

**NOKIA**

# Flood Abatement

## Flood Abatement

- Modern cities have impermeable soils and rely on their drain system to evacuate water. According to FEMA, “Around 20-25 percent of all economic losses resulting from flooding occur in areas not designated as being in a “floodplain,” but as a consequence of urban drainage.”
- High intensity rainfall can cause flooding when the city storm water drainage system does not have the necessary capacity to drain away the amounts of rain that are falling, often due to clogged storm drains.
- This solution monitors the water level of storm drains throughout the city and helps detect anomalies such as clogged drains due to debris. In case of heavy rainfall, storm drain flooding can be monitored in real time, allowing better response, such as traffic redirection.



**TUSSOCK**  
innovation

**NOKIA**

# Flood abatement



## Final product

### Ultra Low Power

Industry leading sub 1uA sleep current with RTC running providing years of battery life. In sensor only mode the battery will last up to 6 years based on 15 minute samples. For outdoor maintenance free sensors, we offer a rechargeable system pushing the battery life to >10 years.

### Durable Enclosure

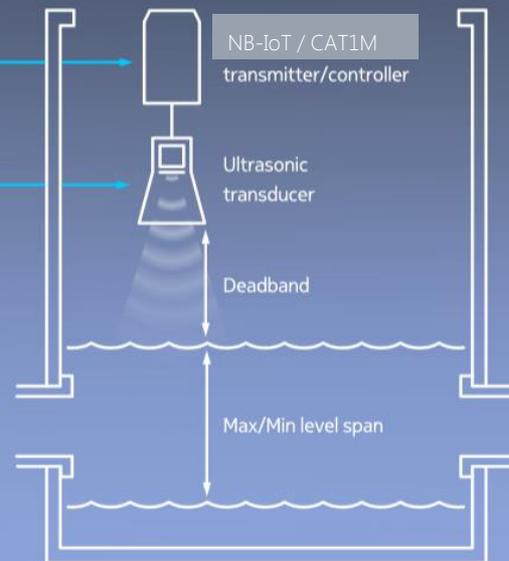
A production ready waterproof enclosure provides options for both outdoor and indoor operation. It also allows users to configure sensing solutions to their requirements.

### NB-IoT, CAT1M Technology

NB-IoT, CAT1M technology are supported at output power up to 20 dbm with FCC approved. NB-IoT power saving features e.g. eDRX, PSM, HLCOM allows longer battery life

