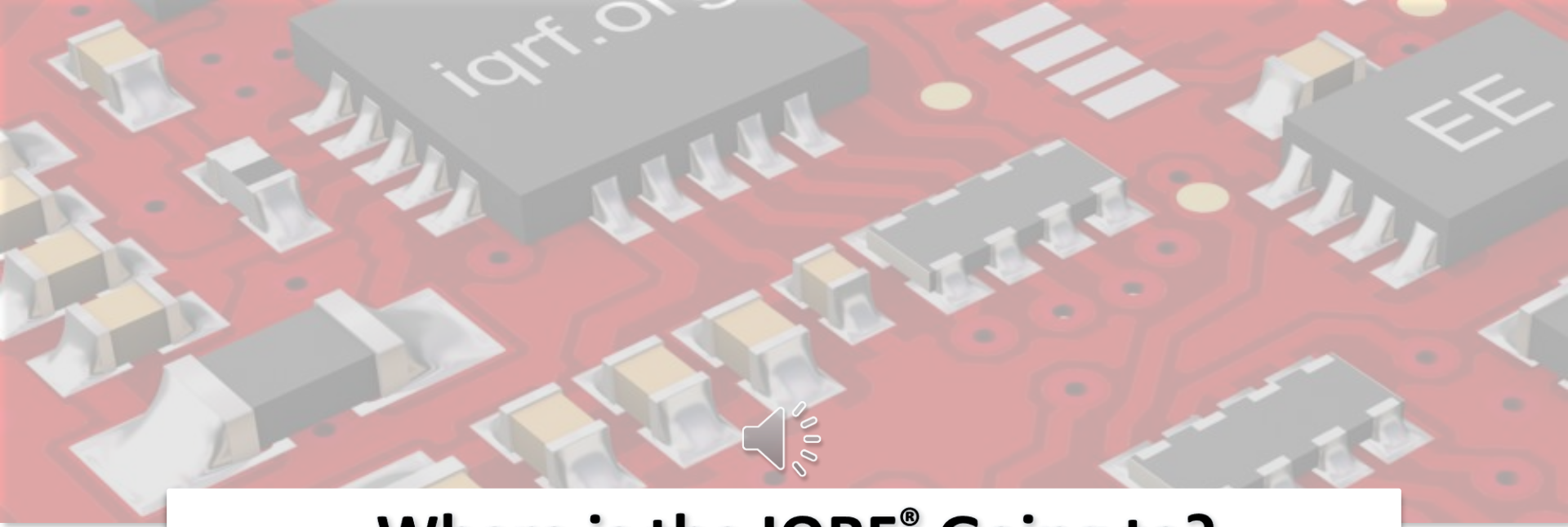


Where is the IQRF® Going to?

Vladimír Šulc, Ph.D. | MICRORISC s.r.o. | sulc@microrisc.com

MICRORISC ENABLING FUTURE INNOVATION

ICSNC 2021, October 03, 2021 to October 07, 2021 - Barcelona, Spain
The Sixteenth International Conference on Systems and Networks Communications

IARIA

Vladimír Šulc is a co-owner and CEO of MICRORISC s.r.o., Czech Republic, working since 1991 on many projects related to the wireless communication and security. He specializes in mesh networking algorithms. Author or co-author of 30+ patents and utility patents in CZ, EU, US, JP, CN.

He graduated Czech Technical University in Prague, Faculty of Electrical Engineering, in 1992, and holds a Ph.D. in Microelectronics wireless networks from Brno Technical University.

As a leader of several project teams he has been actively working on projects related to his specialization: Wireless communication platforms and topologies. Currently, he focus on an IQRF® wireless mesh standardization and as a CEO of the IQRF Alliance he is evangelizing the IQRF® technology.

Dr. Vladimír Šulc has been active in IARIA conferences since 2009. Papers “IQRF Smart House - A Case Study” presented at MESH 2010 and “IQMESH, Technology for Wireless Mesh Networks: Implementation Case Studies” presented at ICNS 2012 were awarded by Best Paper Awards.

Key projects

FI-IM4/034 Smart platform for wireless communication (2007-2010, MPO/FI)

FR-TI1/058 Intelligent house-open platform (2009-2012, MPO/FR)

FR-TI3/254 Open platform for telemetry (2011-2014, MPO/FR)

FR-TI3/275 Open platform for smart cities (2011-2014, MPO/FR)

FV-40303 Communication infrastructure for battery powered devices (2018-2021, MPO/FV)

FV-40132 Development of an autonomous off-grid system for bidirectional communication with wireless nodes (2018-2022, MPO/FV)

What is the IQRF®, its **Positioning** and **Why** to adopt it

Industrial Reliability and protocols behind: IQMESH®, FRC®

IQRF True Low Power® and protocols behind: beaming + offline FRC + local FRC

Interoperability / Simple integration: IQRF Data Controlled Transceivers®

Ultimate security: every single detail matters

Open and fully documented: … simply visit www.iqrf.org

So, where is the IQRF® going to?

What is the IQRF®, its Positioning and Why to adopt it

Industrial Reliability and protocols behind: IQMESH®, FRC®

IQRF True Low Power® and protocols behind: beaming + offline FRC + local FRC

Interoperability / Simple integration: IQRF Data Controlled Transceivers®

Ultimate security: every single detail matters

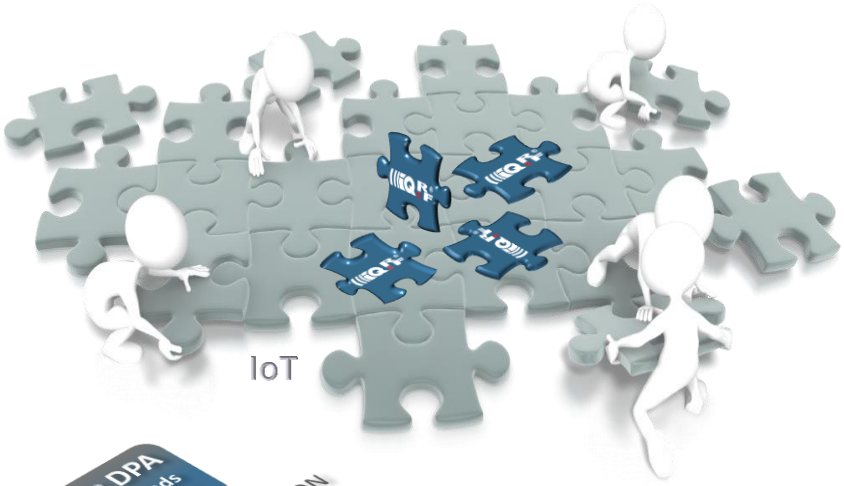
Open and fully documented: … simply visit www.iqrf.org

So, where is the IQRF® going to?

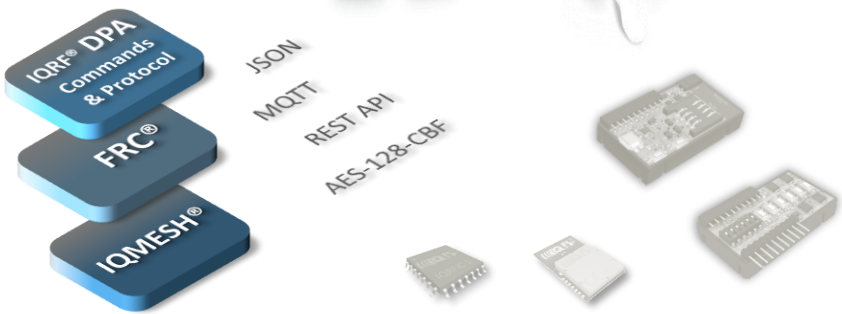
The IQRF® is …

… a wireless mesh technology

connecting things since 2004



protocols
standards
security
components
tools
devices
applications
clouds
services
systems
IQRF Alliance



