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

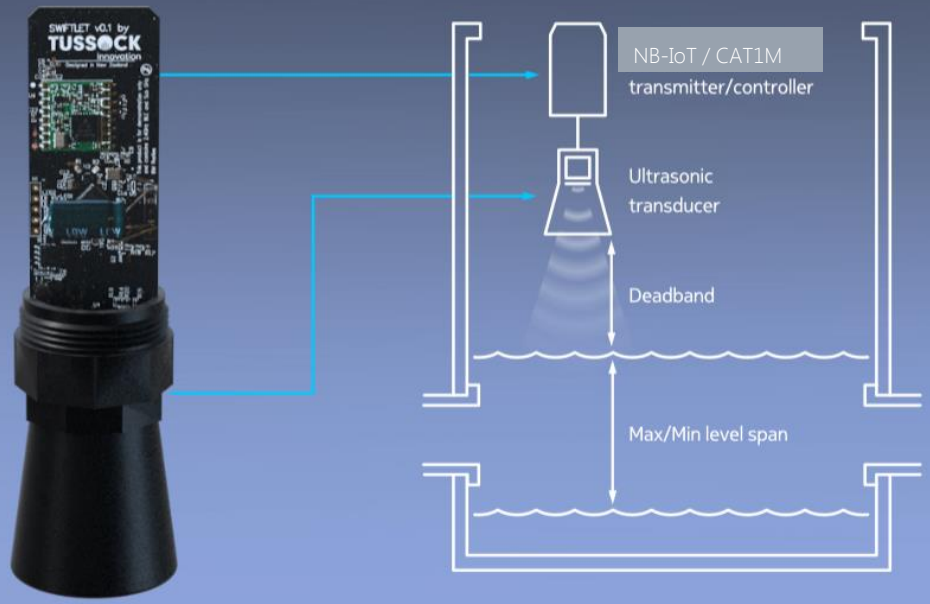
A production ready waterproof enclosure provides options for both outdoor and indoor operation. It also allows users to configure sensing solutions to their requirements.

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

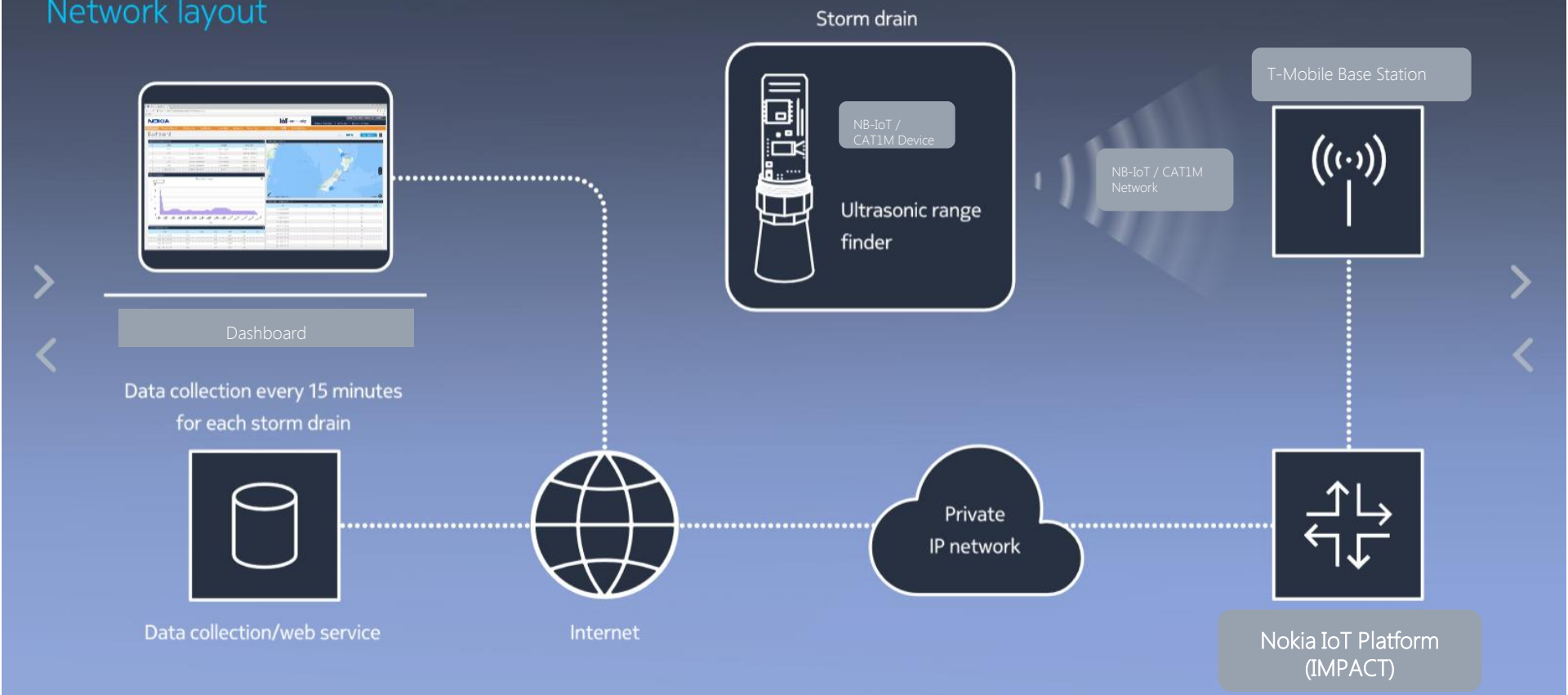
This ultrasonic transducer is a cost-effective solution for applications requiring precision range-finding, low-voltage operation, space saving, low-cost, and IP67 rating for weather resistance. It provides high accuracy and high resolution ultrasonic proximity detection and ranging in air.



