures to increase confidence that a boundary has not been breached thereby ensuring that CoC requirements are satisfied. This approach yields a visual representation of the CoC system, which is hereafter denoted as the 'Model'. The Model is a useful tool for visually depicting the layers of boundaries, the CoC measures that protect each boundary, and the application/verification/removal of CoC in each step of a process. The Model is particularly useful in large process chains.

## **Method**

The boundary-based approach to CoC consists of 5 steps as defined in Figure 1. In the first two steps, the containment and surveillance requirements and processes of interest are defined. The information gathered in steps 1 & 2 constitute the inputs and are the foundation of the boundary-based approach. Accuracy of the inputs is of critical importance as errors will propagate and magnify at the later stages. In the later three steps, process categories are assigned, boundaries are identified and categorized, and CoC technology is assigned. The last 3 steps integrate the inputs into the boundary-based approach, which is used to develop a suitable CoC system that is

compliant with all requirements or to evaluate a CoC system for insufficiencies. Each step is further discussed in the following subsections.



**Figure 1: Boundary-Based Approach to CoC Methodology**

### Step 1: Identify CoC Requirements within the Treaty

CoC requirements are conditions that a CoC system must meet to fulfil the needs of the host and/or inspecting parties. CoC requirements would be derived from treaties, regulations, or facility requirements. A clear understanding of the requirements of the treaty being implemented is needed before a CoC system can be designed. Formulation of CoC requirements will likely require familiarisation with the treaty requirements and may include understanding the TAIs, the treaty inspection time frames, and treaty relevant procedures. CoC requirements are also likely to involve discussions between treaty stakeholders.

Both the host and inspecting parties will typically generate CoC requirements that are specific to their interests. Requirements generated by the host party typically relate to concerns regarding unintended sensitive information disclosure, unintended inspecting party access to TAIs or host technology, facility safety protocols, and preventing obstruction of the facility processes. For example, host facilities may have authorized or prohibited technology groups based on their own safety and security requirements and these requirements would have to be satisfied by the CoC system implemented. Requirements generated by the inspecting party typically relate to concerns regarding unauthorized host access to TAIs, unauthorized host transport of TAIs, unauthorized modification or diversion of TAIs, and unauthorized tampering of inspecting party inspection equipment. For example, an inspecting party may have concerns regarding potential diversion paths within a facility. The associated CoC requirements may include identification and familiarization of relevant facilities or containers, including design verification. CoC requirements should address any security concerns that arise during treaty review and/or discussions with stakeholders.

### Step 2: Identify Process(es) of Interest

Processes of interest are operations where CoC requirements need to be enforced or ensured. Identification of processes of interest is typically informed by treaty familiarization, discussions with experts and stakeholders and/or observing processes to understand how they are performed. Processes of interest need to be fully understood as part of the implementation of an effective CoC system. After the processes of interest are identified, a CoC system may be designed to detect diversion, counterfeiting, or other undeclared processes.

### Step 3: Assign Process Categories

The categories of processes (Table 1) are derived from the findings of a previous US-UK study on Dismantlement Analysis for Treaty Accountable Items, which is a specific scenario of focus for the boundary model. The study describes three categories of processes: Static, Transit, and Dynamic, which describe the primary ways that a process can impact a TAI. Dynamic processes are further divided into three subcategories: Dynamic - container, Dynamic – Non-Nuclear (NN) component, and Dynamic – Special Nuclear Material (SNM), which identify the type of Dynamic change that occurs. Although the process categories were first defined for use in warhead dismantlement processes, they may be applicable to other operations and should not be limited in use where relevant.

The type of process being carried out will impact the choices of boundary types, locations and technologies that are used within the system. To allow for suitable boundaries to be identified, the item/process needs to be understood and the process type assigned. The application of boundaries and suitable technologies will depend on meeting the requirements of the system, focusing on the type of facility, dismantlement process, and technology intrusiveness.

