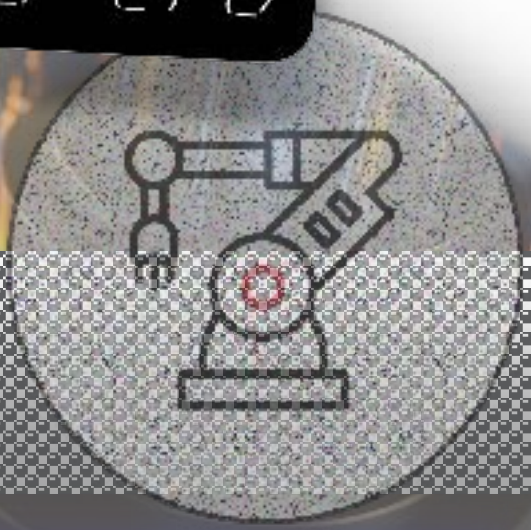


LoRa / LoRaWAN Village

THOTCON October 8th and 9th 2021

Exploring Long Range/Low Power Technology and Contexts of Info-Secure Supply Chain

Mummpy Do

October 2021

Experience And History

Listing of prior related presentations and related experience

- **Logistics Engineering Context**
  - *2014 Systems Engineering and Architecture: October 1, 2014 “Logistics Systems Engineering and Additive Manufacturing” - Burlington MA*
  - *2014 Cyber Security Awareness 2014: October 28, 2014 “Social Engineering Sure, Trust Me” - Burlington MA*
  - *2015 Raytheon Cyber Workshop: May 19-21 2015 “Secure Cyber-Manufacturing” - McKinney TX*
  - *2016 RAMS Workshop: January 29, 2016 “Logistics System Engineering and Additive Manufacturing” - Tucson, AZ*
- **Information Security Solutions & Integrations Context**
  - *2018 NDIA 21st Annual Systems Engineering Conference: October 24th 2018 “Considering Cyber-Resilience and Sustainment Supply Chain with a Blockchain (Shared Ledger) Paradigm - Tampa, FL*
- **Secure Systems Engineering Context**
  - *2019 focus on Software Assurance & Risk Management Framework - Woburn, MA*
  - *2020/2021 focus on Internal Research and Development (IRAD) - Portsmouth, RI*

Value Proposition

What is the value of a project exploring how "Long Range Wide Area Network" protocols are related to a Cyber Secure Supply Chain?

- Risk Management Framework
- Cyber Supply Chain Risk Management Architecture
- Zero Trust Architecture

Risk Management Framework

The NIST Risk Management Framework (RMF) provides a comprehensive, flexible, repeatable, and measurable 7-step process that any organization can use to manage information security and privacy risk for organizations and systems and links to a suite of NIST standards and guidelines to support implementation of risk management programs to meet the requirements of the Federal Information Security Modernization Act (FISMA).

Prepare	Essential activities to **prepare** the organization to manage security and privacy risks
Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis
Select	**Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
Implement	**Implement** the controls and document how controls are deployed
Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to **authorize** the system (to operate)
Monitor	Continuously **monitor** control implementation and risks to the system

https://csrc.nist.gov/Projects/Risk-Management

Risks Management Framework (RMF) is adaptable and tailoring is encouraged

SP 800-53 Controls: Supply Chain

SUPPLY CHAIN RISK MANAGEMENT Family (SR-1 through SR-6)

No.	Control Name	Low-Impact	Moderate-Impact	High-Impact	Privacy Control Baseline
SR-1	POLICY AND PROCEDURES	SR-1	SR-1	SR-1	
SR-2	SUPPLY CHAIN RISK MANAGEMENT PLAN	SR-2 (1)	SR-2 (1)	SR-2 (1)	
SR-3	SUPPLY CHAIN CONTROLS AND PROCESSES	SR-3	SR-3	SR-3	
SR-4	PROVENANCE				
SR-5	ACQUISITION STRATEGIES, TOOLS, AND METHODS	SR-5	SR-5	SR-5	
SR-6	SUPPLIER ASSESSMENTS AND REVIEWS		SR-6	SR-6	