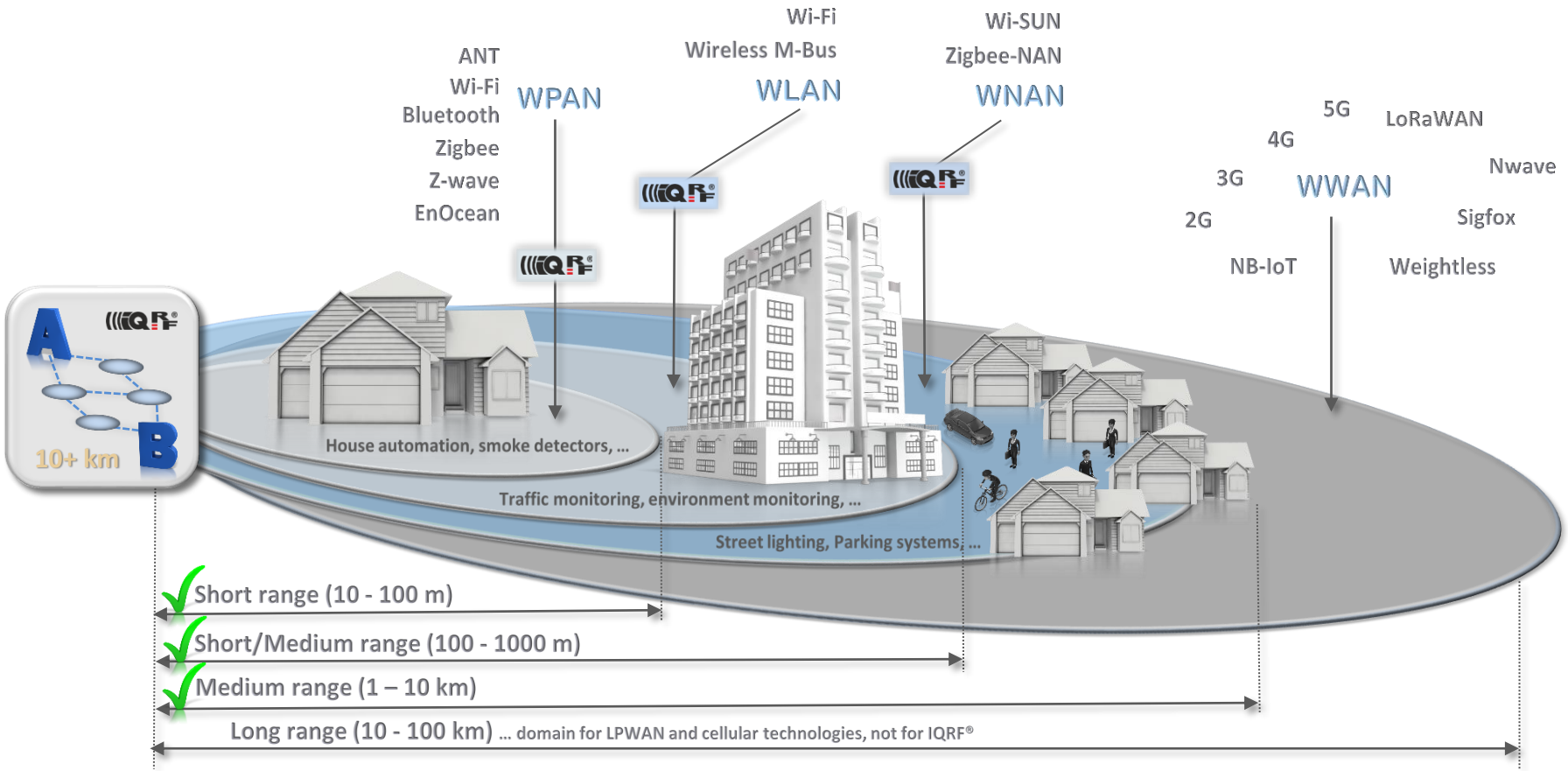
IQRF® evolved into a fast growing ecosystem

and a horizontal platform for building variety of vertical solutions

Smarter wireless. Simply.

Positioning

Market is deeply fragmented, there is no globally accepted standard due to the technological or application limitations.



Thanks to the routing, IQRF® can reliably communicate 10+ km, addressing huge segment of low power applications, as monitoring, automation or control.

Smarter wireless. Simply.

The market is deeply fragmented …

… because of many limitations

Technical

NO (or not efficient) BIDIRECTIONAL COMMUNICATION:
- Cannot be used for control systems
- Maintenance issues, no remote configuration or upgrades
- Problem with security: no security updates available

NO ROUTING (= NO MESH SUPPORT)
- Not covering “difficult” areas (deep indoor, obstacles, …)

COMMUNICATION RANGE AND SPEED should fit to application

LIMITED POWER BUDGET for battery operated devices

LOW COMMUNICATION SPEED (LPWANs)
- higher power consumption
- higher latencies

Legal

OUTPUT POWER LIMITS
Increasing sensitivity to extend range = decreasing immunity to noise

VERY LOW COMMUNICATION SPEED
Legal limits for duty cycle disable more frequent communication
Limits number of packets per hour

Application concerns

MATURITY and AVAILABILITY

Why the IQRF®?

Helps to overcome recognized limitations

Technical

NO (or not efficient) BIDIRECTIONAL COMMUNICATION:
- Cannot be used for control systems
- Maintenance issues, no remote configuration or upgrades
- Problem with security: no security updates available

NO ROUTING (= NO MESH SUPPORT)
- Not covering “difficult” areas (deep indoor, obstacles, …)

COMMUNICATION RANGE AND SPEED should fit to application

LIMITED POWER BUDGET for battery operated devices

LOW COMMUNICATION SPEED (LPWANs)
- higher power consumption
- higher latencies

Legal

OUTPUT POWER LIMITS
Increasing sensitivity to extend range = decreasing immunity to noise

VERY LOW COMMUNICATION SPEED
Legal limits for duty cycle disable more frequent communication
Limits number of packets per hour

Application concerns

MATURITY and AVAILABILITY

The world has (re)discovered the beauty and urgency of wireless mesh networks.

Fast growing ecosystem
from protocols through products to any cloud

Open and fully documented
every piece of hardware or software and all protocols

Technical uniqueness

huge IP is protected by 50+ patents and trademarks

Industrial reliability
thanks to unique IQMESH® routing protocol

IQRF True Low Power
assure years on a battery when needed
orders less consumption per byte vs. LPWANs

Interoperability
integrators can easily combine all products
interoperability lever effect

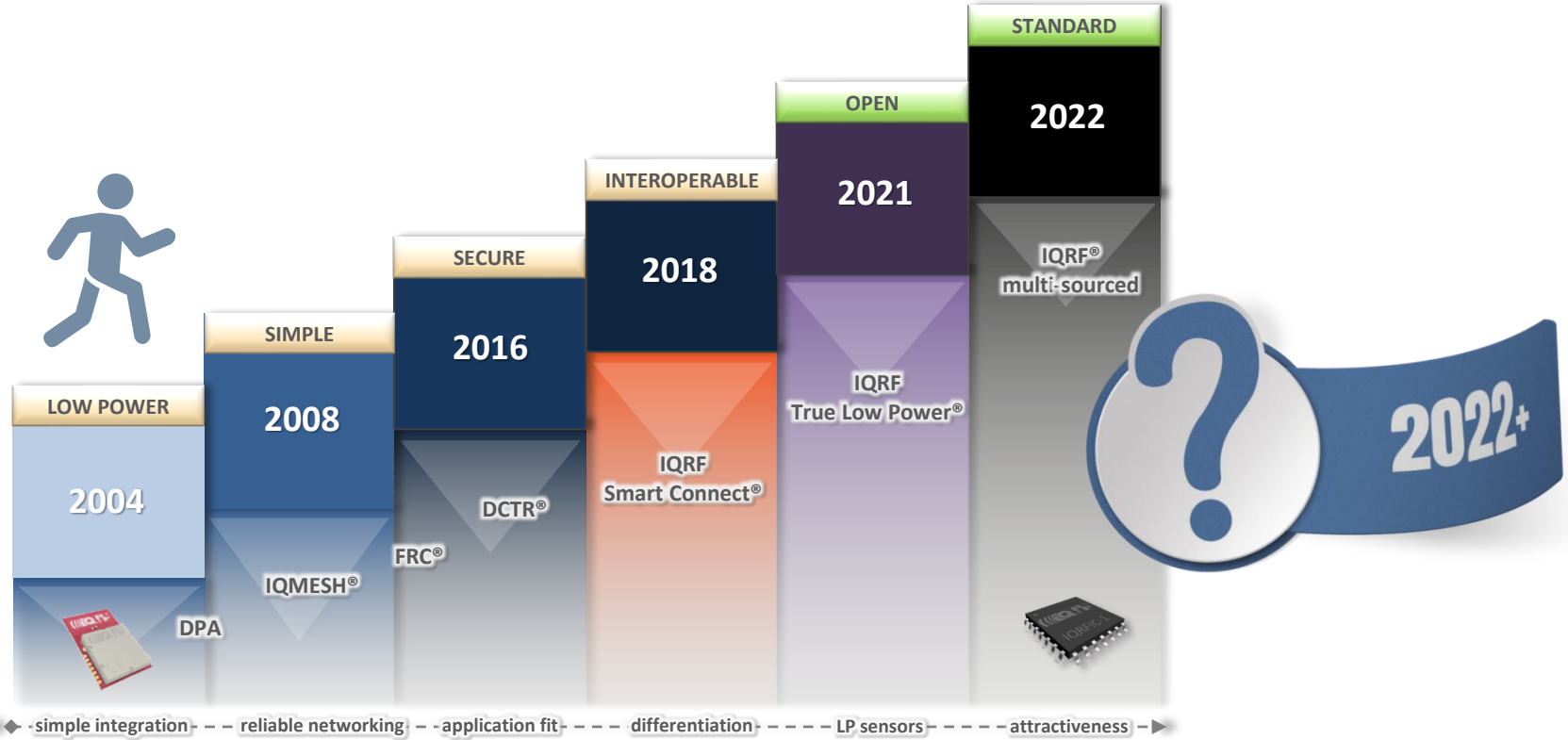
Simple integration
adding wireless connectivity to any device

Ultimate security
based on standards, automatic, multilayered

The IQRF® delivers industrial reliability and overcomes many limitations thanks to the unique IQMESH® routing protocol since 2004

Smarter wireless. Simply.

IQRF® on the timeline …



IQRF® mission is to deliver LOW POWER , SIMPLE, SECURE and INTEROPERABLE WIRELESS MESH connectivity for IoT.

Smarter wireless. Simply.

What is the IQRF®, its **Positioning** and **Why** to adopt it

Industrial Reliability and protocols behind: IQMESH®, FRC®

IQRF True Low Power® and protocols behind: beaming + offline FRC + local FRC

Interoperability / Simple integration: IQRF Data Controlled Transceivers®

Ultimate security: every single detail matters

Open and fully documented: … simply visit www.iqrf.org

So, where is the IQRF® going to?