**Table 1: Boundary-Based Approach to CoC Process Types**

Process Types	Change Location	Access/Change Container	Remove Components
Static			
Transit	X		
Dynamic – Container		X	
Dynamic – NN Component		X	X (NN)
Dynamic - SNM		X	X (SNM)

#### Static Processes

Processes where the TAI's location and form are unchanged are defined as *Static Processes*. Static processes include staging and storage activities, including in-process storage of TAIs, which may occur in a building or room specifically designated for this activity. CoC can most easily be applied to Static processes since the TAI is not involved in any changes (i.e. processing or movements). This would allow CoC to be applied at the container, room, or building level and would require minimal access from inspectors to sensitive operational environments. Static processes are likely to have a Transit process before and after them, as this would require moving the TAI to and from the storage/staging building.

#### Transit Processes

*Transit Processes* occur when a TAI is moved in its container from one location (room or building) to another, but the form, components and, if applicable, container are unchanged. The CoC technology used in Transit processes must accommodate changes in location. CoC at the room or building level is more challenging in Transit processes than Static processes; however, the integrity of the container would remain intact and would still provide a boundary.

#### Dynamic Processes

*Dynamic Processes* describe activities which alter the form, components, or container of a TAI, but not the location. It is assumed that application of CoC to a Dynamic process would be the

most challenging to implement, as inspectors are traditionally not allowed within an operational facility where the container or weapon boundary is breached.

A Dynamic process will occur within a single location and is characterized by a change to the item or its containment. During a Dynamic process, there will be periods where the item is no longer containerized, and the method of containerization may also change. A Dynamic process may also see changes to the item within the processing area (i.e. removing non-nuclear and/or nuclear components from the item). The changes to the item or container likely dictate that the CoC system will not be within the processing location.

#### Step 4: Identify and Categorise Boundaries

Boundaries are identified in Step 4 of the Boundary Approach to discern locations where a CoC measure may be implemented to meet the CoC requirements of the system. Step 4 is heavily influenced by the inputs of the first three steps. The intent of a CoC boundary is to establish a perimeter or barrier that isolates an item from the environment; thereby creating two unique areas: an interior and an exterior. Boundaries may be used alone or in layers as needed to meet the CoC requirements. As previously mentioned, physical CoC boundaries may be formed using integral structures (e.g. walls, doors, containers) or by constructing temporary barriers using a variety of technology and infrastructure. Virtual boundaries (intangible perimeters surrounding a monitored area) may also be considered as part of the CoC system. Virtual boundaries are monitored by technology but would not involve the use of physical barriers. Virtual boundaries would be reliant on the use of portal monitoring, cameras, laser curtains, etc.

CoC boundaries are categorized in three groups: Static, Transit, and Dynamic boundaries, which are discussed in the following subsections.

#### Static Boundaries

Static boundaries are immobile, impermeable perimeters around an area that can be used to physically deter both unauthorized access to and movement of a TAI. Static boundaries should surround an area such that the boundary is difficult to traverse without authorization but may feature secured openings to facilitate travel through the boundary (e.g. a door). Examples of static boundaries include a room enclosed by four walls and a door, a fenced perimeter equipped with a gate, and a hallway with guarded exits.

#### Transit Boundaries

Transit boundaries are mobile, impermeable, physical barriers that deter unauthorized access to a TAI. Transit boundaries contrast with Static boundaries in that they do not restrict or control the movement of a TAI. Transit boundaries should surround an area such that the boundary is difficult to breach without authorization but may feature secured openings to facilitate opening/closing the boundary (e.g. a container door or hatch). Transit boundaries typically surround smaller areas, closer to the TAI than Static boundaries. Examples of Transit boundaries include containers, vehicles, and trailers, which can each be sealed and secured with CoC measures including Tamper Indicating Devices (TIDs). The boundaries, in conjunction with the CoC measures, deter unauthorized access to the TAI but allow for unrestricted transportation of the container.