NOKIA

Flood abatement

Network layout

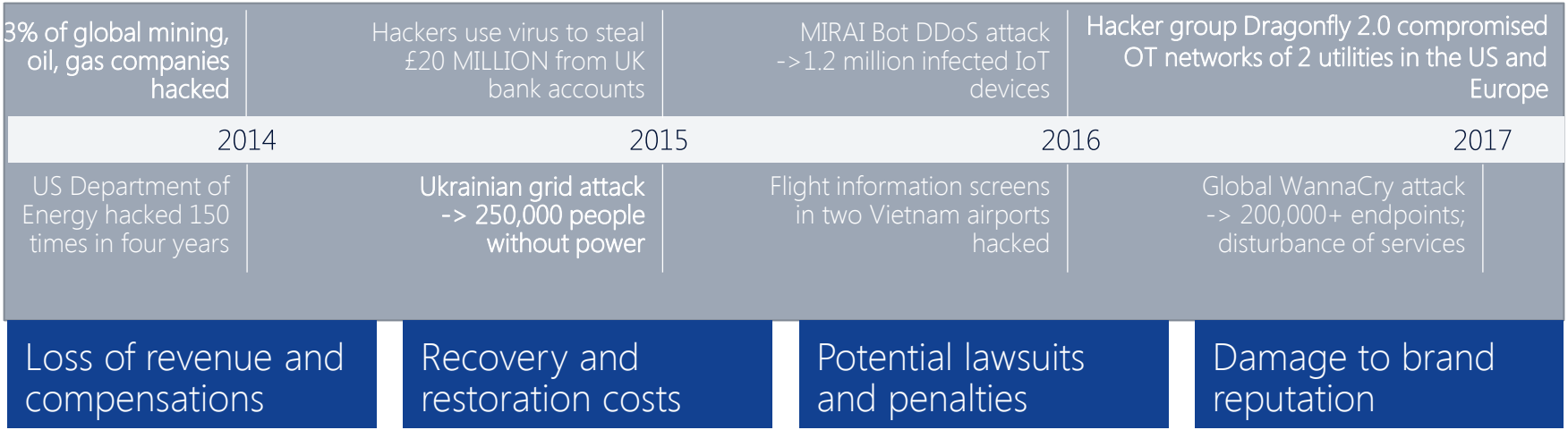


Demo

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

IoT Security

Mission Critical Networks are Under Attack



"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

NOKIA

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!