Supply Chain Control Family (SR-1 through SR-6)

SP 800-53 Controls: Supply Chain

SUPPLY CHAIN RISK MANAGEMENT Family (SR-7 through SR-12)

No.	Control Name	Low-Impact	Moderate-Impact	High-Impact	Privacy Control Baseline
SR-7	SUPPLY CHAIN OPERATIONS SECURITY				
SR-8	NOTIFICATION AGREEMENTS	SR-8	SR-8	SR-8	
SR-9	TAMPER RESISTANCE AND DETECTION			SR-9 (1)	
SR-10	INSPECTION OF SYSTEMS OR COMPONENTS	SR-10	SR-10	SR-10	
SR-11	COMPONENT AUTHENTICITY	SR-11 (1) (2)	SR-11 (1) (2)	SR-11 (1) (2)	
SR-12	COMPONENT DISPOSAL	SR-12	SR-12	SR-12	

Supply Chain Control Family (SR-7 through SR-12)

Cyber Supply Chain Risk Management Architecture

https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management

Low Power/Long Range is architected to support low bandwidth connectivity within a wide area connected ecosystem

Numerous publications and guidance – The SECURE Technology Act and FASC Interim Final Rule gave NIST specific authority to develop C-SCRM guidelines

"The NIST Cyber Supply Chain Risk Management (C-SCRM) program helps organizations to manage the increasing risk of cyber supply chain compromise, whether intentional or unintentional. The factors that allow for low-cost, interoperability, rapid innovation, a variety of product features, and other benefits also increase the risk of a compromise to the cyber supply chain, which may result in risks to the end user."

NIST has authored numerous guidance publications for C-SCRM with a most recent updated NIST SP 800-161

Zero Trust Architecture

Low Power/Long Range is architected to support the security paradigm shift described within Zero-Trust

August of 2020 National Institutes of Standards (NIST) published Zero Trust Architecture: SP 800-207. SP 800-207

