The University of Kansas

INFORMATION
& TELECOMMUNICATION
TECHNOLOGY CENTER
The University of Kansas

Technical Report

SensorNet III Requirements Document: Container Transportation Security Network

Leon S. Searl, Ed Komp, Dan DePardo,
Dan Deavours, and Martin Kuehnhausen

ITTC-FY2011-TR-47750-10

January 24, 2011

Project Sponsor:
Office of Naval Research
Award Number: N00014-07-1-1042

Abstract

The SensorNet I: Transportation and Security SensorNet (TSSN) project implemented an architecture for monitoring the security of Intermodal Containers being shipped by rail. SensorNet II implemented a mechanism for verified handoff of Intermodal Containers between shippers using the architecture of SensorNet I. The lessons learned from the SensorNet I and SensorNet II projects identified several aspects of the software, hardware and deployment that should be improved. In addition, the areas of RF communication and sensor power require further study. SensorNet I focused on the Rail Shipping domain, the challenges of the RF communication, networking, power management and security of the trucking, shipping and sorting yard venues that intermodal shipping containers pass through are an area for additional study. A next generation SensorNet is proposed to address the lessons learned and study the issues revealed by SensorNet I and SensorNet II.

Table of Contents

List of Figures

Figure **Page**

1 Introduction

Contained in this document are the Requirements for SensorNetIII. SensorNetIII would be provide additional value beyond the knowledge gained from the SensorNetI (Transportation Security SensorNet) and SensorNetII efforts by using the lessons learned from these previous projects. Container Transportation Security Network (CTSN) is the more descriptive name given to SensorNetIII. Research on the CTSN would be specific to monitoring the security, safety and status of ISO Intermodal Containers shipped on rail and truck and sorted in sea port and rail sorting yards. The requirements, rather than being formal, are a mix of requirements, topics that required further study and actions needed develop the remaining requirements. Although the sea going ship segment of an Intermodal Container's journey is not considered in this document many of the requirements would be applicable and could be implemented.

2 Requirements

The sub-sections within this section contain the specific requirements, options and commentary for the Container Transportation Security Network.

In some instances the current technical knowledge base or regulatory environment prevents specific requirement generation. In these instances further technical studies or regulatory enhancement will be required.

2.1 Network Requirements

This section contains the requirements for the various components of the network. The network components are based on the network components developed for SensorNetI Transportation Security Sensor Network (TSSN).

The requirements are for messages between the Trade Data Exchange and Shipper's Network Operations Center (NOC) and between the Shipper's NOC and the Container Nodes. Between the NOC and Container nodes are Access Points and Wireless Message Relays.

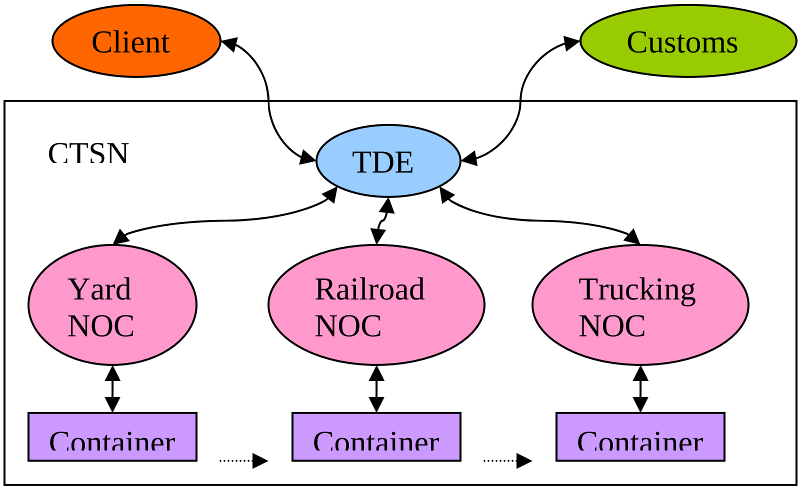

Figure 1 CTSN Player's Connectivity

Figure 1 shows the connectivity requirements of the players in a Container Transportation Security Network (CTSN). A Client/Broker communicates with a Trade Data Exchange (TDE) to setup a cargo shipment that houses the cargo in a CTSN container. The TDE communicates with the Yard (example: Sea Port Sorting Yard), Railroad and Truck shipping companies to arrange a schedule for the shipment and to hand-off custody of the shipment as it passes between the Shippers. At a customs point a customs official communicates with the TDE to obtain the container manifest and to request that security monitoring of the container be relaxed so that cargo may be inspected without setting off alarms. The Shippers communicate with the containers during transit to monitor security and health of the container and report security issues concerning the container to the TDE. The TDE reports container issues to the client when necessary.

2.1.1 TDE and Shipper NOC Network Requirements

Messages between the TDE and NOCs are used in the scheduling and custody exchange of containers between Shippers. These messages are also used for checking and reporting the status of cargo shipments.

The concept of the Trade Data Exchange is a carry over from SensorNetII. For the purposes of this requirements document, the TDE is the portal for shipping clients and customs officials to interface to the CTSN. It also coordinates the transfer of custody of containers from one Shipper to another ensuring that there is always a Shipper taking responsibility for a container during its journey. The TDE is the only authority allowed to make security related configuration changes to the node on a CTSN container.

Each Shipper has a NOC that is responsible for communicating with the TDE and the Container Nodes in the Shipper's custody. Container Node security is monitored and any issues are reported to the TDE.

Requirements of communication between the TDE and NOCs not included in this version of the document include:

- General authentication and authorization
- General message confidentiality/privacy
- Subscription and publication of events/notifications
- Service discovery
- Communication architecture (SOA, ROA, etc).

The following requirements of this section are largely derived from the SensorNetII project.

R-2.1.1.1.1 Each Shipper in the CTSN shall have one or more Unique IDs that identify the Shipper in network messages.

The Shipper Unique ID is used to identify Shippers in network messages. A Shipper may have more than one ID to identify different regions of the globe that the Shipper operates in or different subsidiaries of the Shipper. Each Shipper Unique ID is associated with a unique NOC.

R-2.1.1.1.2 All network messages between CTSN Shippers shall be digitally signed to provide high confidence that the message has not been altered during its travel from the source to the destination.

The digital signing method for messages at this level of the network needs further study and must be agreed upon by a consortium of participants. Since these messages traverse high speed networks with virtually unlimited processor power available the signature length may be long and more computationally intensive compared to the signatures of messages in the Container Network.

R-2.1.1.1.3 The TDE shall provide a Shipper with a best estimate container pickup time and location with sufficient advance notice to prepare for the pickup.

As an example, when a ship carrying containers is to arrive at a sea port sorting yard, the sorting yard must have sufficient time to prepare an empty storing area within the yard for the containers.

For rail transport from a sea port rail yard, the railroad company must move a sufficient number of rail well cars to the rail yard for the expected number of containers.

To transport a container by truck from a sorting yard, the trucking company must send a truck to the sorting yard at the appropriate time.

The same pickup time message is used to notify the Recipient Shipper when a pickup time has changed.

R-2.1.1.1.4 A Shipper shall notify the TDE of a container it is picking up (accepted) from the container's route source or the previous Shipper in the shipping chain.