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

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 accidently over time

•Vulnerabilies are created

Types of Compromise for IoT

Data

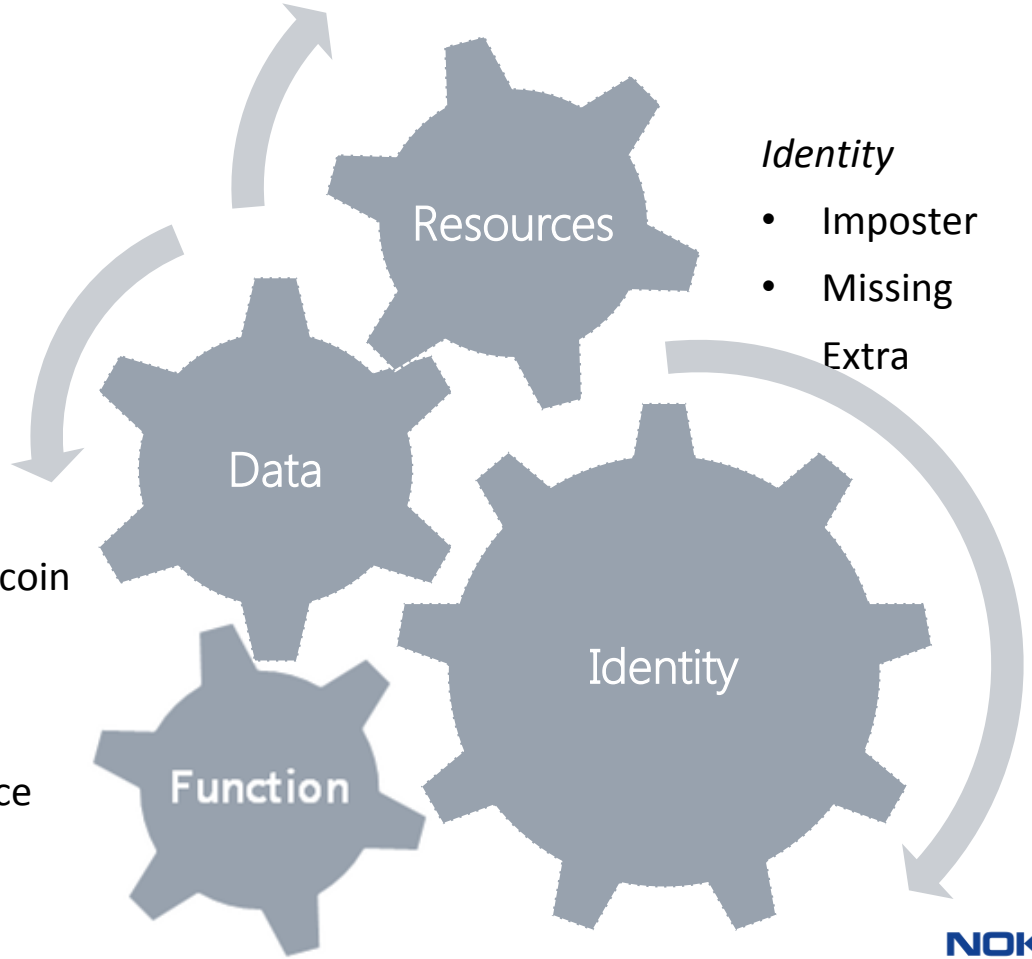
- Data exfiltration
- Data modification/corruption
- Data suppression
- Ransomware