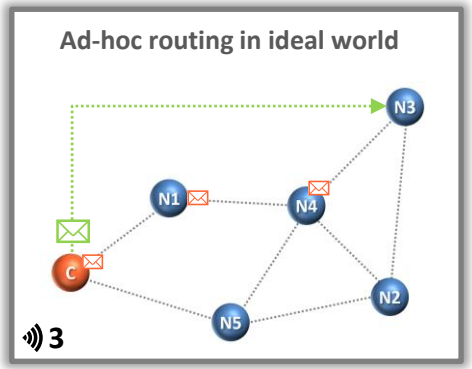
Wireless mesh networks as a technical challenge

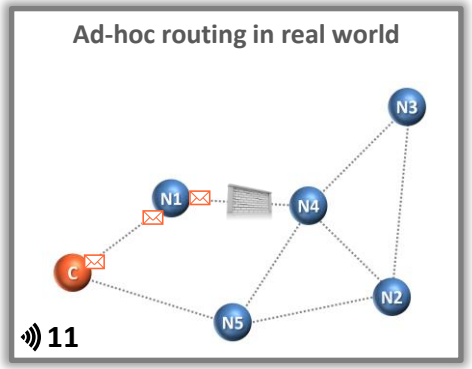
$$N_{MAX} = \frac{n\,(n-1)}{2}$$

n	N_{MAX}
2	1
3	3
4	6
5	10
6	15
100	4950
240	28680

Wireless mesh networks as a technical challenge

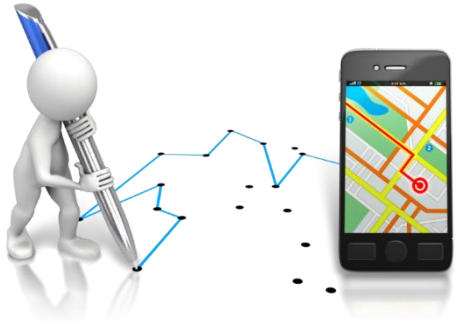
Ad-hoc routing





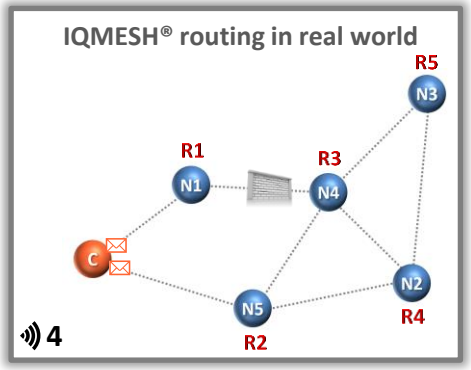
There were many tries to *optimize* routing. Source routing is just an example – looking perfectly in theory, often failing in real world.

Wireless mesh networks as a technical challenge



discovery -> NTW rearrangement
TDMA + oriented flooding

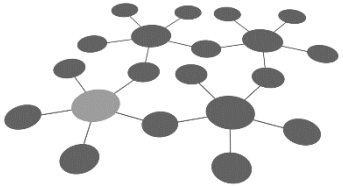
- Redundancy dramatically increases robustness
- It's simple to use and implement
- It's collision free
- It's deterministic
- No partial acknowledgments are needed
- It's proven in real applications



each routing device knows its position thanks to the VRN (Virtual Routing Number)

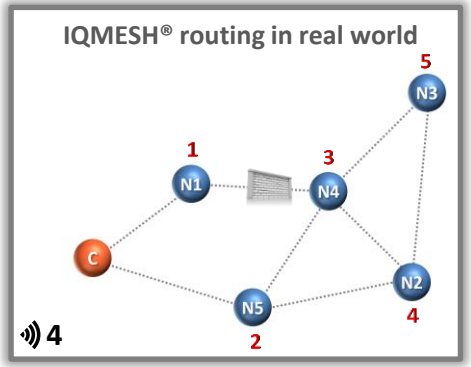
Industrial reliability thanks to the IQMESH® protocol

Industrial reliability



discovery -> NTW rearrangement
TDMA + oriented flooding

- Redundancy dramatically increases robustness
- It's simple to use and implement
- It's collision free
- It's deterministic
- No partial acknowledgments are needed
- It's proven in real applications

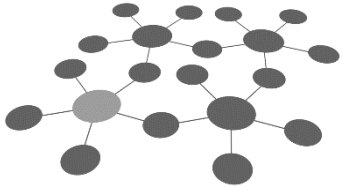


each routing device knows its position thanks to the VRN (Virtual Routing Number)

IQRF® defined totally new level of industrial reliability for wireless mesh networks. It is basically assured directly by the routing protocol.

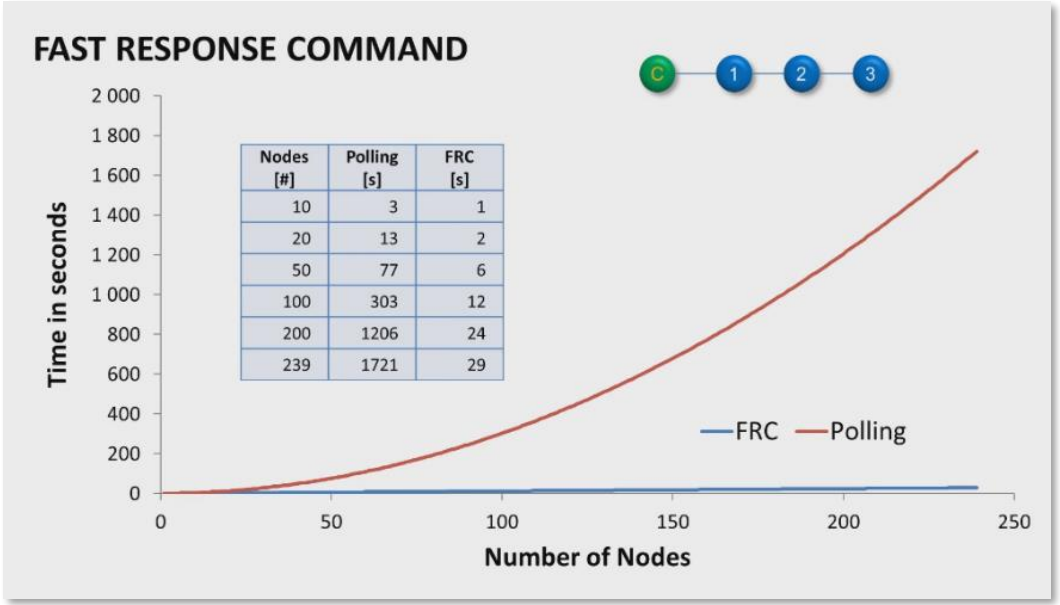
Industrial reliability thanks to the FRC® protocol

Industrial reliability



FRC - Fast Response commands®

- It's unique and patented (EU, USA, CN, JP)
- It deploys IQMESH® configuration
- Further dramatically increases robustness
- It linearizes exponential time for dummy polling
- ~3*N time slots only
- It's a great tool for network maintenance

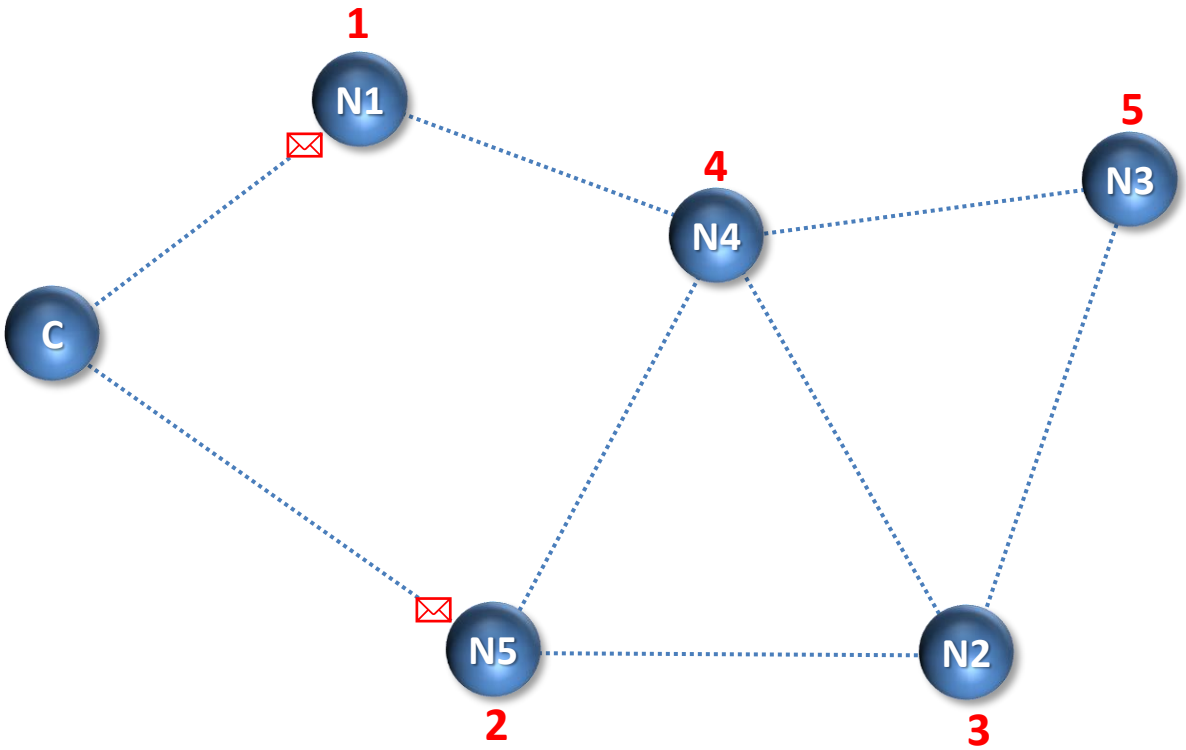


Nodes [#]	Polling [s]	FRC [s]
10	3	1
20	13	2
50	77	6
100	303	12
200	1206	24
239	1721	29

FRC – Fast response commands® further increases reliability and robustness thanks to the broadcast acknowledgments and dramatically speed up data aggregation.