This requirement is part of the chain of custody requirements. A Shipper that has accepted a container is the Custodian Shipper of the shipment.

The actual pick-up time is included in the messages.

The TDE uses the Custodian Shipper's network to notify the Container Node of the new custodian.

R-2.1.1.1.5 The TDE shall have the capability to query the container's Custodian Shipper for the estimated drop-off time of the container based on current movement state of the container.

Using current location, speed and anticipated speed, current and forecast weather conditions and handling time the shipper will estimate the drop-off time of the container.

R-2.1.1.1.6 The TDE shall have the capability to query a Shipper that is in the shipping chain of the container, but has yet to have custody of the container, for the estimated drop-off time of the container based on current estimated pick-up time.

Using estimated pickup time, forecast weather, transportation time and handling time the Shipper shall return the estimated drop-off time.

R-2.1.1.1.7 When the Custodian Shipper has determined that an estimated delivery time has changed due to weather, mechanical failure, human error or other unanticipated events, the Custodian Shipper shall notify the TDE of a new estimated drop-off time.

The TDE shall use the new estimated drop-off time to notify the remaining Shippers in the container's shipping chain of the new estimated pick-up time and ask for a new estimated drop-off time.

R-2.1.1.1.8 A Shipper shall notify the TDE of delivery at its final destination or the transfer of custody to the next Shipper in the shipping chain.

This requirement releases a Shipper from custodianship of the container if the container is being delivered to its destination or as soon as custody is accepted by the next Shipper.

The actual delivery time is included in the message.

This message to the TDE must occur before the next Custodian Shipper can be assigned to the Container Node.

R-2.1.1.1.9 A Cargo Vendor/Recipient shall have the capability to query the TDE for the location of a container.

The TDE queries the Custodian Shipper for the location of the Container Node. The location resolution is not required to be finer than the RF coverage area of the Access Point the Container Node is within. If a finer resolution location is available (Container Node GPS, location determination using RF signal strength and direction, container stack Coupled Magnetic Field location, etc.) then the finer resolution location is used.

The location response shall contain at least the following location information:

- Latitude and Longitude of last location update
- Time stamp of last location update
- Confidence in the location:
  - Good
  - Estimated
  - Location Unknown – Location Unknown generally means that that communication with the Container Node been lost.

R-2.1.1.1.10 A Shipment Client may query the TDE for cargo sensor values. This message may be encrypted.

See the TDE-Shipper Cargo Sensor query requirement for more in formation.

R-2.1.1.1.11 The TDE may query a Shipper for the location of a container. This message may be encrypted.

See the Client-TDE Location Query requirement for the shipment client view of this request.

If the Container Node is equipped with GPS the Container Node GPS position is reported, otherwise the Shipper may report the position of the Access Point communicating with the Container Node.

A rail Shipper may use a more involved method of estimating location. If the rail Shipper knows the rail car position of the container in a train, the Container Node location may be estimated based on the Access Point GPS position and the rail car position in the train.

In a sorting yard, the location of each container is known by yard row and section, allowing latitude and longitude coordinates to be calculated without the need for GPS, although the GPS position of the Access Point communicating with the container should be used to provide a validity bound for the calculated container location.

R-2.1.1.1.12 The TDE may query a Shipper for cargo sensor values. This message may be encrypted.

Cargo within a container may have its own sensors that can be queried by the Container Node. This requirement allows the CTSN to be used by a client to query the cargo sensors.

The cargo sensor query and the values returned by the cargo sensors may be confidential. To provide confidentiality the query and response messages may be encrypted.

The cargo sensors must comply with the wireless sensor specification that results from another requirement in this document concerning communication between cargo sensors and the Container Node.

R-2.1.1.1.13 A Shipper shall notify the TDE of any Container Node generated Alarm messages.

The TDE logs all Alarm messages from the Container Node and notifies the Shipment Client.

The method of client notification is not specified in this document.

R-2.1.1.1.14 The TDE may query the current Container Node’s custodian shipper for the Container Node’s event Log.

When there is an Alarm message from the Container Node, reviewing any preceding Warning or Info events may help resolve the cause of the Alarm.

Warnings and Info events are usually of no value at the TDE level so they are not reported to the TDE unless requested by the TDE.

R-2.1.1.1.15 The TDE may command the Custodian Shipper of a Container Node to clear the Node’s event log.

This requirement is intended to be used at the end of a shipment when the log is no longer needed or at the beginning of the shipment if the log had not been previously cleared.

Only the TDE may request that a Container Node log be cleared. It is undesirable for a Shipper to be allowed to clear a log since the Shipper may try to avoid responsibility for cargo theft or damage that occurred while it was custodian by clearing the Container Node log.

2.1.2 Shipper Intra Network Requirements

There are few requirements for network messaging within a Shipper's Network. The Shipper is free to use any networking medium within the NOC and between the NOC and its Access Points that meet the following requirements.

R-2.1.2.1.1 Messages between TDE and a Container Node shall pass between the Custodian Shipper's NOC and Access Points without modification.

The message between the TDE and Container Nodes may be encapsulated in the data portion of a Shipper's network message.

Shipper encryption of the messages for transfer between the NOC and Access Points with subsequent decryption of the Shipper's own encryption shall not be considered modification of the message.

R-2.1.2.1.2 The time from receipt of a TDE message at a Shipper's external network portal to the receipt of the message at the Container Node shall not exceed X seconds.

A study must be conducted to determine a number for X. X will be less than the time for determining that a Container Node is missing.

In the event that the Container Node a message is destined for is missing, the NOC shall report the Container Node as missing.

In the event that an expected communication loss with the Container Node is occurring, the NOC shall report to the TDE the expected time that communication with the Container Node shall resume. Expected loss of communication may occur in remote areas where land mobile communication is used between the Access Point and the NOC but the Access Point is outside the range of the nearest communication tower.

2.1.3 Container Network Requirements

This section contains requirements pertaining to the operation and networking of communications between a Shipper's Access Point and Container Nodes. The Container Network is a wireless network of Access Points, Wireless Message Routers and Container Nodes.

These requirements consider 3 types of Container Networks.

1) Sorting Yard – The Sorting Yards are large areas to temporarily hold and sort containers when the containers are to change Shippers or change shipping conveyance. An example of a Sorting Yard is a sea side dock where containers are moved to/from ships from/to trains or trucks. As a point of reference, Sorting yards may have more than 10 thousands containers in the yard at one time.
2) Train – Containers are transported on rail using container well cars. It is not unusual for these trains to be up to 300 cars long with up to 3 containers per car.

3) Truck – Containers are transported in single units by truck over roadways.