Resources

- Theft of device resources for bitcoin mining or spambots

Function

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



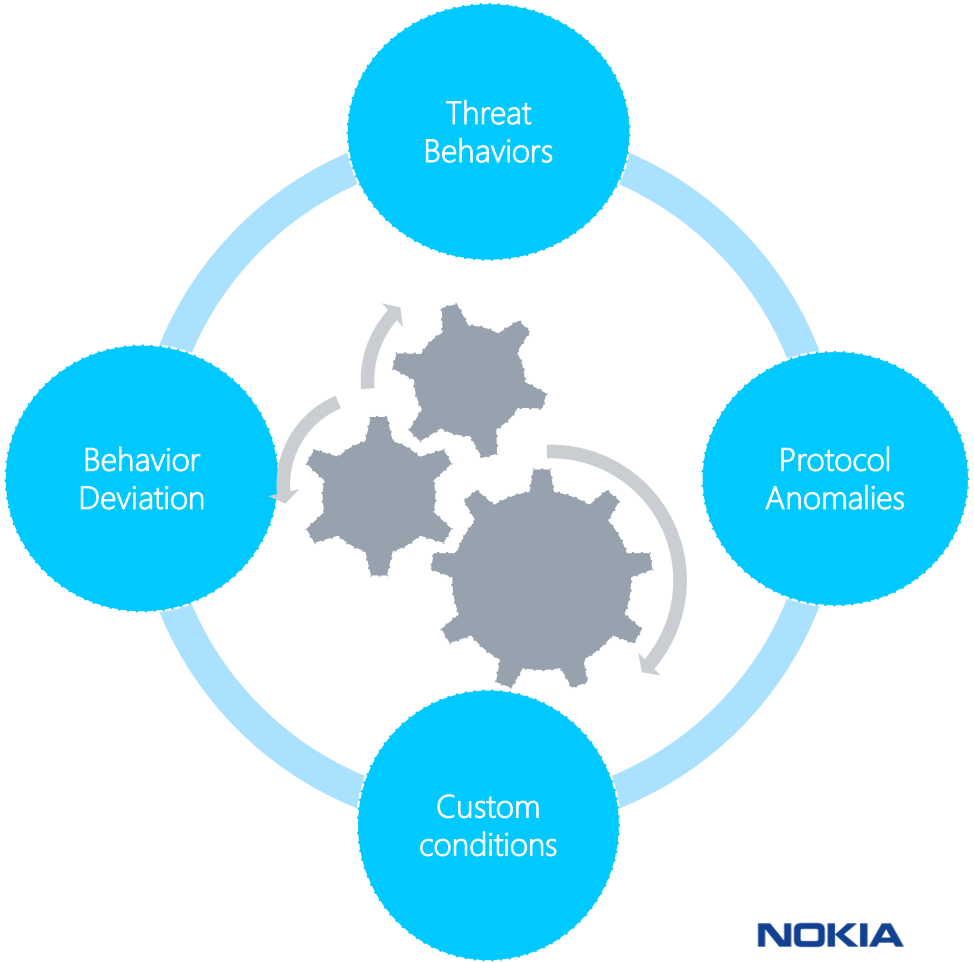
Identity

- Imposter
- Missing
- Extra

NOKIA

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	CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENT	INFORMATION PROTECTION
1. BSS CYBER SYSTEM IDENTI-FICATION	1. CYBER SECURITY POLICY FOR HIGH/MED SYSTEMS	1. CONFIGU-RATION CHANGE MANAGEMENT	1. INFORMATION PROTECTION
2. REGULAR APPROVAL	2. CYBER SECURITY POLICY FOR LOW SYSTEMS	2. CONFIGU-RATION MONITOING	2. BES CYBER ASSET REUSE AND DISPOSAL
		3.VULNERABILITY ASSESSMENTS	

Privileged Account Management

- Implement access control policies
- Proactively secure privileged credentials
- Rotate admin credentials after each use
- Monitor privileged account usage to detect anomalies

Configuration Compliance Checking

- Develop and maintain baseline configurations
- Record deviations from baselines
- Update baseline configurations after a change
- Monitor the baseline configuration every 35 days

Scan for Malware

Secure Networking

- Encrypt communications with external routable connectivity

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 SPECIFICA-TIONS	NACM	NETGUARD DATA PROTECTION (NDP)
2. REGULAR APPROVAL	NSMC	2. TRAINING	NIAM	NSMC	2. SECURITY PATCH MANAGEMENT	2. INCIDENT RESPONSE PLAN IMPLE-MENTATION AND TESTING	2. RECOVERY PLAN IMPLEMENTA-TION AND TESTING	NACM + NSMC	2. BES CYBER ASSET REUSE AND DISPOSAL
		3. PERSONNEL RISK ASSESSMENT PROGRAM	1.5 DETECTION OF MALICIOUS COMMUNICATIO N	3. MAINTENANCE AND TESTING PROGRAM	NIAM + NETGUARD AUDIT COMPLIANCE MANAGER (NACM)	3. INCIDENT RESPONSE PLAN REVIEW, UPDATE AND COMMUNICATIO	3. RECOVERY PLAN REVIEW, UPDATE AND COMMUNICATIO N	NSMC	
		NETGUARD IDENTITY ACCESS MANAGER (NIAM)	NETGUARD ENDPOINT SECURITY (NES)		NSMC				
		NIAM			5. SYSTEM ACCESS CONTROLS				

Products

Services


NOKIA

Copyright and confidentiality