### Dynamic Boundaries

Dynamic boundaries are intangible, permeable boundaries or a combination of intangible, permeable boundaries coupled with physical boundaries. Dynamic boundaries, when used in conjunction with Dynamic CoC measures, deter unauthorized access to a TAI, unauthorized movement/diversion of a TAI, and unauthorized modifications to a TAI. Dynamic boundaries do not physically prevent an unauthorized party from traversing the boundary, but rather deter unauthorized access by threat of detection. Dynamic boundaries are permeable; therefore, they are well suited for Dynamic processes where non-nuclear components and tools are frequently passing through the boundary. Dynamic boundaries provide confidence that a TAI has not been manipulated in an unauthorized manner and are typically the least process-disruptive boundary category for the host.

### Step 5: Assign CoC Measures to Boundaries

After each boundary has been defined, specific CoC measures are assigned to secure or monitor openings or vulnerabilities of the boundaries. CoC measures may include technologies such as seals, unique identification, surveillance, and portal monitoring, or actions such as line-of-sight, design verification, etc. CoC measures may often be used to secure more than one boundary type. For example, a TID can be used to seal a static boundary such as a storage room or it can be used to seal a Transit boundary such as a container.

### Static CoC Measures

Static CoC measures are those that deter unauthorized access to and movement of a TAI when applied to Static boundaries. Static CoC measures include locks, seals, alarmed doors, guards, video surveillance, portal monitoring, etc. Static CoC measures need not accommodate any change in location or form of the TAI by nature of the process. Static CoC measures are often applied at the room or facility level. Examples of Static CoC measures are locks and/or seals that secure a room or facility boundary.

### Transit CoC Measures

Transit CoC measures are those that deter unauthorized access to a TAI, while allowing movement of the TAI. Transit CoC measures include locks, seals, and line-of-sight. Transit CoC measures must accommodate a change in TAI location by nature of the process. Transit CoC measures are often applied at the container level.

### Dynamic CoC Measures













Dynamic CoC measures are those that deter unauthorized access to a TAI, unauthorized movement/diversion of a TAI, and unauthorized modifications to a TAI when applied to a dynamic boundary. Dynamic CoC measures include video surveillance, portal monitors, and signature measurement equipment. Dynamic CoC measures are unique in that they have the potential to validate whether a TAI or item of interest has changed form in some way. For example, a portal monitor can determine whether items moving through it are nuclear or non-nuclear. A video surveillance system that monitors the exit of a single-exit room can track the size and quantity of containers that enter or exit the room.







### Visual model key

Each aspect of the boundary model is identified by a unique, colour-coded icon where, in general, black represents static boundaries/CoC measures, blue represents transit boundaries/CoC measures, and red represents dynamic boundaries/CoC measures. The icons

used in this report are defined below; however, users of the boundary model are not limited to these icons.

**Table 2: Model Icon Descriptions**

Icon	Meaning	Definition
	Static Process	Processes where the TAI's location and form are unchanged.
	Transit Process	A TAI is moved in its container from one location (room or building) to another, but the form, components and, if applicable, container are unchanged.
	Dynamic Process	Activities which alter the form, components, or container of a TAI, but not the location.
	Static Boundary	Immobile, impermeable perimeters around an area that can be used to physically deter both unauthorized access to and movement of a TAI.
	Transit Boundary	Mobile, impermeable, physical barriers that deter unauthorized access to a TAI.
	Dynamic Boundary	Intangible, permeable boundaries or a combination of intangible, permeable boundaries coupled with physical boundaries.
	Static CoC Applied	Static CoC measures, which deter unauthorized access to and movement of a TAI when applied to Static boundaries, are applied. Includes CoC initialization/setup if applicable (e.g., reference images for future verification).
	Transit CoC Applied	Transit CoC measures, which deter unauthorized access to a TAI, while allowing movement of the TAI, are applied. Includes CoC initialization/setup if applicable (e.g., reference images for future verification).
	Dynamic CoC Applied	Dynamic CoC measures, which deter unauthorized access to a TAI, unauthorized movement/diversion of a TAI, and unauthorized modifications to a TAI when applied to a dynamic boundary, are applied. Includes CoC initialization/setup if applicable (e.g., reference images for future verification).
	Static CoC Removed	Static CoC measures, which deter unauthorized access to and movement of a TAI when applied to Static boundaries, are verified, if applicable, and removed.
	Transit CoC Removed	Transit CoC measures, which deter unauthorized access to a TAI, while allowing movement of the TAI, are verified, if applicable, and removed.
	Dynamic CoC Removed	Dynamic CoC measures, which deter unauthorized access to a TAI, unauthorized movement/diversion of a TAI, and unauthorized modifications to a TAI when applied to a dynamic boundary, are verified, if applicable, and removed.