### Ultrasonic range finder

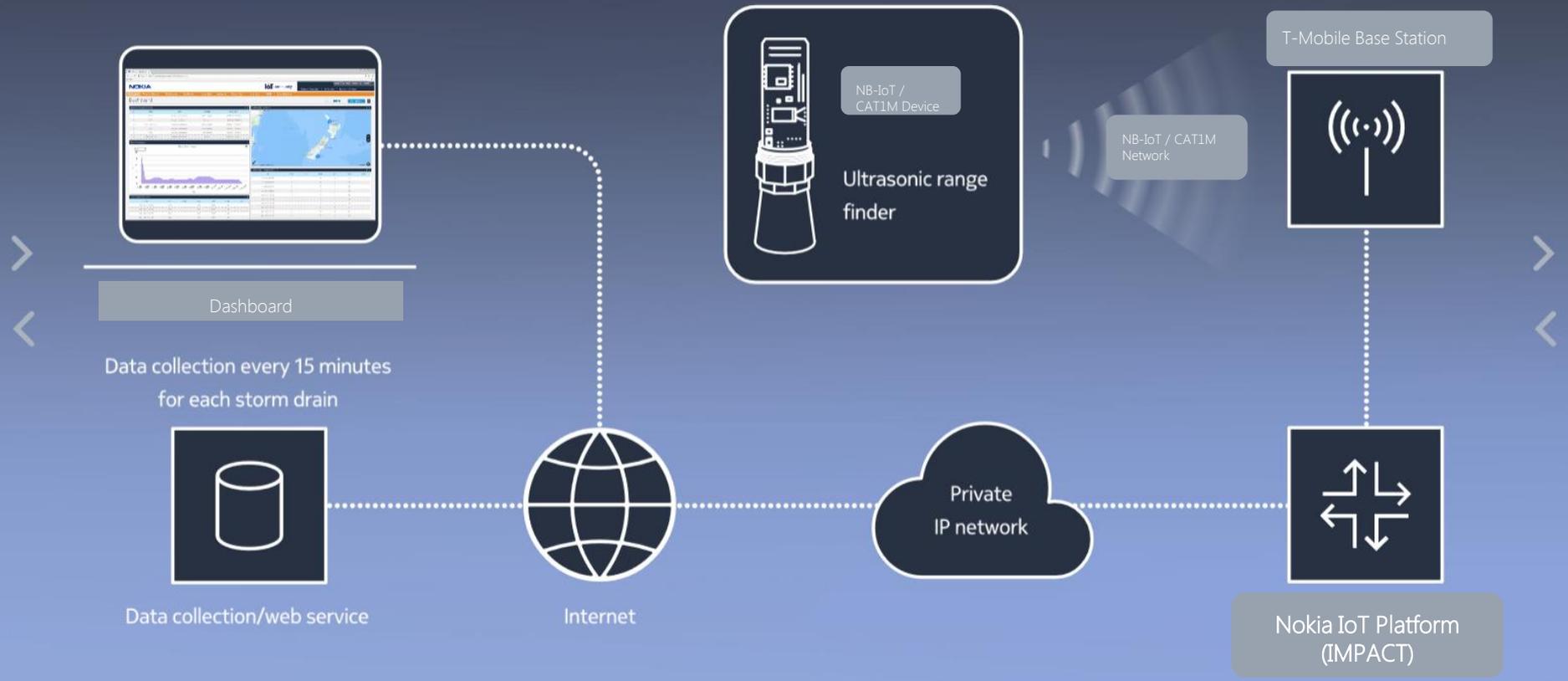
This ultrasonic transducer is a cost-effective solution for applications requiring precision range-finding, low-voltage operation, space saving, low-cost, and IP67 rating for weather resistance. It provides high accuracy and high resolution ultrasonic proximity detection and ranging in air.



# Flood abatement



## Network layout



# Demo

<http://209.202.115.189/MainDemos/2017/floodabatement3.0/>

# IoT Security

## Mission Critical Networks are Under Attack

3% of global mining, oil, gas companies hacked	Hackers use virus to steal £20 MILLION from UK bank accounts	MIRAI Bot DDoS attack ->1.2 million infected IoT devices	Hacker group Dragonfly 2.0 compromised OT networks of 2 utilities in the US and Europe
2014	2015	2016	2017
US Department of Energy hacked 150 times in four years	Ukrainian grid attack -> 250,000 people without power	Flight information screens in two Vietnam airports hacked	Global WannaCry attack -> 200,000+ endpoints; disturbance of services
Loss of revenue and compensations	Recovery and restoration costs	Potential lawsuits and penalties	Damage to brand reputation

"While many cyber defenses are improving in global enterprises, the number of bad actors is also growing rapidly. The breadth and depth of cyber threats and online vulnerabilities continues to grow - especially with new Internet of Things (IoT) devices coming onto the market."

*Dan Lohrmann on cybersecurity & infrastructure, Government Technology magazine, Dec. 2016*

# IoT Security Challenges

The 'S' in IoT stands for 'Security' OT vs IT

## Long IoT Device Lifetime

High effort to update devices in the field.  
Outdated security mechanisms needed for legacy devices.

### Encryption power decreases over lifetime

→ Cracking of encryption in 5-10 years possible!

### Anti-Malware support seldom available for 10+ years

→ Small quantities might not get any support!

## maintained IoT devices

How many users really care as long as it works?

### Who updates the camera?

→ Vulnerable devices can be hijacked by attackers

Nobody will care about it as long as the camera works,...

### Overlap of IT and OT

- Unintentional linkages are formed accidentally over time
- Vulnerabilities are created

## Signaling Storms

There will be many IoT devices.  
Normal IoT device signaling footprint will often be low.