Smarter wireless. Simply.

Industrial reliability thanks to the FRC® protocol



✉					
C	1	2	3	4	5

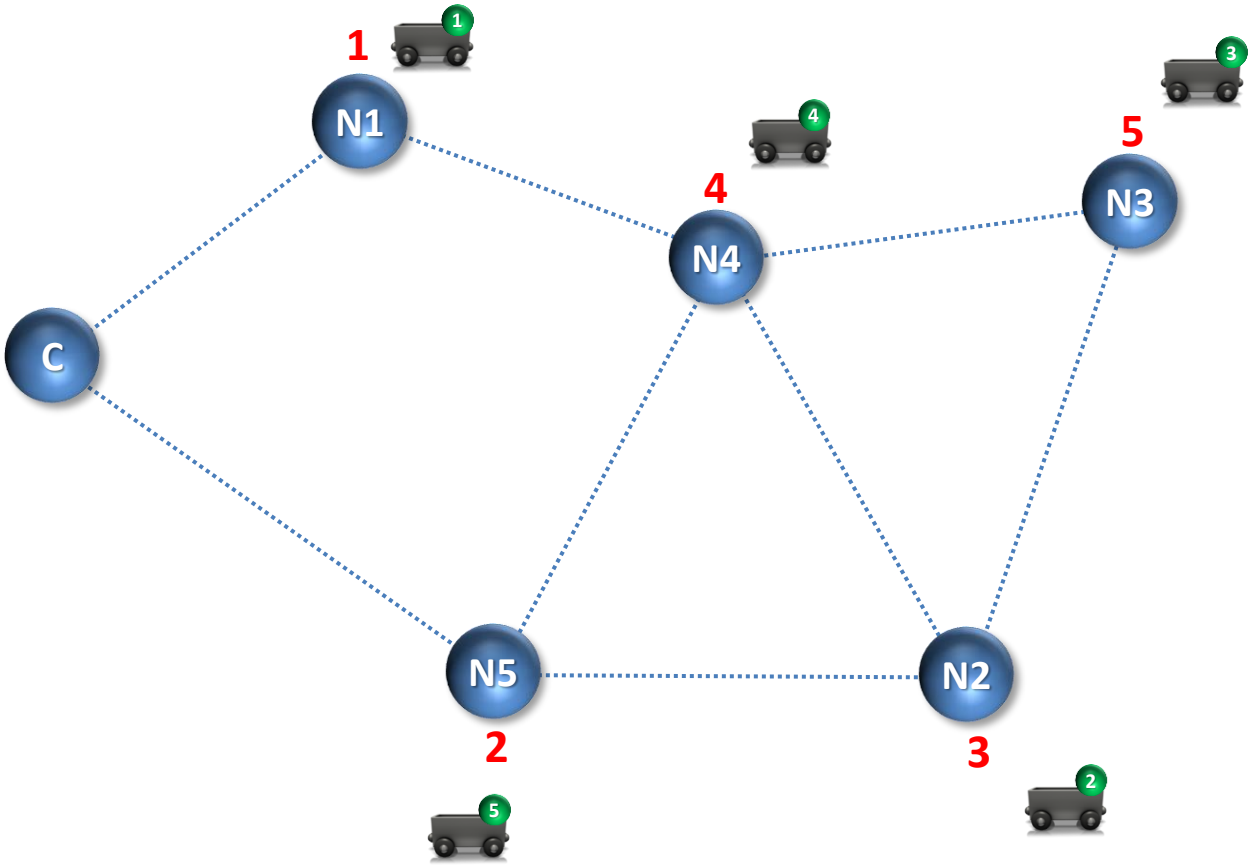
50 ms / hop

300 ms
timer

FRC® PHASES

- Broadcast FRC request
- Send data locally
- Aggregation

Industrial reliability thanks to the FRC® protocol



30 ms / addressed node

300 ms
timer

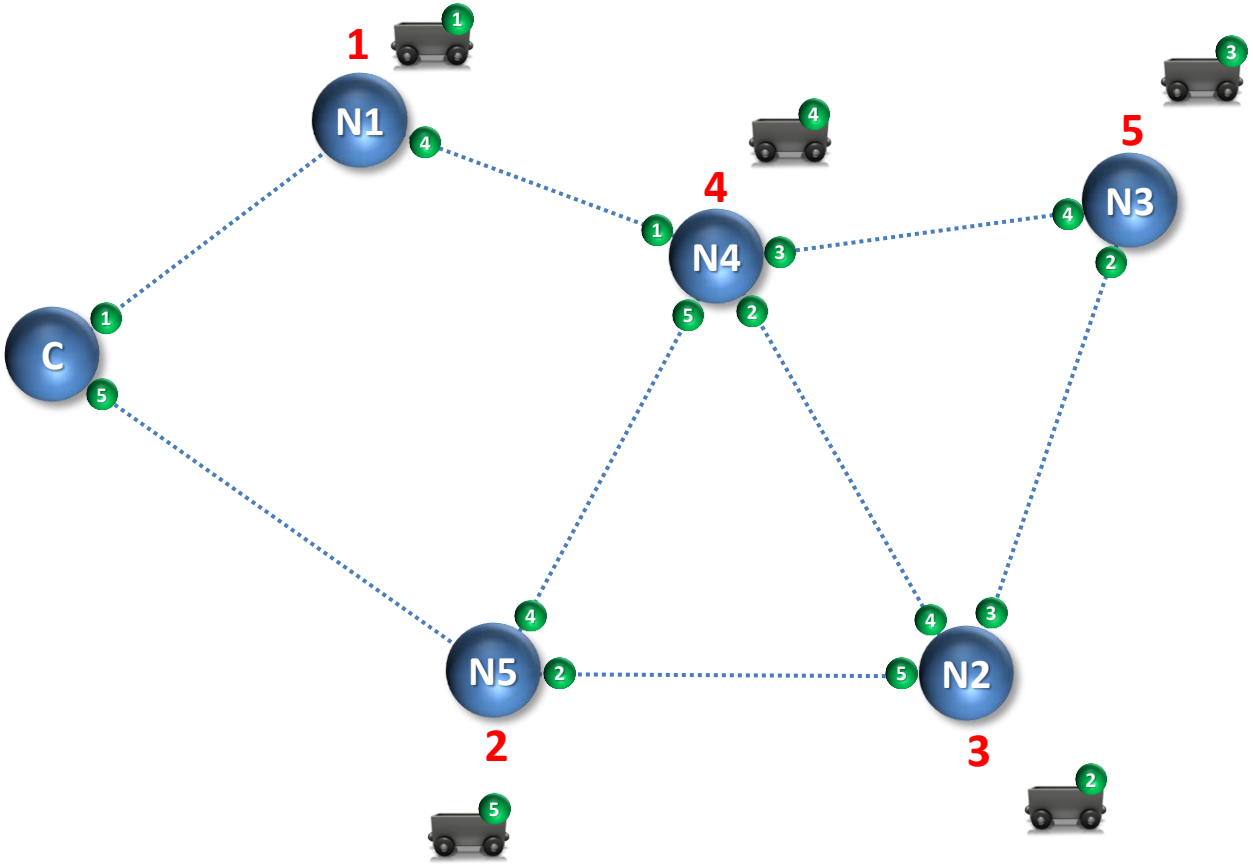
FRC® PHASES

Broadcast FRC request

Send data locally

Aggregation

Industrial reliability thanks to the FRC® protocol



30 ms / addressed node

450 ms
timer

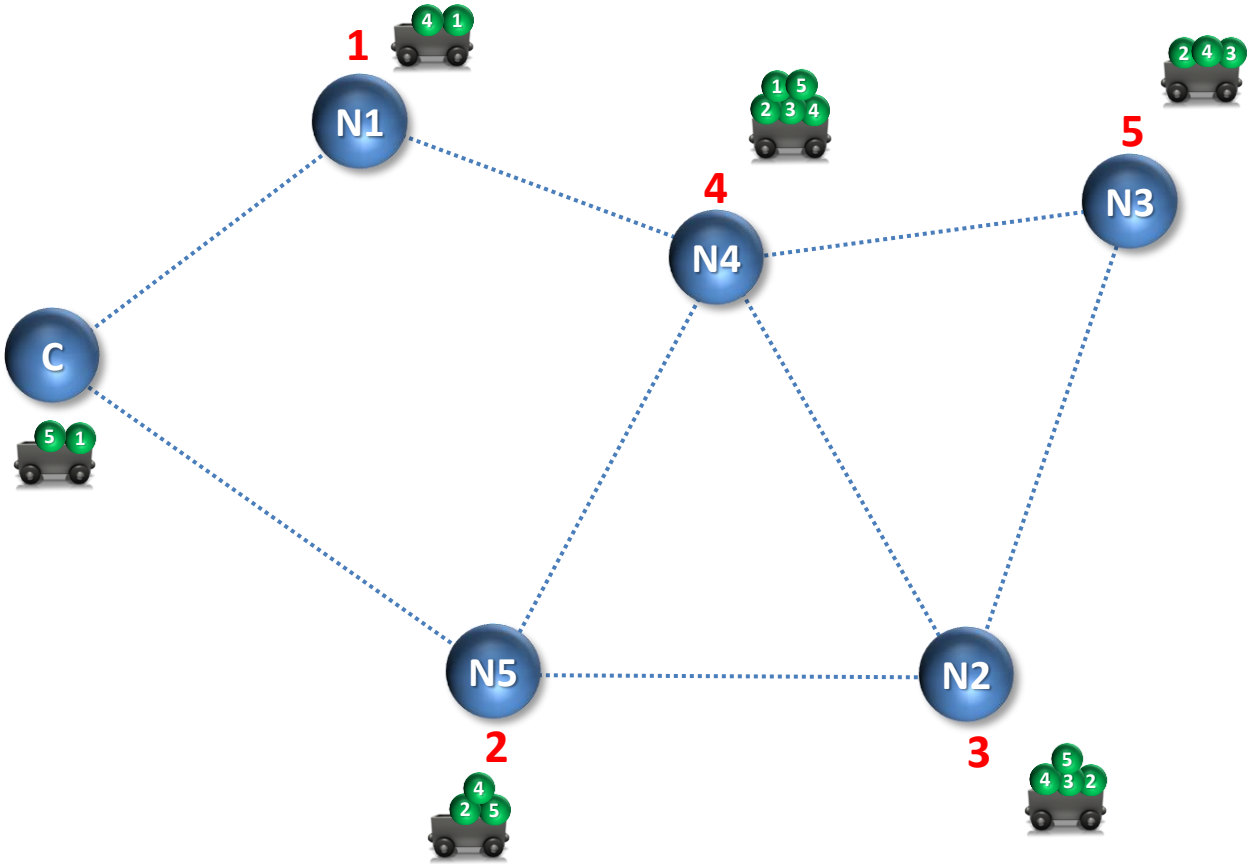
FRC® PHASES

Broadcast FRC request

Send data locally

Aggregation

Industrial reliability thanks to the FRC® protocol



450 ms
timer

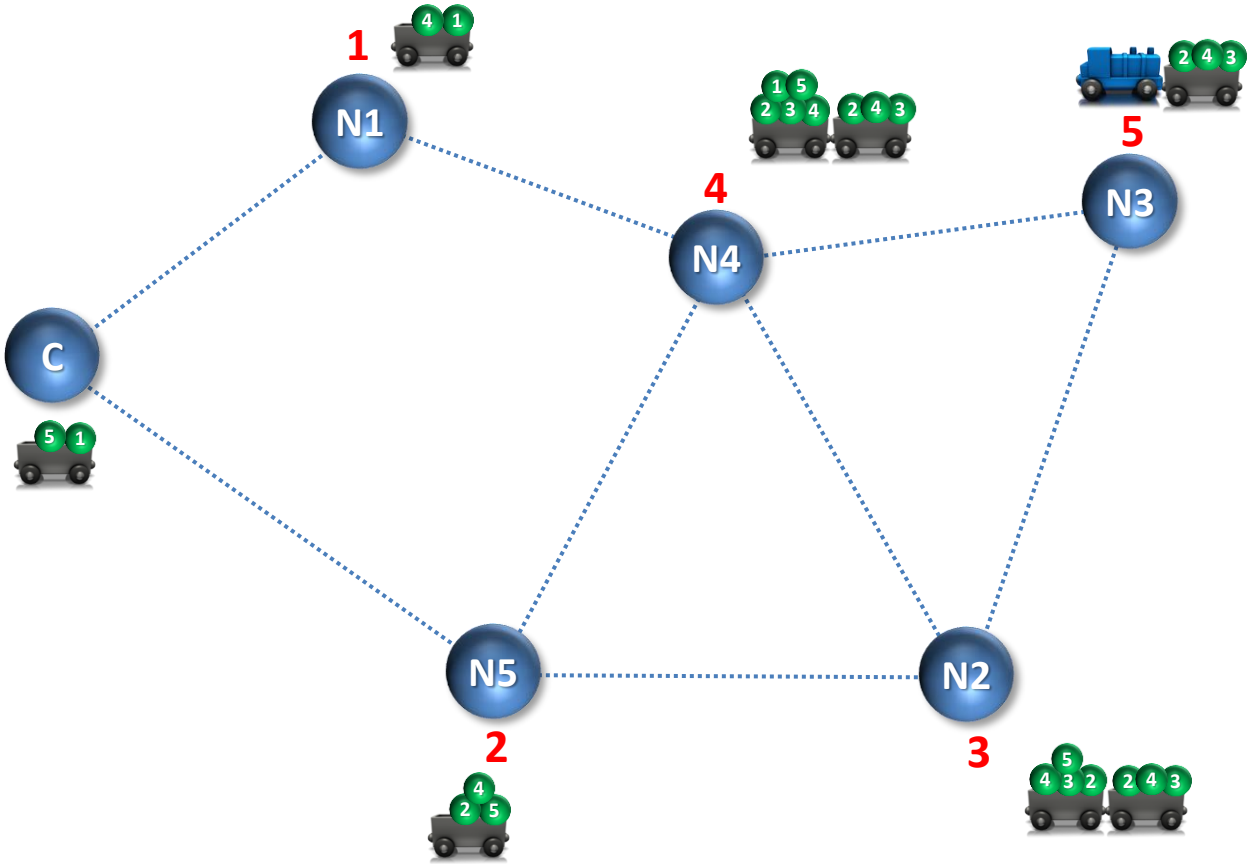
FRC® PHASES

Broadcast FRC request

Send data locally

Aggregation

Industrial reliability thanks to the FRC® protocol



60 ms / routing node

510 ms
timer

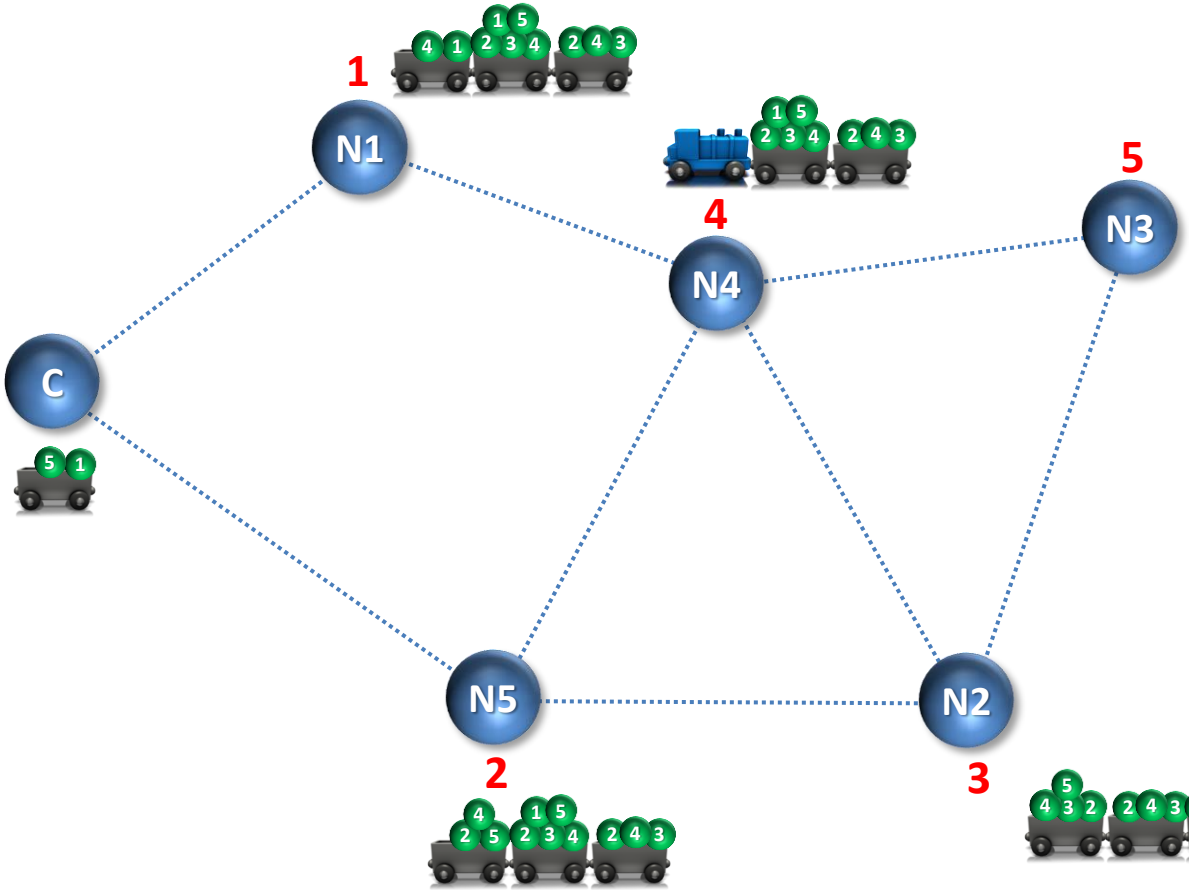