https://www.nist.gov/publications/zero-trust-architecture

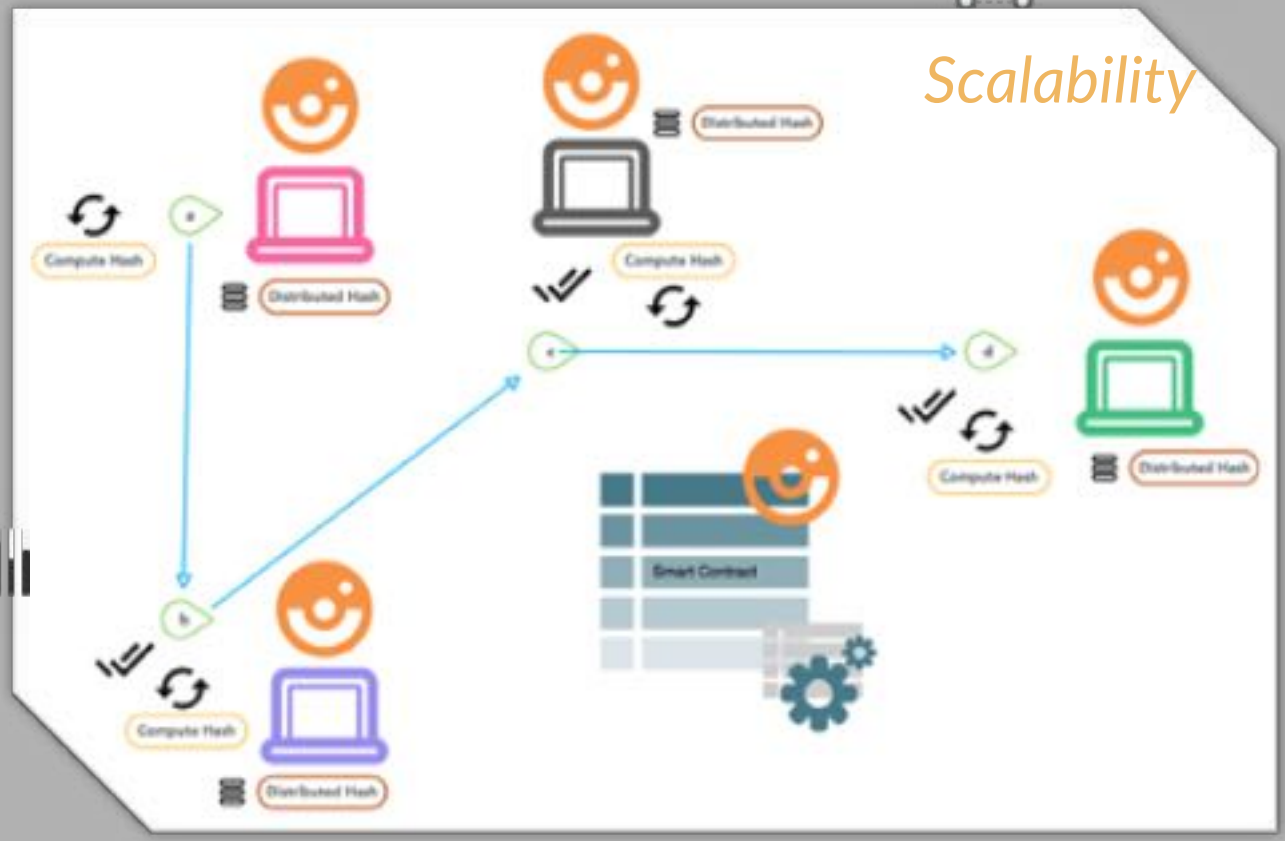
"Zero trust refers to an evolving set of security paradigms that narrows defenses from wide network perimeters to individual or small groups of resources. Its focus on protecting resources rather than network segments is a response to enterprise tends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary"

Low Power/ Long Range is architected to support shifting paradigm of Zero-Trust environments

Cyber Secure Supply Chain

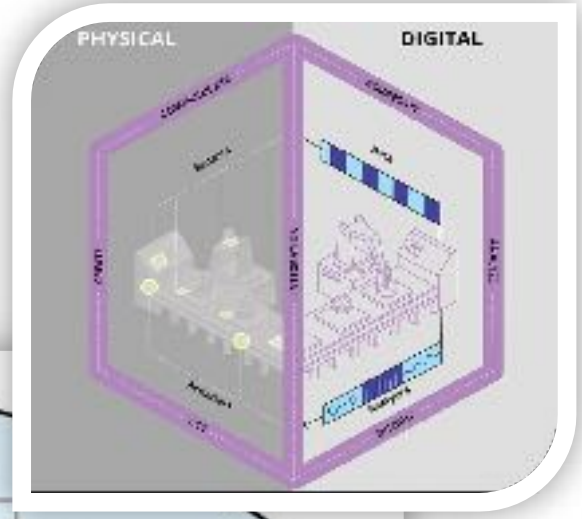
Supply Chain leverages technologies supporting ***digital trust***

Verified via ***cryptographic*** based hashing algorithms



Complex automated ecosystem tied together with Standards, Architectures, and Technologies