### Malware could increase device activity drastically

- Networks can overload
- Battery drain

Networks are not overprovisioned to cater for unexpected high loads

### Roaming devices could jump between networks

- Affects visited network and roaming interfaces

When a network goes down or locks out devices, they seek for connectivity



# Types of Compromise for IoT

## *Data*

- Data exfiltration
- Data modification/corruption
- Data suppression
- Ransomware

## *Resources*

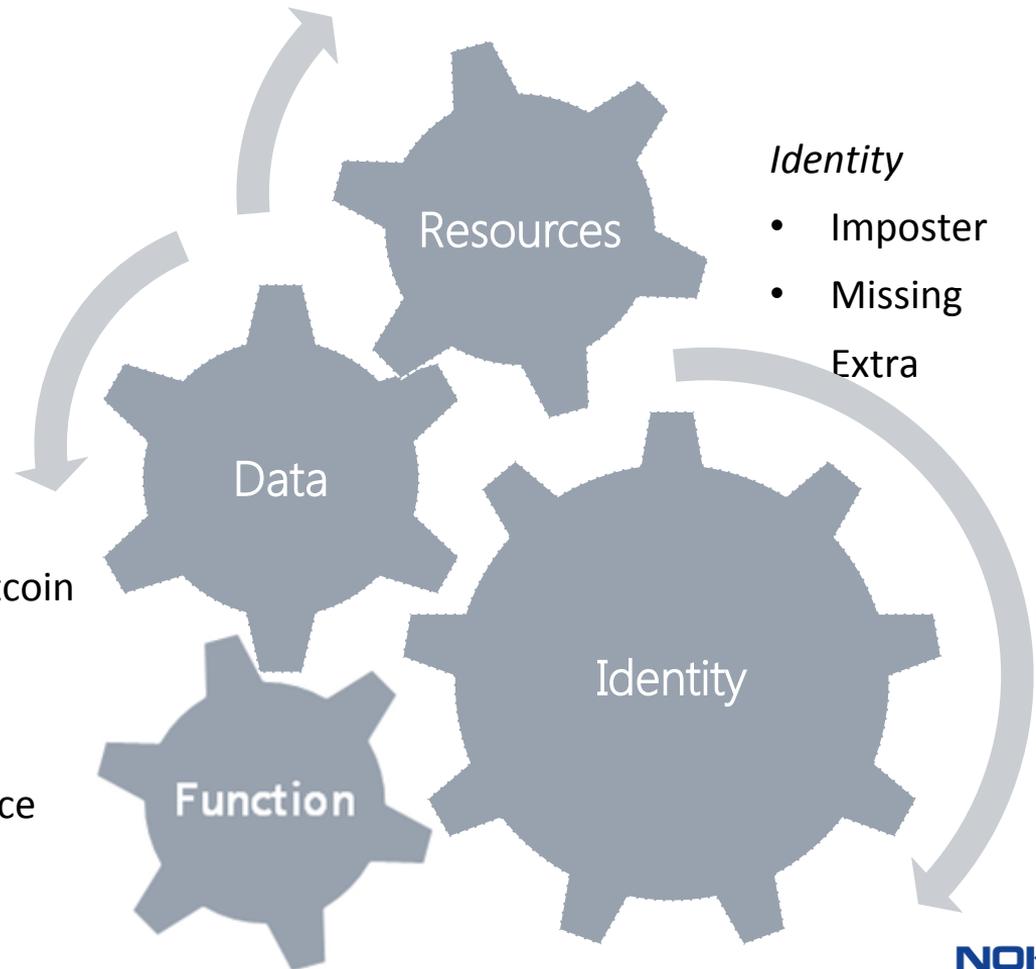
- Theft of device resources for bitcoin mining or spambots