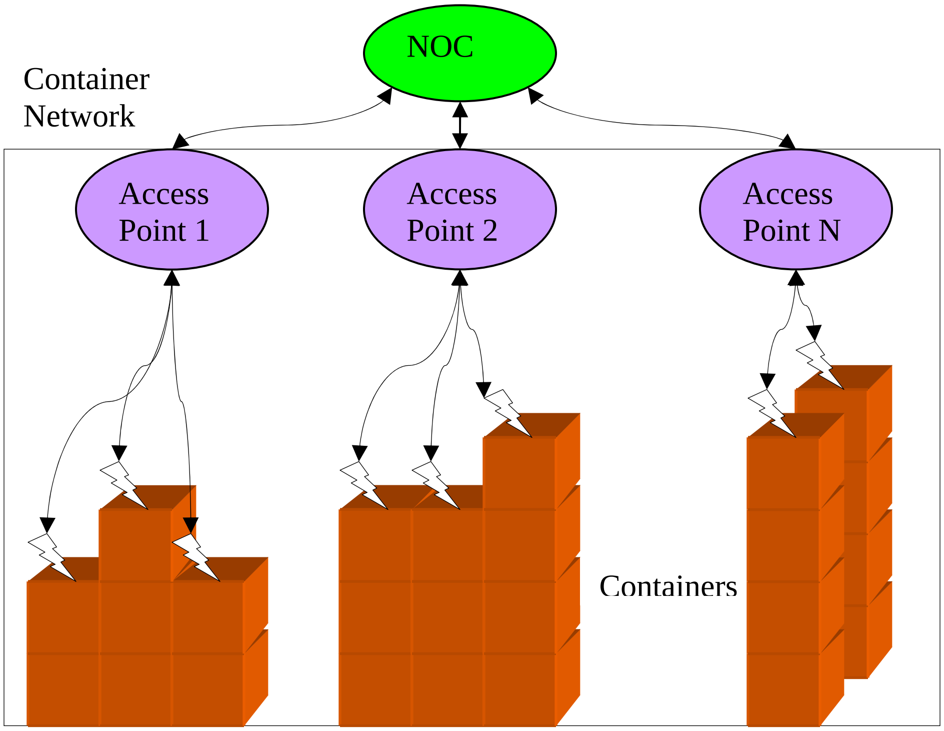

Figure 2 Sorting Yard Container Network

The diagram in Figure 2 illustrates a portion of a Container Network for a Sorting Yard. The Shipper's NOC has a connection to each Access Point in the Sorting Yard. The NOC-AP connection may be wireless or wired. This document does not specify the physical medium for the NOC-AP link. Access Points are spread through out the yard to provide RF coverage for all container locations. Access Points communicate with Container Nodes through either a RF link or a Coupled Magnetic Field.

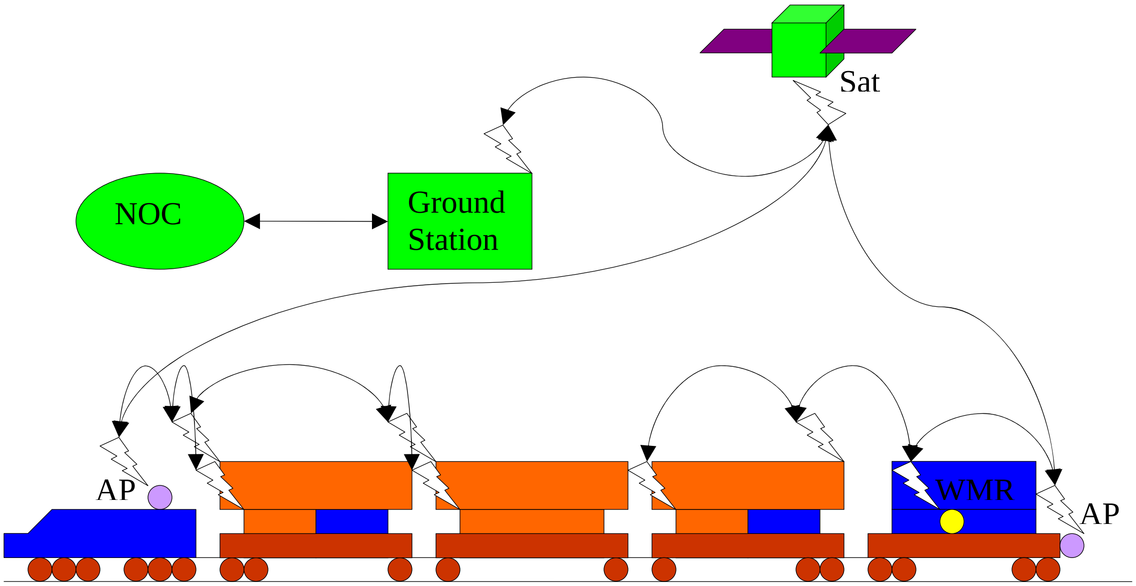

Figure 3 Train Container Network

The diagram in Figure 3 shows a schematic of a Container Network on a train. The train has two Access Points (APs). One Access Point is at the front of the train with the engine. The second is at the end of the train with the End-of-Train device. Container Nodes in the first half of the train form a wireless network with the Access Point in the engine. Container Nodes in the last half of the train form a wireless network with the trailing Access Point. Wireless Message Relays (WMR) may be used to relay messages between CTSN containers and between containers and Access Points. The WMR is particularly useful when non CTSN containers are in the train making the span between CTSN containers too great to complete a wireless connection. Since WMRs are required to have more power available than Container Nodes, they relieve the Container Nodes of the communications power consumption that would otherwise be required to relay messages to Containers Nodes out of Access Point range.

The train's APs must use a wireless communications link to the NOC. The communications link may be any number of available services including: Satellite (Iridium), Cellular (GSM, EV-DO) and Private Land Mobile (Radio).

Figure 3 illustrates one method of connecting the Shipper's NOC to the train's APs. A satellite forms a connection between a ground station and the train Access Points. The Shipper's NOC has a hard line connection to the ground station.

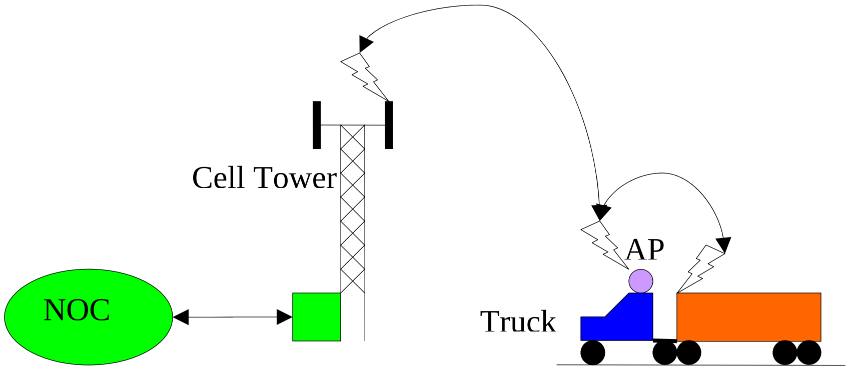

Figure 4 Truck Container Network

In Figure 4 a Truck Container Network is shown with a truck hauling a CTSN container. The Container Node communicates with the truck mounted Access Point. The Access Point uses a wireless link to the NOC, in this case through a Cellular connection.

2.1.3.1 General Container Network Requirements

R-2.1.3.1.1 RF Frequency use by the Container Network shall be centered at X MHz.