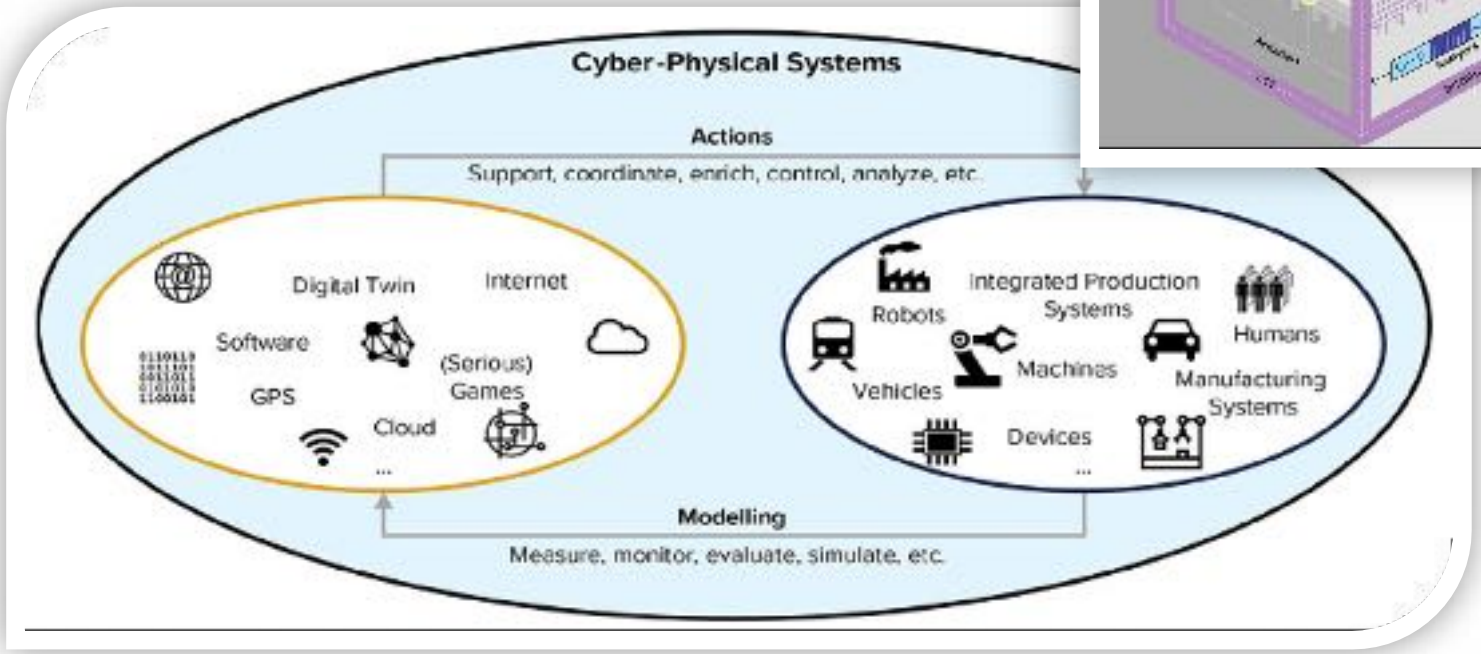
Digital Supply Networks



Core Principles:

- Connectivity
- Virtualization
- Data Utilization

Industry 4.0



Images Source: Digital Supply Networks: Transform Your Supply Chain and Gain Competitive Advantage with Disruptive Technology and Reimagined Processes by Amit Sinha, Ednilson Bernardes, et al.

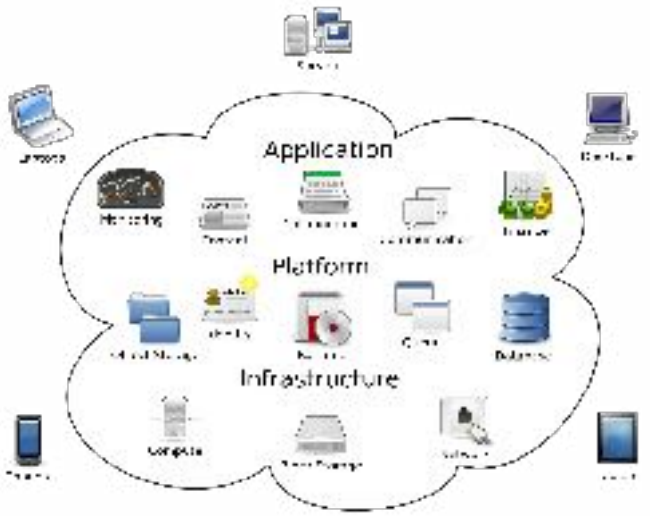
Any part of supply network that can be Digital, shall be Digital