## *Function*

- Disrupt the function of the service for business or political aims

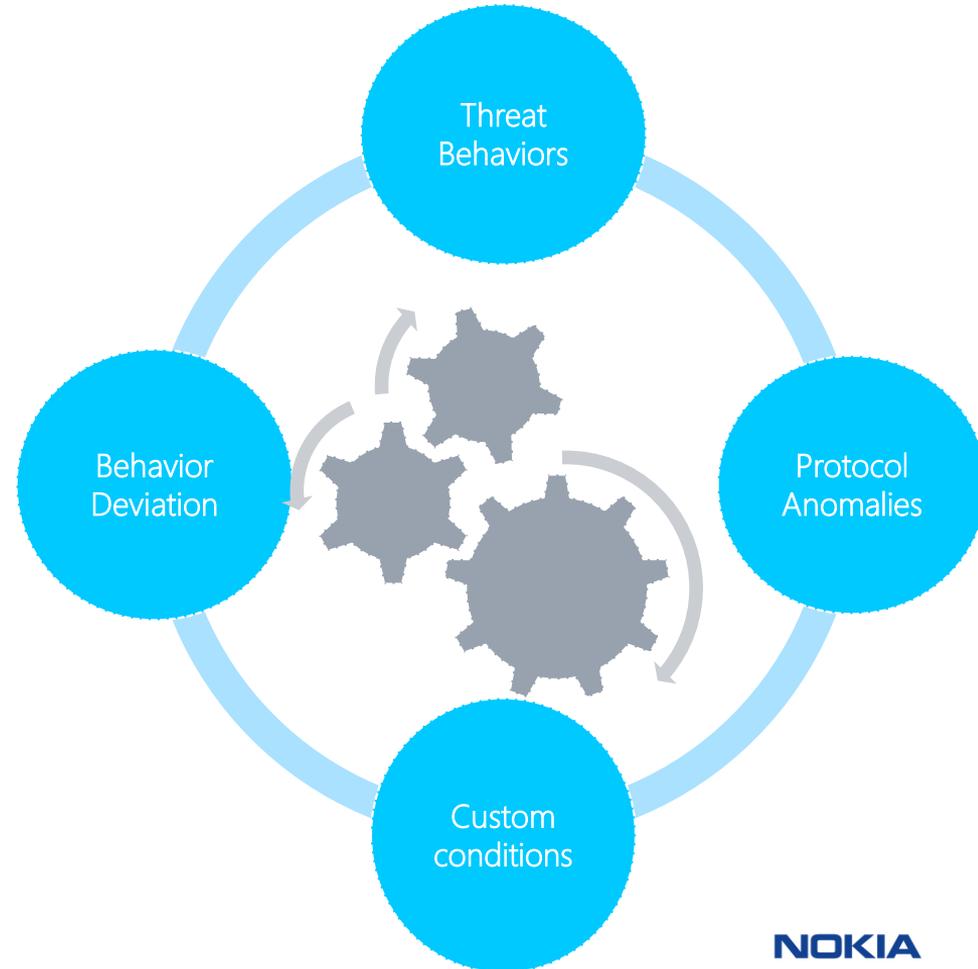
## *Identity*

- Imposter
- Missing  
Extra



## 360 degrees of monitoring

- 1) **Malware/threat behavior** – exact match with a threat conditions
- 2) **Device profile anomalies** – not correct per approved profile
- 3) **Protocol anomalies** – even if not defined as a threat behavior (DNP3, Modbus)
- 4) **Custom conditions** – can be defined and expressed.



# Recommended Best Practices

## A Closer Look NERC CIP: 10 Standards, 30 Requirements



CIP-002	CIP-003		CIP-010	CIP-011
BES CYBER-SYSTEM IDENTIFICATION AND CATEGORIZATION	SECURITY MANAGEMENT CONTROLS	<b>Privileged Account Management</b> <ul style="list-style-type: none"> <li>• Implement access control policies</li> <li>• Proactively secure privileged credentials</li> <li>• Rotate admin credentials after each use</li> <li>• Monitor privileged account usage to detect anomalies</li> </ul>	CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENT	INFORMATION PROTECTION
1. BSS CYBER SYSTEM IDENTIFICATION	1. CYBER SECURITY POLICY FOR HIGH/MED SYSTEMS		1. CONFIGURATION CHANGE MANAGEMENT	1. INFORMATION PROTECTION
2. REGULAR APPROVAL	2. CYBER SECURITY POLICY FOR LOW SYSTEMS	<b>Configuration Compliance Checking</b> <ul style="list-style-type: none"> <li>• Develop and maintain baseline configurations</li> <li>• Record deviations from baselines</li> <li>• Update baseline configurations after a change</li> <li>• Monitor the baseline configuration every 35 days</li> </ul>	2. CONFIGURATION MONITORING	2. BES CYBER ASSET REUSE AND DISPOSAL
			3. VULNERABILITY ASSESSMENTS	
		<b>Scan for Malware</b>		
		<b>Secure Networking</b> <ul style="list-style-type: none"> <li>• Encrypt communications with external routable connectivity</li> </ul>		