At this time there is no specific RF frequency requirement. The following will have to be done to have a feasible requirement:

- Determine the frequency range that is most conducive to container wireless communications in the Sorting Yard and Train configurations. Frequency selection would be based upon available spectrum and propagation simulations followed by empirical verification of the highly reflective RF environment created by stacks and lines of metal containers.
- Obtain international agreement on an unlicensed frequency range for container wireless network use.

Current unlicensed frequency ranges are not suitable for wireless container networks.

- The 435MHz ISM band is expected to be too narrow for the data rates that will be required for Container Nodes and Wireless Message Relays near the ends of trains since all of the messages from half of the containers must pass through the last relay or last few nodes nearest the Access Point in the corresponding portion of the train.
- The 2.4GHz band is heavily utilized by a range of 802.11, ZigBee, Bluetooth, and other devices which would pose interference and desensitization issues.
- The 915MHz ISM band is only available in North and South America. In addition, railroads use 915MHz readers at the trackside which can block other RF communications in the same band.
- 868MHz is only available in Europe.
- Use of unlicensed spectrum above 2.4GHz would potentially require additional power consumption by Container Nodes to offset propagation losses.

R-2.1.3.1.2 All wireless messages between CTSN containers and between a CTSN container and a CTSN Access Point shall have digitally signed messages.

This requirement is to provide high confidence that messages have not been altered during travel from the source to the destination. It also provides verification of the identity of the source of the message.

This requirement is critical for messages that are used to change the state or configuration of a Container Node. Only authorized sources (primarily the TDE) may change the configuration a Container Node.

2.1.3.2 Containers

R-2.1.3.2.1 Each CTSN container shall have an ID that uniquely identifies the container.

This ID is called the Container CTSN ID. In this document the term Container ID may also be used when there will be no confusion with any other type of container identification.

R-2.1.3.2.2 CTSN enabled containers shall be wireless networked with each other and/or with CTSN Access Points in the following shipping situations:

- Rail Transport
- Sorting yards (Railroad and Shipping)
- Over the Road Truck Transport.

We are leaving ships out of the requirements at this point since ships are reasonably secure while at sea. There is no reason that ships could not also adhere to the requirements for trains.

R-2.1.3.2.3 CTSN containers shall have two physical communications mediums.

- Coupled Magnetic Field
- RF

The various environments that intermodal containers are placed prompts the need for a hybrid communications mechanism.

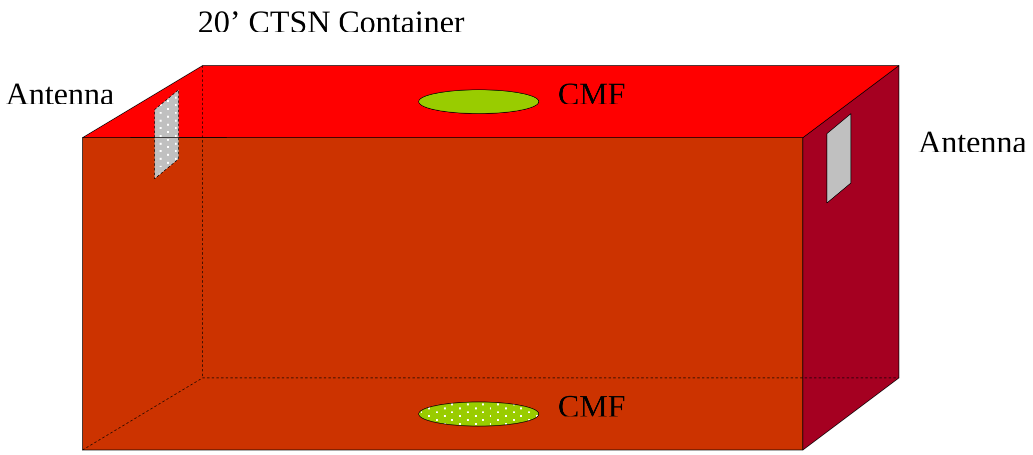

Figure 5 20' CTSN Container with RF Antennas and Couple Magnetic Field positions

When there is space around one of the Container Node’s RF antennas that is much greater than the communication frequency wavelength, using RF communications will be effective if the Container Node is within the range of an Access Point. RF communication will be used for truck transported Container Nodes and will typically be available for use on rail well cars.

When a container is tightly packed with other containers (as is the case in sorting yards) RF communication for those containers buried inside a stack may not be effective. In this case a Coupled Magnetic Field for communications between adjacent containers would be used. Messages would be relayed from a Container Node inside of a stack and to a container located where RF communication is possible.

R-2.1.3.2.4 Containers shall communicate with vertically adjacent CTSN containers by means of a Coupled Magnetic Field.

The same magnetic field coupler that serves to transfer power between containers is also used for adjacent container communications. At least one coupler is on top of the container and an additional coupler(s) is on the bottom of the container.

The couplers must be placed to align when containers are stacked.

A study must be conducted to determine the best location for the Coupled Magnetic Field coils. In particular the case of a 40 foot or longer container placed on two 20 foot containers on a rail well car must be considered.

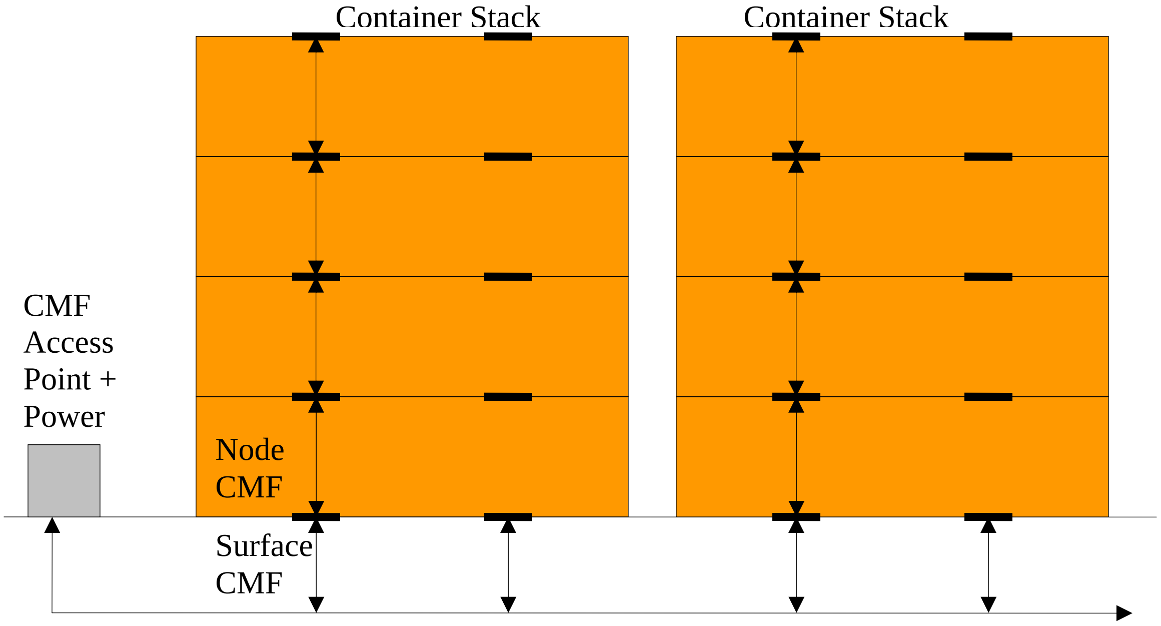

Figure 6 Sorting Yard Couple Magnetic Field Power and Communication with Nodes

R-2.1.3.2.5 Containers shall have a RF antenna mounted on each end of the container near the top of the container. The antenna and mount shall be designed such that damage to the antenna is unlikely under ‘normal’ container handling conditions.