Cloud Computing Connections

AWS IoT Core for Long Range/Low Power WAN

A key and tremendously important technology to understand is how Cloud deployment fits into infrastructure

https://aws.amazon.com/iot-core/lorawan



Images Source: Digital Supply Networks: Transform Your Supply Chain and Gain Competitive Advantage with Disruptive Technology and Reimagined Processes by Amit Sinha, Ednilson Bernardes, et al.

Cloud Computing is no longer an option, but rather a core business decision

Basic Understanding

Low Power/Long Range

Low Power/Long Range is a wireless modulation technique derived from Chirp Spread Spectrum (CSS) technology. It encodes information on radio waves using chirp pulses - similar to the way dolphins and bats communicate! Long Range/Low Power modulated transmission is robust against disturbances and can be received across great distances

Wide Area Layer (MAC)

Wide Area Layer is a Media Access Control (MAC) layer protocol built on top of Low Power/Long Range modulation. It is a software layer which defines how devices use the protocol hardware, for example when they transmit, and the format of messages.

Long Range/Low Power is the physical layer and Wide Area Network is the software layer

Technical Specs

Standard: IEEE802.15.4

Frequency: ISM bands 433, 868, 915 MHz

Bandwidth: 125Khz, 250Khz, 500 KHz

Data Rate: Up to 50kbps

Range: Up to 20 KM or approx. 12.5 milesv

Data Rate (Rb) Formula

$$R_b = SF * \frac{\left[\frac{4}{4+CR}\right]}{\left[\frac{2^{SF}}{BW}\right]} * 1000$$

SF = Spreading Factor (6,7,8,9,10,11,12)
CR = Code Rate (1,2,3,4)
BW = Bandwidth in KHz (10.4,15.6,20.8,31.25,41.7,62.5,125,250,500)
Rb = Data rate or Bit Rate in bps

Key Indicators and expected Operational Parameters

Benefits:Long Range/Low Power

The physical layer uses robust CSS modulation. CSS stands for Chirp Spread Spectrum. It uses 6 SF (spreading factors) from SF 7 to 12. This delivers orthogonal transmissions at different data rates. Moreover it provides processing gain and hence transmitter output power can be reduced with same RF link budget and hence will increase battery life.

It uses Long Range/Low Power modulation which has constant envelope modulation similar to FSK modulation type and hence available PA (power amplifier) stages having low cost and low power with high efficiency can be used.

Long Range/Low Power supports three different types of devices viz. class-A, class-B and class-C.

Uses 868MHz/915MHz ISM available worldwide (EU/US)

Very wide coverage: ~5km/Urban and 15km suburbs

Very low battery consumption - Temp/Humid ~10 years

Single Gateway designed to handle 1000s of devices/nodes

Simple Architecture - discussed earlier

Widely available for M2M/IIoT devices/applications

Weakness of Protocol

Can be used for applications requiring low data rate, up to about 27 Kbps

Network size is limited based on parameter called as duty cycle. It is defined as percentage of time during which the channel can be occupied. This parameter arises from the regulation as key limiting factor for traffic served in the network.

Unable to use trademarked term of specific alliance without being member of alliance

It is not ideal candidate to be used for real time applications requiring lower latency and bounded jitter requirements.