# Nokia Helps Utilities Implement Best Practices

CIP-002	CIP-003	CIP-004	CIP-005	CIP-006	CIP-007	CIP-008	CIP-009	CIP-010	CIP-011
BES CYBER-SYSTEM IDENTIFICATION AND CATEGORIZATION	SECURITY MANAGEMENT CONTROLS	TRAINING AND PERSONNEL SECURITY	ELECTRONIC SECURITY PERIMETER	PHYSICAL SECURITY OF BES CYBER SYSTEMS	SYSTEMS SECURITY MANAGEMENT	INCIDENT REPORTING AND RESPONSE PLANNING	RECOVERY PLANS FOR BES CYBER SYSTEMS	CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENT	INFORMATION PROTECTION
NETGUARD INTEGRITY AUDIT COMPLIANCE MANAGER	NETGUARD SECURITY MANAGEMENT CENTER (NSMC)	1. AWARENESS	1. ELECTRONIC SECURITY PERIMETER	NSMC	NSMC	NSMC	1. RECOVERY PLAN SPECIFICATIONS	NACM	NETGUARD DATA PROTECTION (NDP)
2. REGULAR APPROVAL	NSMC	2. TRAINING	NIAM	NSMC	2. SECURITY PATCH MANAGEMENT	2. INCIDENT RESPONSE PLAN IMPLEMENTATION AND TESTING	2. RECOVERY PLAN IMPLEMENTATION AND TESTING	NACM + NSMC	2. BES CYBER ASSET REUSE AND DISPOSAL
		3. PERSONNEL RISK ASSESSMENT PROGRAM	1.5 DETECTION OF MALICIOUS COMMUNICATION	3. MAINTENANCE AND TESTING PROGRAM	NIAM + NETGUARD AUDIT COMPLIANCE MANAGER (NACM)	3. INCIDENT RESPONSE PLAN REVIEW, UPDATE AND COMMUNICATION	3. RECOVERY PLAN REVIEW, UPDATE AND COMMUNICATION	NSMC	
		NETGUARD IDENTITY ACCESS MANAGER (NIAM)	NETGUARD ENDPOINT SECURITY (NES)		NSMC				
		NIAM			5. SYSTEM ACCESS CONTROLS				

 Products  
 Services

**NOKIA**

# Copyright and confidentiality

---

The contents of this document are proprietary and confidential property of Nokia. This document is provided subject to confidentiality obligations of the applicable agreement(s).

This document is intended for use of Nokia's customers and collaborators only for the purpose for which this document is submitted by Nokia. No part of this document may be reproduced or made available to the public or to any third party in any form or means without the prior written permission of Nokia. This document is to be used by properly trained professional personnel. Any use of the contents in this document is limited strictly to the use(s) specifically created in the applicable agreement(s) under which the document is submitted. The user of this document may voluntarily provide suggestions, comments or other feedback to Nokia in respect of the contents of this document ("Feedback"). Such Feedback may be used in Nokia

products and related specifications or other documentation. Accordingly, if the user of this document gives Nokia Feedback on the contents of this document, Nokia may freely use, disclose, reproduce, license, distribute and otherwise commercialize the feedback in any Nokia product, technology, service, specification or other documentation.

Nokia operates a policy of ongoing development. Nokia reserves the right to make changes and improvements to any of the products and/or services described in this document or withdraw this document at any time without prior notice.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose,

are made in relation to the accuracy, reliability or contents of this document. NOKIA SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT or for any loss of data or income or any special, incidental, consequential, indirect or direct damages howsoever caused, that might arise from the use of this document or any contents of this document.

This document and the product(s) it describes are protected by copyright according to the applicable laws.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.