	Static CoC Verified	Static CoC measures, which deter unauthorized access to and movement of a TAI when applied to Static boundaries, are verified, but not removed.
	Transit CoC Verified	Transit CoC measures, which deter unauthorized access to a TAI, while allowing movement of the TAI, are verified, but not removed.
	Dynamic CoC Verified	Dynamic CoC measures, which deter unauthorized access to a TAI, unauthorized movement/diversion of a TAI, and unauthorized modifications to a TAI when applied to a dynamic boundary, are verified, but not removed.
	Inspector Restricted Area	Locations in a host facility where neither the inspecting party nor inspecting party equipment is permitted.
	TAI Process Flow	Directional indicator for processes of interest (i.e. processes that involve a TAI).
	Non-Nuclear Item Flow	Directional indicator for processes that are not of interest (i.e. processes that do not involve a TAI).

## Case Studies

Case studies were performed for treaty monitored dismantlement activities that tested the utility of the boundary-based approach for TAI tracking and whether changes need to be made to enhance its ease of use. Key assumptions made for this study included the following:

- Treaty monitored dismantlement would be conducted in a dedicated facility
- Inspectors are assumed to not have access into the rooms where weapon disassembly operations take place
- Normal production work on weapons was considered out of scope for this study.

A notional Plant Within a Plant, or PWIP, was utilized for this study. The PWIP is a disassembly area cordoned off from the rest of the weapons assembly/disassembly plant by physical or virtual boundaries. This approach allows for inspector access to the facility; however, inspectors would not be allowed in areas of the plant where operations not subject to treaty verification are performed. Figure 2 shows how the model was used to map CoC of a TAI through a notional dismantlement process.

## Conclusion

The case studies performed indicate that the Boundary-Based Approach to CoC is a tool that can provide valuable insights to personnel in the arms control community. Lessons learned from the case studies include:

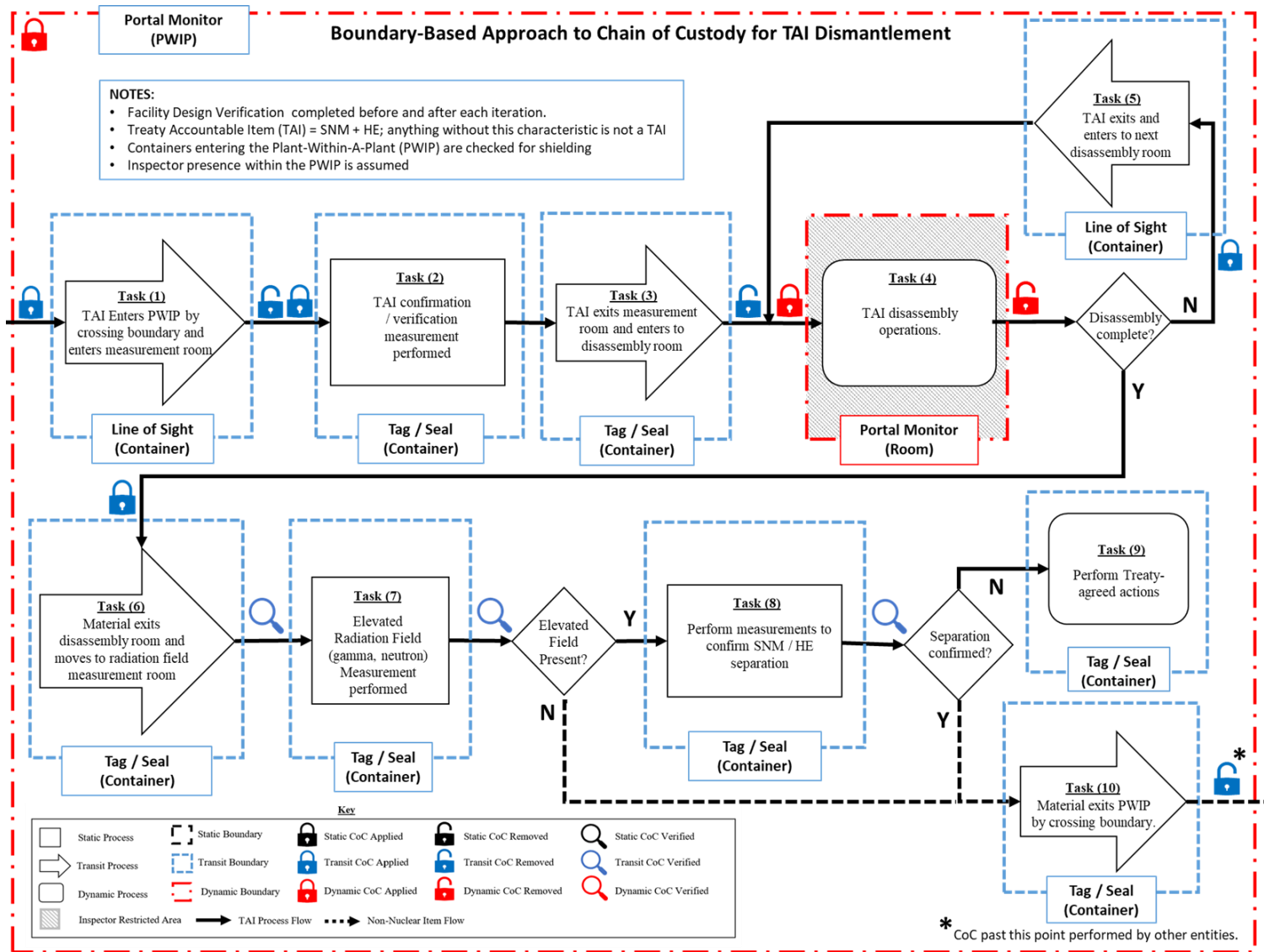
- A review of the boundary approach document and discussion of the tool key is vital for personnel new to the tool as a basic understanding is required to properly interpret the diagrams.
- Development of a final form process map prior to any discussion of CoC measures helps prevent confusion during diagram development.



- Intermediary diagrams indicating the levels of containment available at each process step were found to be useful in evaluating CoC options and down-selecting the desired approaches.

The boundary-based approach to CoC is a tool that simplifies complex processes within a physical environment such as a nuclear weapon disassembly facility. It does this by identifying individual processes, possible boundaries that can be used within a specific physical environment and mapping CoC measures to monitor these for undeclared access or movement of TAIs across a boundary, thereby giving confidence in compliance to a potential treaty.

Testing the boundary-based approach against real facilities proved useful for thinking about how process monitoring is applied and assessed, within a complex system, by CoC measures. In application the tool was refined through use and developed the working group's understanding of methods to represent processes and monitoring opportunities within realistic and relevant physical environments. This tool was developed agnostic of specific technologies or specific monitoring data, it focused on mapping the process accurately and where boundaries could be utilised, with prospective styles of CoC measures e.g. visual data could range from continuous inspector presence, to CCTV recording. To progress this work, technology application could be considered. While the working group considers this a useful tool for considering process or infrastructure monitoring options within any given treaty scenario, it is clear that this is only one potential methodology that could be used for this purpose.



**Figure 2: CoC Approach for Monitored Dismantlement within a PWIP**