FRC® PHASES

Broadcast FRC request

Send data locally

Aggregation

Industrial reliability thanks to the FRC® protocol



60 ms / routing node

570 ms
timer

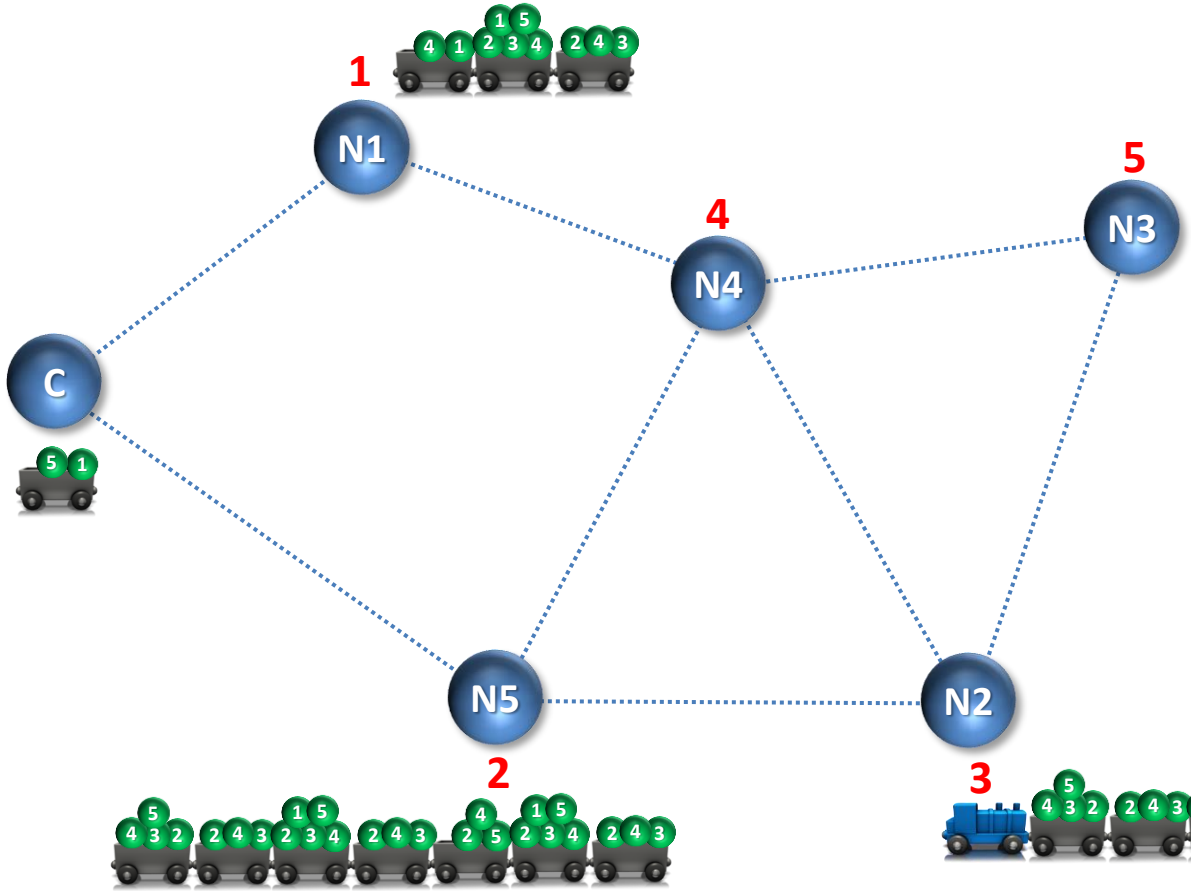
FRC® PHASES

Broadcast FRC request

Send data locally

Aggregation

Industrial reliability thanks to the FRC® protocol



60 ms / routing node

630 ms
timer

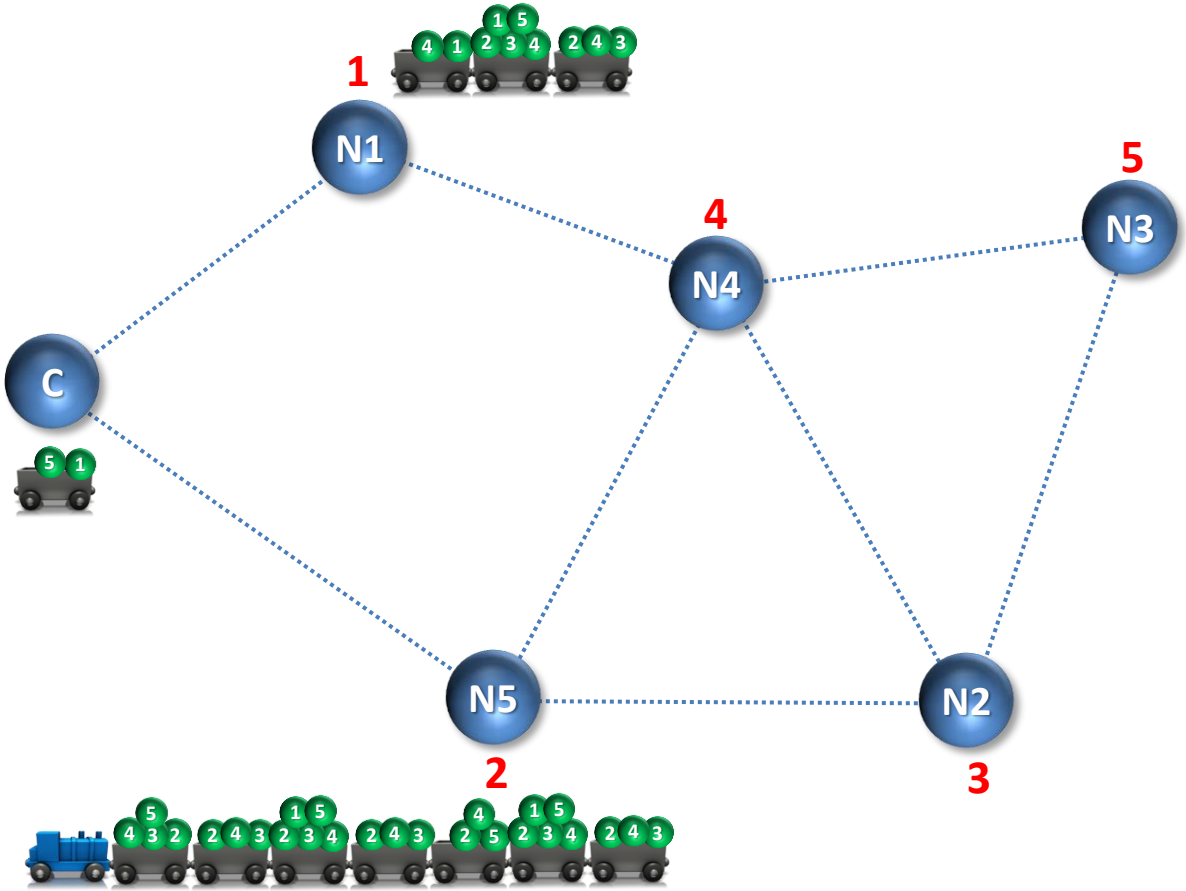
FRC® PHASES

Broadcast FRC request

Send data locally

Aggregation

Industrial reliability thanks to the FRC® protocol



60 ms / routing node

690 ms
timer

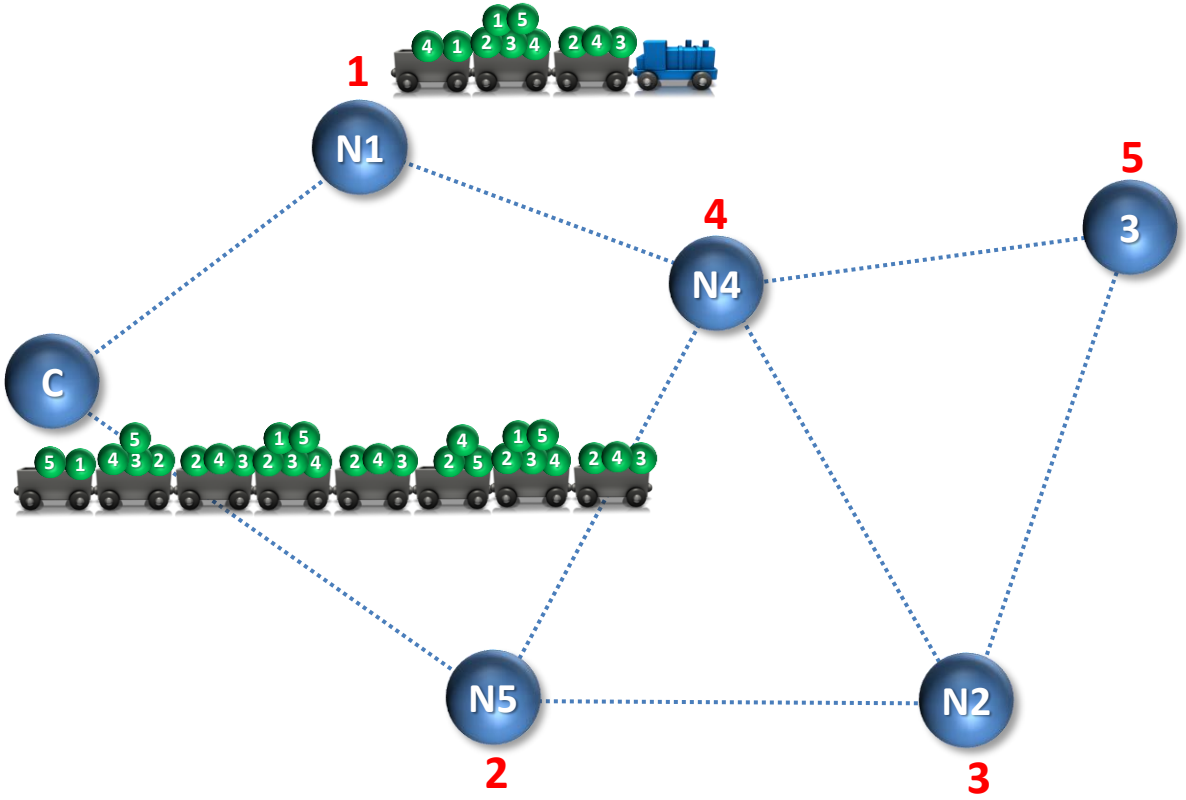
FRC® PHASES

Broadcast FRC request

Send data locally

Aggregation

Industrial reliability thanks to the FRC® protocol



60 ms / routing node

750 ms
timer

FRC® PHASES

Broadcast FRC request

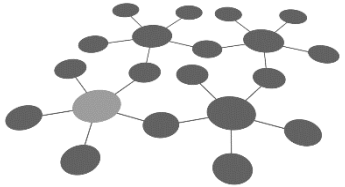
Send data locally

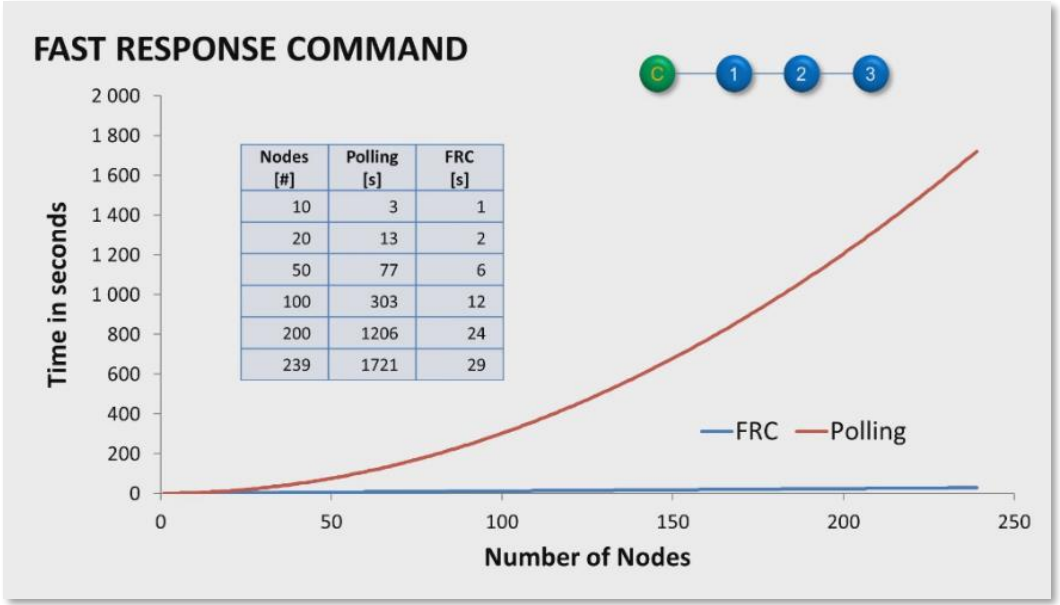
Aggregation

Industrial reliability thanks to the FRC® protocol