An antenna mounted on the top, bottom or sides of the container would be blocked when buried in a container stack in a sorting yard making these locations unsuitable for antennas with just a few exceptions.

Since it is unlikely that all containers will be fitted with CTSN, it is assumed that there a probability of a mix of CTSN and non-CTSN containers in the same sorting yard stack. This means that some Containers Node’s in a stack could be prevented from using the Coupled Magnetic Field system to communicate, due to vertically adjacent non-CTSN containers. An isolated Container Node in a stack could potentially send and receive messages to other RF containers in the stack or an adjacent stack by way of a reflected RF signal using the antennas located at the ends of containers.

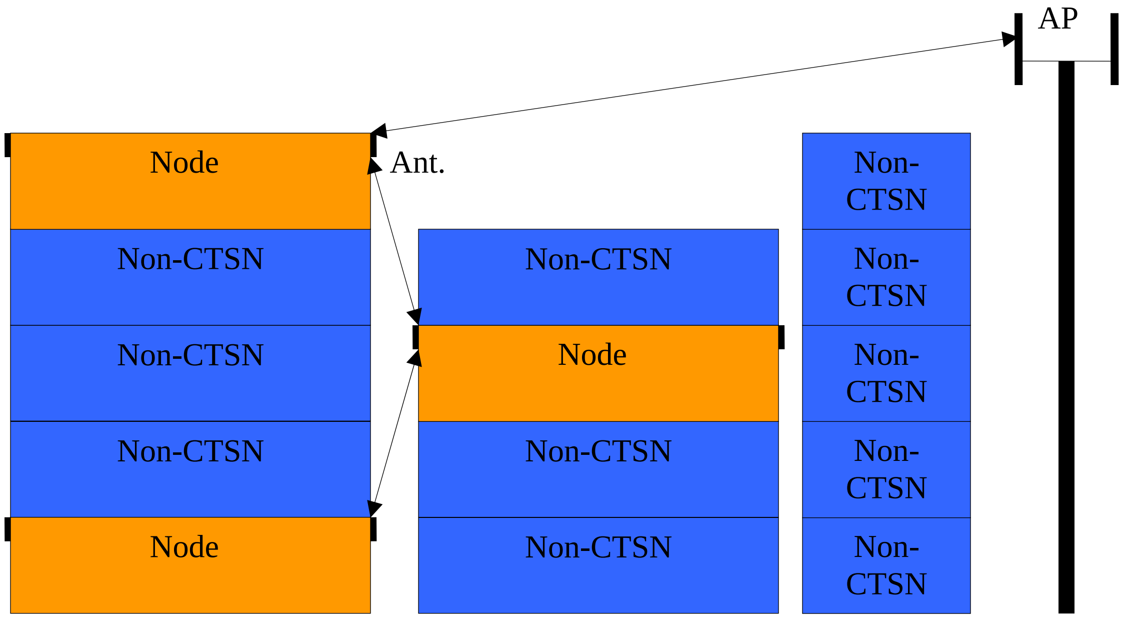

Figure 7 Container Stack with Nodes Relaying RF messages to Access Point

The only situations where antennas on the ends of containers are completely blocked are when two 20 foot containers are placed end-to-end in a rail well car. The antennas on the adjacent container ends are blocked but the antennas on the other ends of the Container Nodes are not blocked.

R-2.1.3.2.6 Container Nodes shall be network configurable to facilitate multi-hop messaging using other Container Nodes for intermediate hops.

This requirement is needed for utilizing the Coupled Magnetic Fields within a container stack, for using RF communications in a stack of sparsely populated CTSN capable containers and for train networking when there is a lack of Wireless Message Relays.

Examples of multi-hop message relaying are shown in Figure 3 and Figure 7.

R-2.1.3.2.7 Container Network topology shall be configured by a Shipper’s NOC via commands sent to Access Points, Wireless Message Relays and Container Nodes.

The Shipper NOC has knowledge of the container IDs and at least general container location. This knowledge allows the Shipper NOC to determine a network configuration faster and with less Container Node power usage than an ad-hoc network determined by the container nodes themselves.

2.1.3.3 Access Points

An Access Point is a bridge between the Container Node’s wireless link and the remainder of a Shipper’s network. It may bridge directly to a wired network or it may use another wireless technology (802.11, GSM and other high speed digital WAN [3G, 4G, etc], Satellite Data link) to communicate with a Shipper’s wired network.

R-2.1.3.3.1 All container transporting vehicles and vessels shall have at least one Access Point

- Truck – Shall have one Access Point. This access point will obtain power from the truck's electrical system.
- Train – Shall have two Access Points.
  - Shall have an Access Point located at the front of the train powered by the engine's power supply.
  - Shall have an Access Point located at the rear of the train. This requirement provides an available redundant path for Container Node data, reduces by half the amount of message traffic that must be relayed to the front Access Point when not used as a redundant data route, and can use a convenient power source in the End of Train device. The End of Train uses the compressed air from the train braking system to spin an air turbine electric generator.

R-2.1.3.3.2 Sorting Yards shall have Access Points placed in a physical topology to allow any potential CTSN container position within the yard to be within direct line range of at least one Access Point.

Direct line range assumes that no other containers are blocking the RF path between the container and the AP. In practice, many Container Nodes will not have a clear Line of Sight (LOS) path to an Access Point due to the configuration of stacked containers in a yard. This requirement is intended to set a maximum distance between CTSN Container Nodes and the nearest Access Point.

Light poles in sorting yards are potentially ideal locations to place Access Points. The light fixtures are already supplied with power and are positioned above the highest container stacks. The layout of the light poles to provide task and security lighting of the yard also is conducive to good RF coverage of the container sorting yard.

With RF antennas placed at each end of the container near the top edge as given in a Container Node requirement, the highest container in a stack will typically have a clear LOS path to at least one light pole mounted AP.

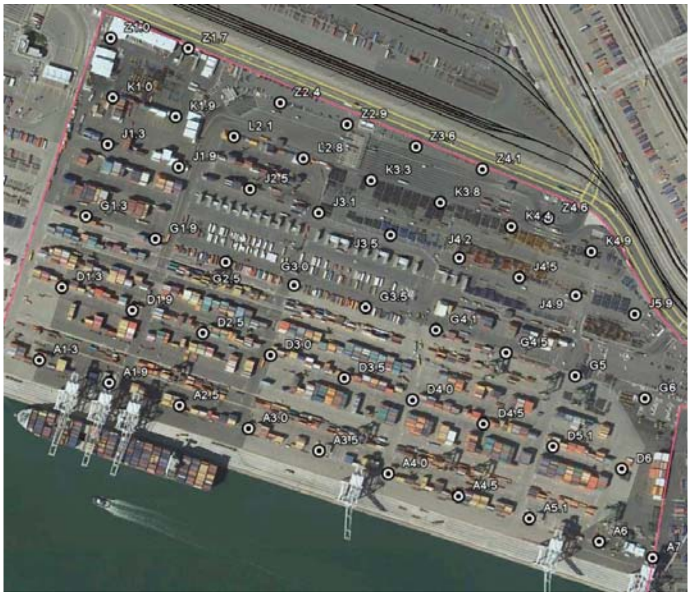

Figure 8 Oakland International Container Terminal light pole locations

As shown in Figure 8, many sorting yards have a matrix of light poles that cover the sorting yard. This light pole pattern is common in North America and Europe. For the Oakland International Container Terminal, the light poles are in a nearly square grid pattern with approximately 120 meters between adjacent light poles. This light pole pattern is ideal for Access Point RF coverage of the containers.