Small Number of Use Cases

Suitable use-cases:

- Long range - multiple kilometers
- Low power - can last years on a battery
- Low cost - less than 20€ CAPEX per node, almost no OPEX *(2020 Alliance study)*
- Low bandwidth - between 250 bit/s and 11 kbit/s in Europe using LoRa modulation (depending on the spreading factor)
- Coverage everywhere - you are the network. Just install your own gateways
- Secure - 128 bit end-to-end encrypted

Not Suitable use-cases:

- Realtime data - you can only send small packets every couple of minutes
- Phone calls - you can do that with GPRS/3G/LTE
- Controlling lights in your house - check out ZigBee or Bluetooth
- Sending photos, watching Netflix - check out Wi-Fi

Expectation examples suitable and non-suitable uses cases

Frequency Allocations

US902-928

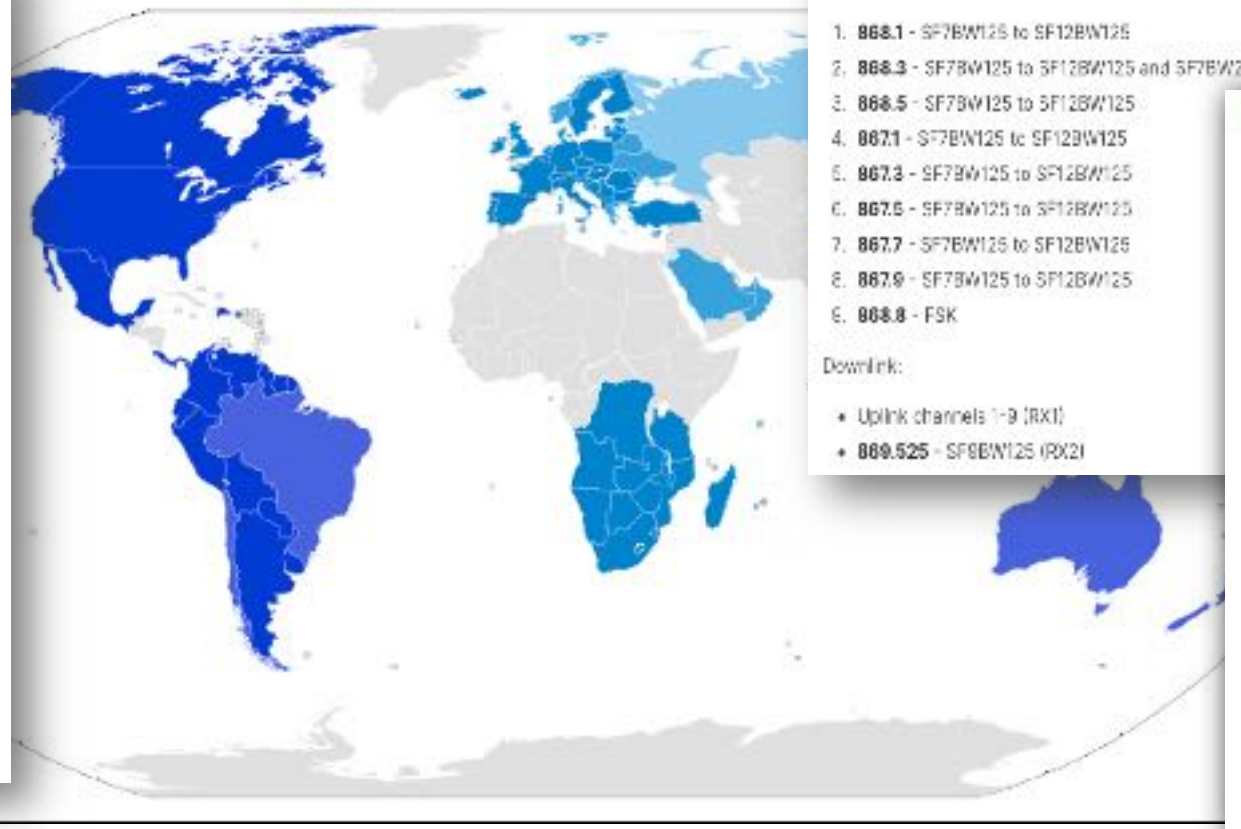
Used in USA, Canada and South America

Uplink:

1. **903.9** - SF7BW125 to SF10BW125
2. **904.1** - SF7BW125 to SF10BW125
3. **904.3** - SF7BW125 to SF10BW125
4. **904.5** - SF7BW125 to SF10BW125
5. **904.7** - SF7BW125 to SF10BW125
6. **904.9** - SF7BW125 to SF10BW125
7. **905.1** - SF7BW125 to SF10BW125
8. **905.3** - SF7BW125 to SF10BW125
9. **904.6** - SF8BW500

Downlink:

1. **923.3** - SF7BW500 to SF12BW500 (RX1)
2. **923.9** - SF7BW500 to SF12BW500 (RX1)
3. **924.5** - SF7BW500 to SF12BW500 (RX1)
4. **925.1** - SF7BW500 to SF12BW500 (RX1)
5. **925.7** - SF7BW500 to SF12BW500 (RX1)
6. **926.3** - SF7BW500 to SF12BW500 (RX1)
7. **926.9** - SF7BW500 to SF12BW500 (RX1)
8. **927.5** - SF7BW500 to SF12BW500 (RX1)
9. **923.3** - SF12BW500 (RX2)



EU863-870

Uplink:

1. **868.1** - SF7BW125 to SF12BW125
2. **868.3** - SF7BW125 to SF12BW125 and SF7BW250
3. **868.5** - SF7BW125 to SF12BW125
4. **867.1** - SF7BW125 to SF12BW125
5. **867.3** - SF7BW125 to SF12BW125
6. **867.5** - SF7BW125 to SF12BW125
7. **867.7** - SF7BW125 to SF12BW125
8. **867.9** - SF7BW125 to SF12BW125
9. **868.8** - FSK

Downlink:

- Uplink channels 1-9 (RX1)
- **869.525** - SF9BW125 (RX2)

AU915-928

Uplink:

1. **916.8** - SF7BW125 to SF12BW125
2. **917.0** - SF7BW125 to SF12BW125
3. **917.2** - SF7BW125 to SF12BW125
4. **917.4** - SF7BW125 to SF12BW125
5. **917.6** - SF7BW125 to SF12BW125
6. **917.8** - SF7BW125 to SF12BW125
7. **918.0** - SF7BW125 to SF12BW125
8. **918.2** - SF7BW125 to SF12BW125
9. **917.5** - SF8BW500

Downlink:

1. **923.3** - SF7BW500 to SF12BW500 (RX1)
2. **923.9** - SF7BW500 to SF12BW500 (RX1)
3. **924.5** - SF7BW500 to SF12BW500 (RX1)
4. **925.1** - SF7BW500 to SF12BW500 (RX1)
5. **925.7** - SF7BW500 to SF12BW500 (RX1)
6. **926.3** - SF7BW500 to SF12BW500 (RX1)
7. **926.9** - SF7BW500 to SF12BW500 (RX1)
8. **927.8** - SF7BW500 to SF12BW500 (RX1)
9. **923.3** - SF12BW500 (RX2)