https://doc.iqrf.org/DpaTechGuide/misc/IqMeshTiming.htm

Industrial reliability





Nodes [#]	Polling [s]	FRC [s]
10	3	1
20	13	2
50	77	6
100	303	12
200	1206	24
239	1721	29

FRC - Fast Response commands®

- It's unique and patented (EU, USA, CN, JP)
- It deploys IQMESH® configuration
- Further dramatically increases robustness
- It linearizes exponential time for dummy polling
- ~3*N time slots only
- It's a great tool for network maintenance

FRC – Fast response commands® further increases reliability and robustness thanks to the broadcast acknowledgments and dramatically speed up data aggregation.

What is the IQRF®, its **Positioning** and **Why** to adopt it

Industrial Reliability and protocols behind: IQMESH®, FRC®

IQRF True Low Power® and protocols behind: beaming + offline FRC + local FRC

Interoperability / Simple integration: IQRF Data Controlled Transceivers®

Ultimate security: every single detail matters

Open and fully documented: … simply visit www.iqrf.org

So, where is the IQRF® going to?

IQRF True Low Power®

TR-76D power consumption example

- Deep sleep mode: **< 100 nA**
- Run mode
  - RF sleep: 1.6 mA
  - RF ready: 3.0 mA
- TX mode: **8.3 - 19 mA**
- Sleep mode: **< 1 µA**
- RX mode
  - STD: 12.3 mA
  - LP: **233 µA**
  - XLP: **15 µA**

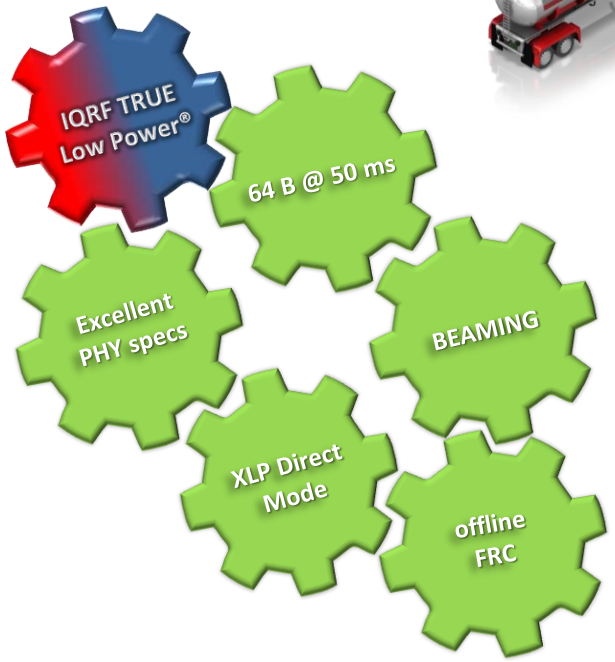
Look at other RF platforms boasting ultra/extra low power.

IQRF **lifetime** * for 1 Ah, 3.6 V, ½ AA sized battery:

- **1000 years** in Deep **sleep**
- **7 years** continually **receiving** in XLP **
- **300 MB** data **received**
- **200 MB** data **transmitted** (at highest RF output power)

* *Theoretical values*

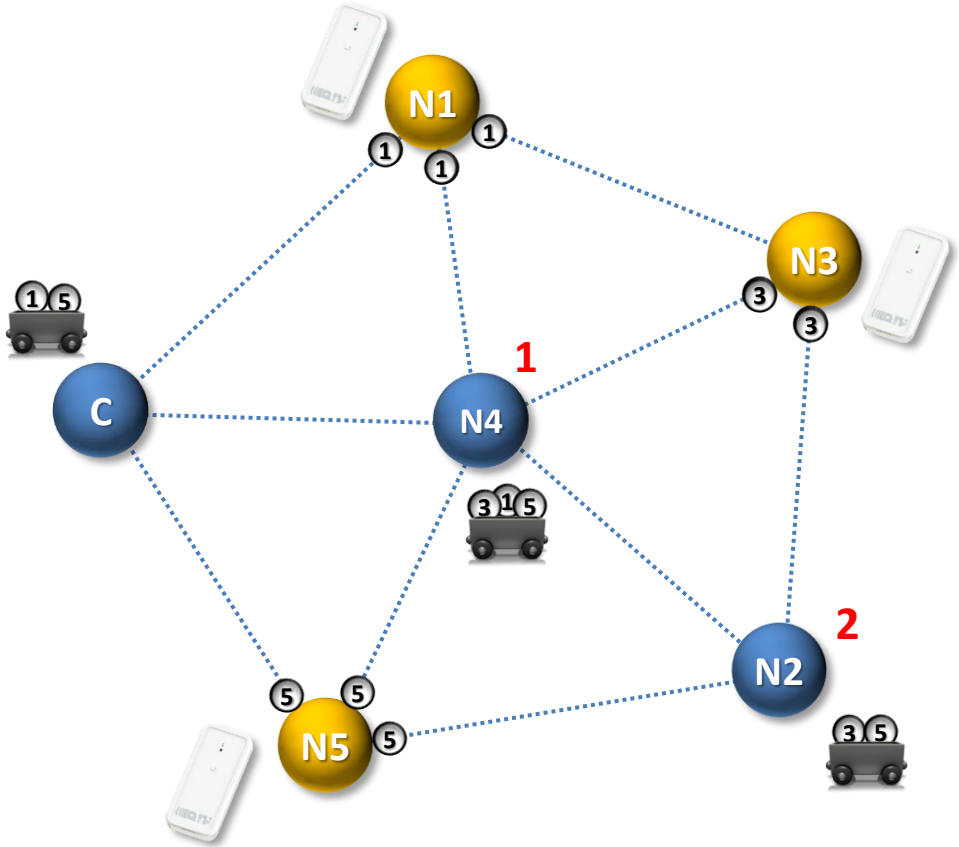
** *Without an incoming RF signal including a noise*



Sensors

- Sending data **regularly, as needed**
- Life expectancy: years
- **True life expectancy: millions of packets**
- AES 128b encryption