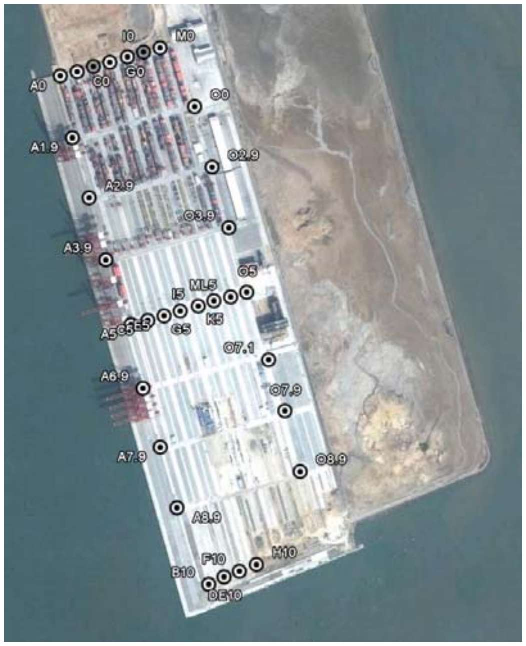

Figure 9 Da Chan Bay Terminal rectangle boundary light pole pattern

A light pole pattern that is common in Asia is shown in Figure 9. For these sorting yards the light poles are concentrated at the ends of aisles on the periphery of the yard. With this light pole pattern containers in the interior of the yard are farther from the Access

Points and more difficult to reach through an RF connection. For these yards more Access Point locations may be required or the use of Wireless Message Relays may be needed.

R-2.1.3.3.3 Access Points shall have the same Tamper Reporting requirements as Container Nodes.

Since criminals may try to block Container Node Alarm messages by disabling an Access Point, Access Points must Alarm if tampering is detected.

R-2.1.3.3.4 Access Points using On-Demand communications with its Shipper NOC shall have the responsibility of detecting missing Container Node Status Reports. A missing Status Report shall result in an immediate Alarm to the NOC.

Some Access Points will not have continuous connectivity with their NOCs. An example is using Satellite Dialup communication only when there is a message to send. Using On-Demand communications can reduce communication costs in some instances.

Access Points expect a Status Report from each Container Node assigned to its portion of the network every X seconds where each node has its own X value depending on Security Mode and remaining stored power.

If an Access Point fails to detect a Status Report from a node within X seconds of its last Status Report, the Access Point shall establish communication with its NOC and send an Alarm message to the NOC containing the following:

- Last Status Report of the missing container Node.
- Time of Missing determination.

R-2.1.3.3.5 Access Points shall report missing Wireless Message Relays with the same requirements of reporting missing Container Nodes.

The Access Point knows the topology of the Container Nodes and Wireless Message Relays. It will not expect Status Reports from Container Nodes that are linked to a missing Wireless Message Relay.

R-2.1.3.3.6 Mobile Access Points shall have GPS. Mobile Access Points shall report their GPS position when queried by their NOC.

Since not all Container Nodes shall have GPS and GPS is not usable for containers buried within a sorting yard stack, the next best container location mechanism is for the Access Point that Container Node is using to provide GPS data. The Access Point GPS gives a general location for the Container Nodes in its network if no other location mechanism is available.

2.1.3.4 Wireless Message Relays

Wireless Message Relays are primarily needed in the train transport scenario. In a mixed CTSN environment on a train (where there are numerous containers that are not CTSN capable) there may be many car lengths between CTSN compliant containers thus making message Container Node hopping improbable. Wireless Message Relays are either temporarily placed on rail cars in the CTSN gap or the Wireless Message Relays are a permanent component of rail well cars to relay CTSN messages.

Temporary Wireless Message Relays may also be beneficial in sorting yards where Access Point coverage may be insufficient.

Wireless Message Relays may be implemented as specialized Container Node hardware since the Wireless Message Relays Requirements are largely a subset of the Container Node requirements.

R-2.1.3.4.1 Wireless Message Relays, when available, shall be configured by the Shipper's NOC to relay messages between Container Nodes, other Wireless Message Relays and Access Points.

The purpose of the relay is to extend the message routing range between Container Nodes and Access Points. It does this by repeating and routing messages.

R-2.1.3.4.2 Wireless Message Relays shall have the same Tamper reporting requirements as Container Nodes and Access Points.

Disabling or tampering with a WMR is a potential method of preventing a Container Node intrusion Alarm. Some attempts to disable a Wireless Message Relay can be detected before the Relay is successfully disabled. Attempts to disable the Relay are immediately reported as a Tamper Alarm.

R-2.1.3.4.3 Wireless Message Relays are required to have an external power source. The external power source may be intermittent.

This requirement is to accommodate Wireless Message Relays on railroad container well cars where the WMR is powered by a well car wheel or axle mounted generator. The WMR may also be powered by solar power or some other intermittent power source that is not an energy storage device.

R-2.1.3.4.4 Wireless Message Relays with an intermittent external power source shall have an energy storage device for backup power source.

In order to continuously power a Wireless Message Relay a backup power source that has energy storage is needed. This is generally a battery. The capacity of the energy storage must be sufficient to keep the WMR powered for 99.XXXX percent of anticipated intervals of no power from the intermittent power source. The XXXX value must be determined by a study.

R-2.1.3.4.5 The Wireless Message Relay must charge the backup power source from the intermittent external power source when excess power is available.

With this requirement it is possible that a WMR will not require any battery maintenance for many years until the battery materials fail. There is no need for the frequent battery replacements that are required for non-rechargeable batteries used in many current wireless sensing applications.

R-2.1.3.4.6 A Wireless Message Relay has the same Status Reporting requirements as a Container Node.

Wireless Message Relays may incur the same failures and tampering as Container Nodes therefore a Shipper must know when they are missing due to a failure to receive a Status Report when one is expected.

2.2 Container Requirements

This section contains requirements for CTSN compliant containers.

2.2.1 General Container Requirements

R-2.2.1.1.1 CTSN containers may be manufactured with integrated CTSN hardware or may be retrofitted.

Retrofitting containers poses issues with routing and protecting wires within the container for power and communications that are not resolved within these requirements.

R-2.2.1.1.2 A CTSN compliant container shall be fitted with the following:

- Sensor Node
- RF Antennas
- Magnetic field Communication and Power Coupler (MCPC).
- Intrusion Sensors
- Optional additional sensors.