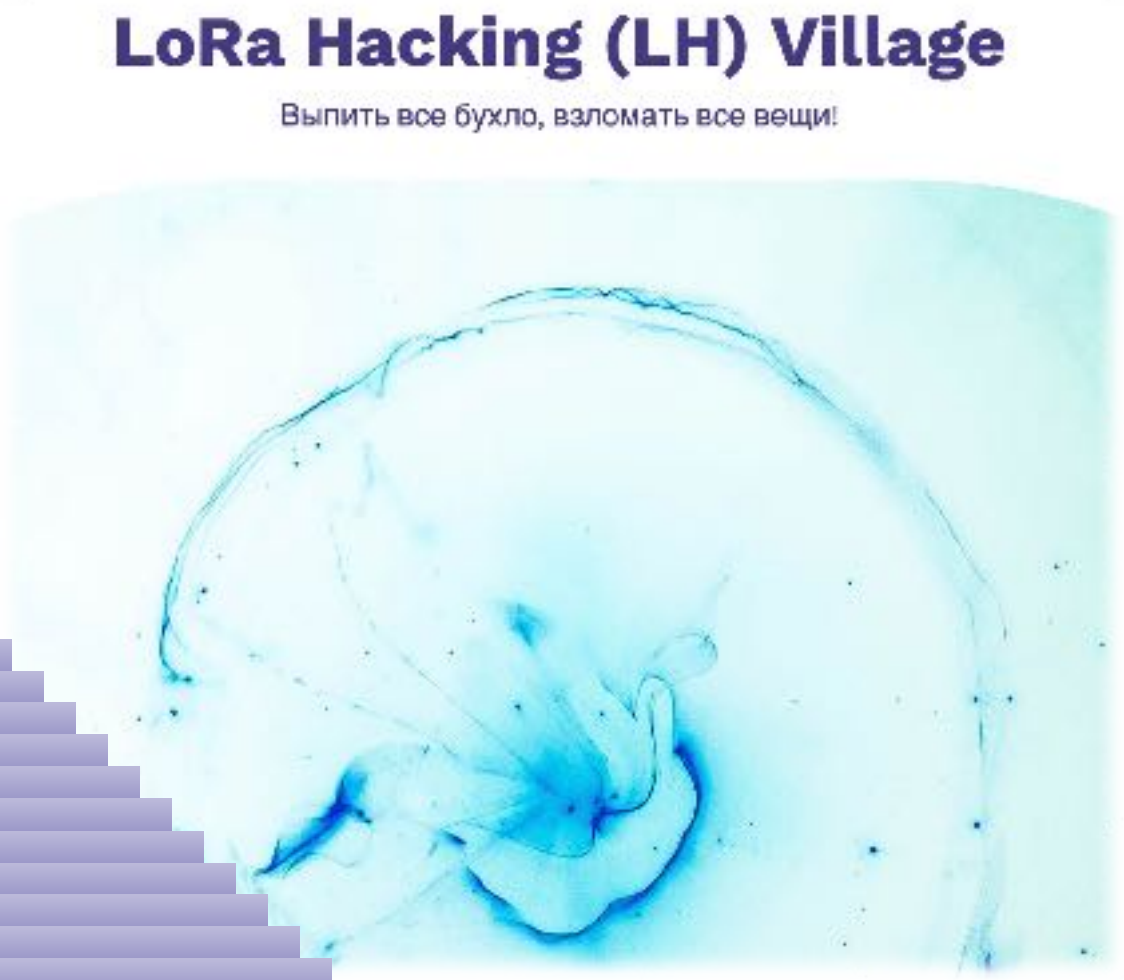
Data & Image Source: https://www.thethingsnetwork.org/docs/lorawan/frequency-plans/

Listed allocations are for North & South America, European Union, Brazil/Australia

Summary and Questions

- Value Proposition
- Standards
- Cybersecurity as a core competency
- Low Power/ Long Range details

Thank you.



https://lorahackingvillage.org

“In The Sandbox” / Demo

“The next Monday, when the fathers were all back at work, we kids were playing in a field. One kid says to me, “See that bird? What kind of bird is that?” I said, “I haven’t the slightest idea what kind of a bird it is.” He says, “It’s a brown-throated thrush. Your father doesn’t teach you anything!” But it was the opposite. He had already taught me: “See that bird?” he says. “It’s a Spencer’s warbler.” (I knew he didn’t know the real name.) “Well, in Italian, it’s a Chutto Lapittida. In Portuguese, it’s a Bom da Peida. In Chinese, it’s a Chung-long-tah, and in Japanese, it’s a Katano Tekeda. You can know the name of that bird in all the languages of the world, but when you’re finished, you’ll know absolutely nothing whatever about the bird. You’ll only know about humans in different places, and what they call the bird. So let’s look at the bird and see what it’s doing—that’s what counts.” I learned very early the difference between knowing the name of something and knowing something.”

https://jeremykun.com/2016/09/19/zero-knowledge-definitions-and-theory/