R-2.2.1.1.3 A Container Node shall consists of:

- Microcontroller
- Internal backup power
- Power converter for optional external power
- RF Modulator/Demodulator – The modulator/demodulator may be integrated with the antennas instead of the Container Node.
- Magnetic field Coupling Modulator/Demodulator – The modulator/demodulator may be integrated with the CMF coil.
- Passive Sensor monitoring
    - A minimum of enough open/close lines for each container door.
- Optional Sensor Wire Bus for Active sensors – A study is required to determine a suitable low power communication bus for active sensors.
- Optional Sensor Wireless connectivity for cargo/pallet mounted sensors. The requirements of cargo/pallet sensor communications with the Sensor Node are not covered within these requirements.

2.2.2 Container Node Operation Requirements

This section contains requirements related to CTSN Container Node behavior.

R-2.2.2.1.1 The Container Node shall utilize the following categories of sensor and Node events.

- Intrusion – Intrusion can be any of the following but is not limited to these events:
  - Container door opening
  - Unexpected natural or artificial light in container
  - Detection of movement within container
  - Carbon dioxide above normal levels within container (possible human presence).
- Tampering – Tampering can be any of the following but is not limited to these events:
  - Light within the Node's Electronic enclosure.
  - Light within any active sensor's enclosure
  - An increase in the VSWR of the RF transmissions
  - Unexpected power supply voltage fluctuations
  - Unexpected change in sensor electrical current draw
- Electronics Health – An Electronics Health event can be any of the following but is not limited to these events.
  - Backup power supply is near depletion.
  - Failure of active sensor to respond to message from Node
- Safety
  - Sensors indicate smoke, fire or excessive high temperature
  - Sensors indicate chemical leak
- Sensor/Node State
  - Low voltage from external power
  - Switching to internal power
  - Switching to external power (include type of power: solar, kinetic, thermal)

The category of the event is used to determine which personnel to notify.

R-2.2.2.1.2 The Container Node shall utilize the following Attention Level for reporting events:

- **Alarm** – The container node sensor event must be investigated immediately. Notification of responsible personnel must be by the most immediate means.
- **Warning –** The event may indicate a current or future problem and should be investigated but it is not an emergency.
- **Information** – The event is noteworthy and should be reported to the appropriate personnel by non intrusive means. The event by itself does not indicate a problem to investigate.

Each event message to the Container Node's current Shipper Custodian's NOC shall contain an indicator of the severity of the event. The NOC uses the severity of the event to determine what method to use to alert the appropriate Shipper's or emergency response personnel of the event.

R-2.2.2.1.3 Individual CTSN containers shall have the following security modes:

- **Secure –** The Secure Security Mode is used when the container is loaded with cargo and has been sealed.
    - In the Secure Security Mode the following categories of events are Alarm Attention Level:
        - Intrusion
        - Tampering
        - Safety
        - Electronics Heath – Readings of problems with electronics heath could be due to tampering.
- **Unsecure –** The Unsecure Security Mode is utilized when the container is being loaded, unloaded or the cargo is being inspected.
    - The following event categories are expected in the Unsecure Security Mode and are reported as Information Attention Level instead of Alarm or Warning Attention Level:
        - Intrusion
    - The following event categories are reported as Alarm Attention Level:
        - Tampering – No tampering of the container or electronics is allowed
        - Safety – During loading, unloading, or inspection the cargo may be damaged leading to a dangerous heath issue that may not be noticed by the personnel involved.
        - Electronics Health
    - All other Event Categories are Information Attention Level.
- **Inactive –** The Inactive Security Mode is used when the container has no cargo.
    - In this Security Mode the following events are Alarm Attention Level:
        - Tampering
    - In this mode the following events are Warning Attention Level
        - Electronics Health
    - All other Event Categories are Information Attention Level.
- **Maintenance –** In this security mode it is expected that the electronics are undergoing maintenance. No events are reported.

R-2.2.2.1.4 A Container Node shall send a Status Report to its current Shipper Custodian every X seconds.

The purpose of the periodic Status Report is to allow the container's current Shipper Custodian to determine that there may be a security or maintenance problem with a CTSN container if there is a missing Status Report. A Status Report is missing if the Access Point or NOC does not receive a Status Report from a Container Node within a window Y seconds long centered X seconds from the last received Status Report from the Container Node.

A study must be performed to determine a value for X and Y that keeps battery power usage low but has high enough frequency to allow the Shipper Custodian to determine that a node is missing with sufficient time to raise an alarm and get responders to the last known node location so that cargo loss may be minimized.

The value of X may change based on the node's current Security Mode. A Secure Security Mode would require more frequent Status Reports than Inactive Security Mode.

The status report contains the following:

- Current Security Mode
- Power status (remaining hours of stored power)
- Last Alarm event.
- GPS location if available.

R-2.2.2.1.5 All Container Node events are stored into the Node's non-volatile memory with an event timestamp and all information associated with the event. In the case that the non-volatile memory has been filled, new Information and Warning Attention level messages shall be dropped. The last 10 Alarm Attention level messages shall always be kept in non-volatile memory.

This requirement is intended to prevent an intruder from causing Information or Warning category events to fill up the log memory and then break into the container without the Alarm event being logged due to the full log memory. Information or Warning events that would fill the log memory might be caused by pounding on the side of a container that has an acoustic sensor but the processed sound does not indicate an Alarm to the sensor, just a Warning or Information event.

When all but the last 10 entries in a log memory are full all Warning and Info category events are no longer logged but are still reported to the NOC.

R-2.2.2.1.6 A container's CTSN Node shall retain in non-volatile memory the Shipper ID of the Shipper that has CTSN custody of the container. This shall be named the Custody ID.

R-2.2.2.1.7 The Custody ID in the container Node may only be changed by the TDE through the Custodian Shipper's NOC and Container Node network.

This is used to change the Custody ID of a Node to the next shipper to take custody of container when the container changes Shippers.

The authenticity of the message is verified by the digital signature in the message.

R-2.2.2.1.8 A Container Node's Security Mode shall only be changed by the TDE through the Custodian Shipper's NOC and Container Node network.

The authenticity of the message is verified by the digital signature in the message.

R-2.2.2.1.9 An authorized Customs Agent may request that the TDE change a Container Node's Security Mode from Secure to Unsecure or Unsecure to Secure.

The request shall be made to the TDE over the Custom Agency's network to the TDE. See Figure 1.

This requirement is needed for customs officials to inspect containers without causing an Intrusion Alarm.

R-2.2.2.1.10 Node Alarm, Warning and Information event messages shall be reported immediately by the Container Node to the Custodian Shipper's CTSN NOC via the Container Node wireless network.

If the container is not in a container node wireless network when the event occurs, the event message becomes an unreported event message within the node. As soon as the container joins a container node wireless network the node reports all unreported event messages. All Alarm event messages are reported first.

R-2.2.2.1.11 The Container Node shall clear its non-volatile event log upon a Clear Log message from the TDE.

The Container Node shall validate the Clear Log message from the TDE, via the current Custodian Shipper's network, using the TDE's digital signature for the message.

2.2.3 Container Sensor Requirements

This section contains requirements concerning the sensors that are for monitoring container security, integrity, safety and node health. Cargo specific sensors are not covered in this section. Note that security sensing is required while other sensing is optional.

R-2.2.3.1.1 A CTSN Container Node shall detect the occurrence and duration of a container intrusion event.

Container intrusion may be detected using one or more of the following methods:

- **Door open sensor** to detect when a door of the container has been opened. Potential door open sensors are:
  - Mechanical switch
  - Magnetic switch
  - Proximity switch
  - Photo-beam
- **Photo-diode** or similar light sensing device capable of detecting that a door has been opened or an opening has been cut into the container resulting in sun light or exterior artificial light illuminating the interior of the container.
- **Motion sensor** to detect movement in the container where there should be no movement.
- **Carbon dioxide sensor** to detect the presence of persons or animals in the container.

R-2.2.3.1.2 A CTSN container node *may* monitor sensors to detect safety issues.

Sensors to detect safety issues include but are not limited to the following:

- Smoke detection sensor
- Heat sensor
- Chemical detection sensor
- Radiation detection sensor

R-2.2.3.1.3 CTSN container *may* monitor any of the following:

- Environmental parameters inside container
  - Temperature
  - Humidity
  - Acceleration, G-force
- GPS.
- Cargo mounted wireless sensors
  - A study is required to determine a good physical layer and protocol for communicating with Cargo Sensors. One candidate would be Dash-7.

R-2.2.3.1.4 CTSN Container's sensors shall operate at temperatures between -20C and +70C.

Containers are shipped to cold climates such as Alaska, United States and hot climates such as Dubai, UAE.

2.2.4 Container Power Requirements

Power management is one of the most important aspects of any mobile sensing device that also uses RF communication. This section covers power requirements of Container Nodes.

R-2.2.4.1.1 Containers *may* obtain power from self generated means including but not limited to:

- Solar cells
- Kinetic motion

R-2.2.4.1.2 Vehicles and vessels transporting containers and sorting yards *may* provide power to the top or bottom container in a stack via the Coupled Magnetic Field power device.

An example would be a railroad container well car using a permanent magnet on a car wheel or axle with a pickup coil that generates power that is then delivered, via power cable, to a coupled magnetic field power delivery pad on the bottom of the well car directly under the bottom container's Coupled Magnetic Field power coupler.

R-2.2.4.1.3 Vertically stacked containers shall transfer excess Node power from a container being supplied power (either external or self generated) to other containers in a stack by means of a Coupled Magnetic Field between any two vertically adjacent CTSN containers.

The most likely self generated power source for containers would be solar power. Solar power will not work for containers buried in a stack of containers in a sorting yard but a container at the top of a stack can utilize solar power. This requirement allows a container with a self generated power source to share excess power with other vertically adjacent containers that can not utilize self generated power.

A container with self generated solar power on the top of a stack could provide power to all other CTSN containers in the stack through the Coupled Magnetic Field devices on the containers provided there are no non-CTSN containers in the stack.

In a sorting yard it is possible to place Coupled Magnetic Field devices in the pavement surface at the location for each container stack to provide external power from the bottom of a stack. The pavement placed Coupled Magnetic Field devices are powered from the sorting yard infrastructure. See Figure 6.

The bottom container in a rail well car may be powered from an axle or wheel mounted generator through a Coupled Magnetic Field device in the bottom of the well car. The bottom container could power the top container through another Coupled Magnetic Field device.

R-2.2.4.1.4 CTSN container Coupled Magnetic Field power couplers shall be placed in a location on the container and housed to prevent damage to the power coupler under normal handling of the container.

It would be best if the couplers were flush with the top/bottom of the container and able to sustain a direct impact with the same resilience as the remainder of the top/bottom of the container.

R-2.2.4.1.5 CTSN container Coupled Magnetic Field power couplers shall be placed in a location on the containers to allow power transfer between a 40 foot and longer container placed on top of two 20’ containers in the rail transport container stack configuration.

External power applied to one 20 foot container shall pass up to the 40 foot container and then down to the other 20 foot container unless both 20 foot containers are directly powered by the rail well car.

A likely location for CMF couples is at both ends on top and bottom for a total of four couplers. This configuration allows a long container to be stacked on two 20 foot containers and have at least 1 coupler pair line up for each container.

R-2.2.4.1.6 CTSN container Coupled Magnetic Field power couplers shall be placed in a standard location on containers. The location shall allow 40 foot and larger containers to be stacked in either end-for-end orientation.

The likely configuration for this requirement is to place couplers at a prescribed distance X that is less than 20 foot from the center of the container.

On 20 foot containers the CMF couples would be placed 20' – X from the end of the container.

A possible value for X is 10'. This would place one CMF in the middle of the top and bottom of the 20' containers. The 40' and longer containers would have 4 CMF, two on top and two on bottom 10' from the center line of the container.

R-2.2.4.1.7 Containers shall provide Node power from rechargeable electrical energy storage when external or self generated power is not available or is insufficient.

Container electrical energy storage capacity must be sufficient to power communications with adjacent containers or CTSN Wireless Access Point for 99.9XXX% of the statistical durations that external or self generated power is not available.

A study is needed to determine a reasonable value for XXX.

R-2.2.4.1.8 CTSN container power system shall operate at temperatures between -20C and +70C.

CTSN must be able to operate in extreme cold conditions seen in locations such as Alaska and hot locations such as United Arab Emirates.

R-2.2.4.1.9 When a CTSN container is obtaining external or self generated power, excess power shall be transferred to vertically adjacent CTSN containers through the Coupled Magnetic Field power coupler. Stored electrical power is never transferred to another container.

A container with external or self generated power may be able to power a whole stack of containers.

Stored electrical power is never used to power adjacent containers. This prevents tampering by draining the electrical power of a Container Node through external demand.

R-2.2.4.1.10 All cargo mounted sensors shall provide their own power.

The practical constraints of designing a Container Node capable of supplying power to cargo mounted sensors drive this requirement. However, using magnetic coupled power transfer similar to the method used to transfer power between vertically stacked containers should be considered for powering cargo mounted sensors.

R-2.2.4.1.11 When a container is using stored electrical power for the Node, communication with cargo mounted sensors is limited to reduce the stored power drain.

This requirement will need a solid X kBytes/hour limit once the physical medium, protocol and data rate have been determined for container node–cargo sensor communication.

3 Recommendations

Refrigerated containers should be the first type of containers to have CTSN installed

- These containers are continuously powered for refrigeration (except for brief periods) so power is available for the Container Node.
- These containers are used to transport perishable goods, with the client and Custodian Shipper having a vested interest in immediate notification of elevated temperatures or failure of the refrigeration system.

Another early adoption candidate for CTSN would be containers carrying goods of very high value (example: PC CPU or GPU chips).

During early adoption a small portion of a sorting yard may be retrofitted with the Access Points where CTSN containers are sorted.

During early adoption a small portion of the yard surface may be retrofitted with the Magnetic Coupled Power and Communication pads in appropriated locations within the indicated container placement grid where CTSN containers are sorted.