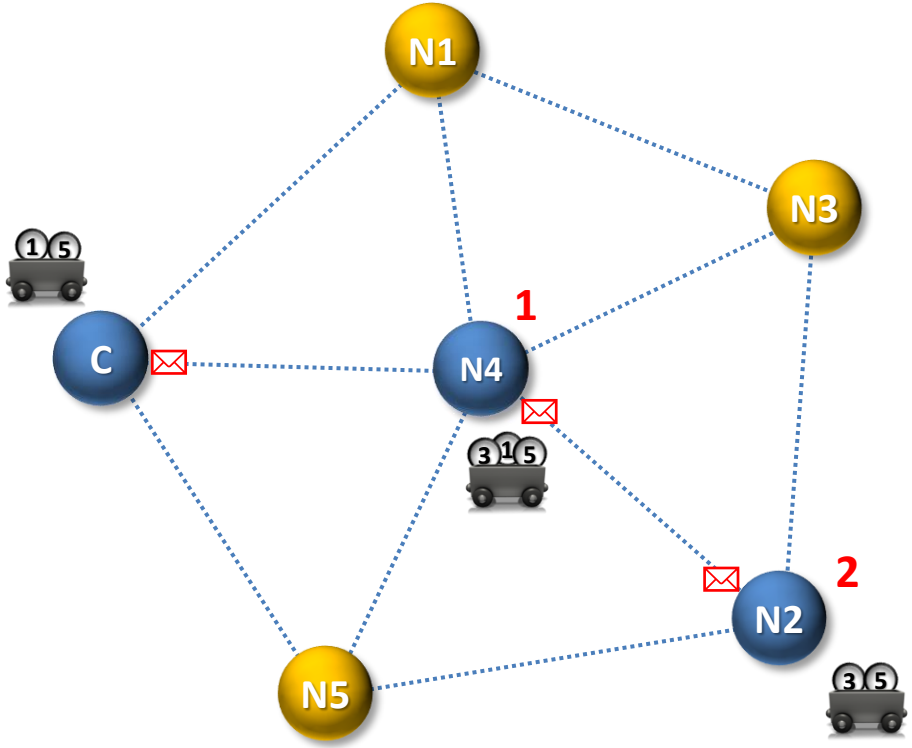
BEAMING in detail



Data are sent periodically

… and logged on repeaters

offline FRC in detail

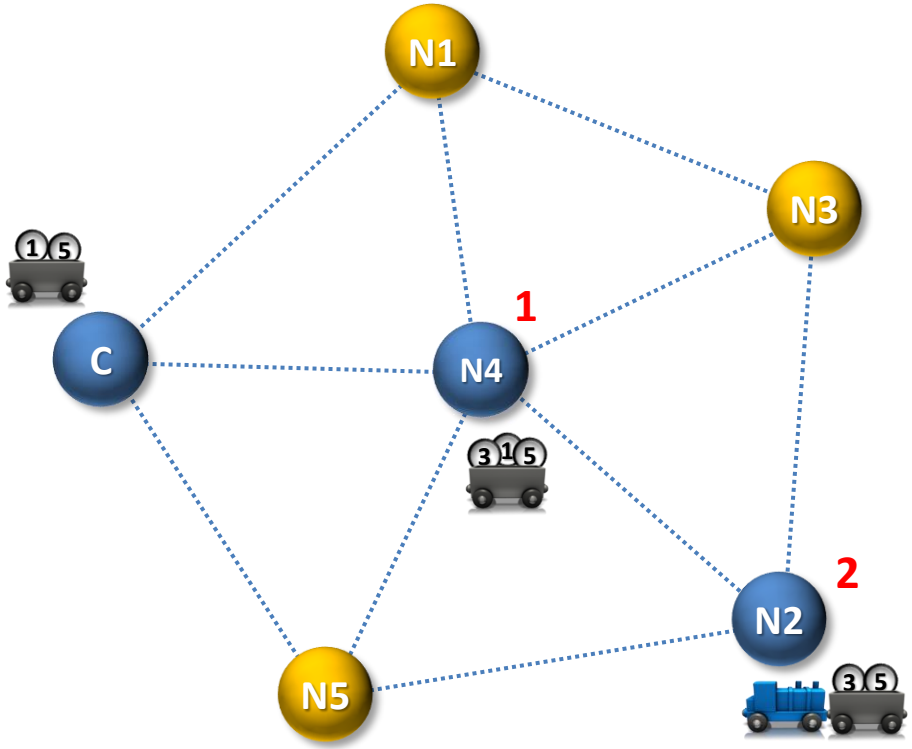


Data from sensors are available
(logged on repeaters)

offline FRC® PHASES

- **Broadcast FRC request**
- ~~Send data locally~~
- **Aggregation**

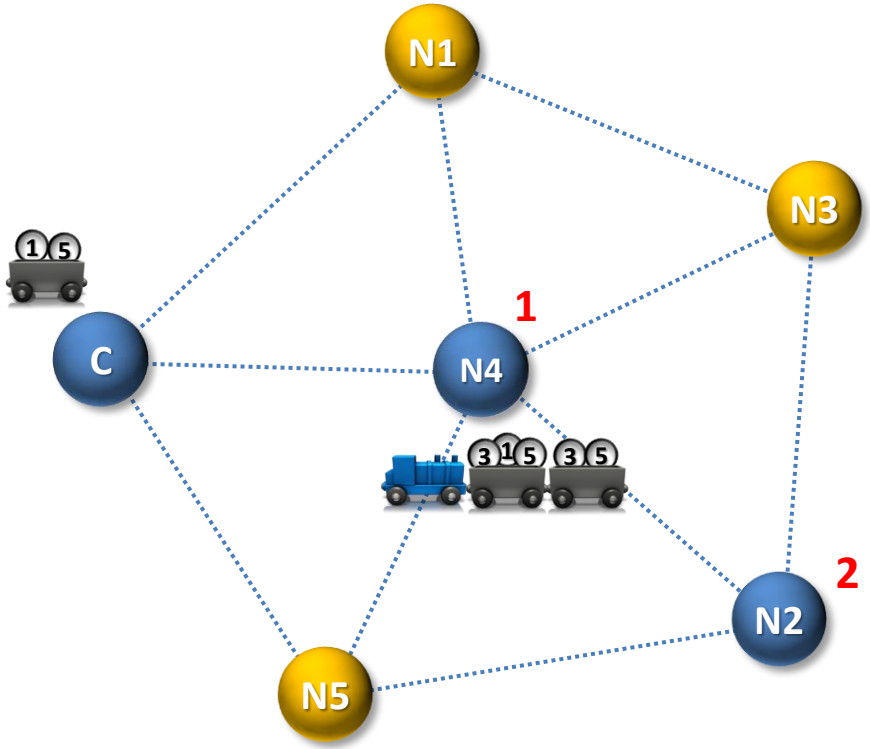
offline FRC in detail



offline FRC® PHASES

- Broadcast FRC request
- ~~Send data locally~~
- **Aggregation**

offline FRC in detail



offline FRC® PHASES

Broadcast FRC request

~~Send data locally~~

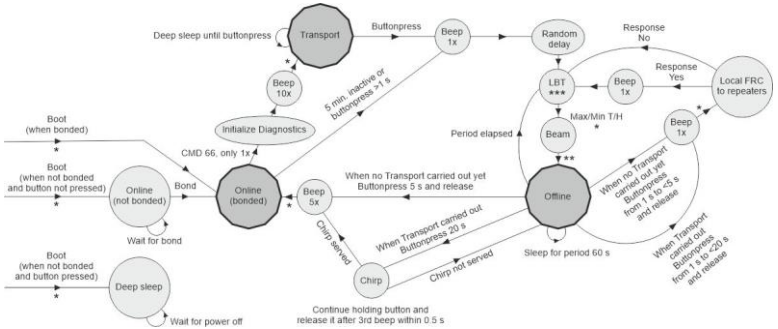
Aggregation

IQRF True Low Power®

Real example

Industrial T + rH sensor

- Battery: 1x $LiSClO_2$ AA size
- Sending complete data **every 1 minute**
- Life expectancy: **10+ years**
- **True life expectancy: >10.000.000 packets**
- 500+ MB
- Standard network encryption



What is the IQRF®, its **Positioning** and **Why** to adopt it

Industrial Reliability and protocols behind: IQMESH®, FRC®

IQRF True Low Power® and protocols behind: beaming + offline FRC + local FRC

Interoperability / Simple integration: IQRF Data Controlled Transceivers®

Ultimate security: every single detail matters

Open and fully documented: … simply visit www.iqrf.org

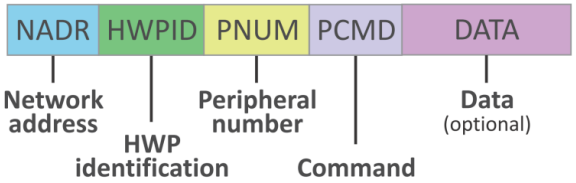
So, where is the IQRF® going to?

Interoperability simplifies design and enables global cooperation

Interoperability

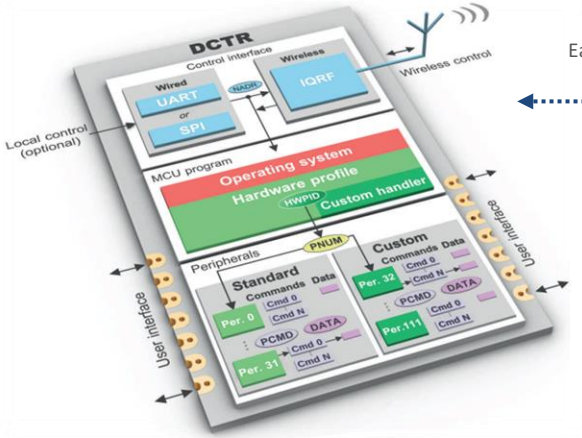
Simple integration

IQRF® DPA Command

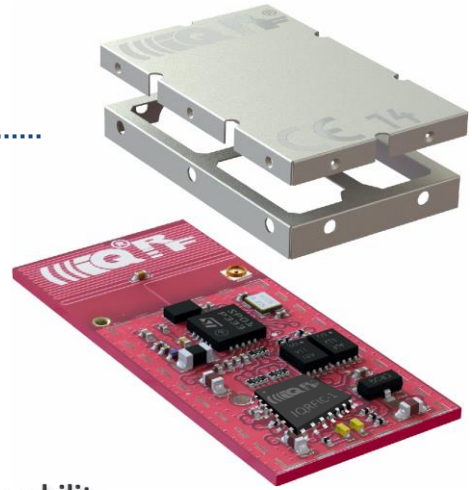


- IQRF® OS is built-in at each IC/TR
- IQRF® DPA is available as a SW plugin
- DPA plugins are Plug & Play
- DPA plugins are free of charge
- Further customizable via Custom handler
- **Dramatically shorten development phase**

IQRF Data Controlled Transceivers®



Each peripheral / service on any device is simply available by sending of DPA Commands, **without programming.**



IQRF OS assures physical & IQRF DPA application interoperability

IQRF Data Controlled Transceivers® dramatically shorten development phase. This results in huge savings and products come to the market much earlier.

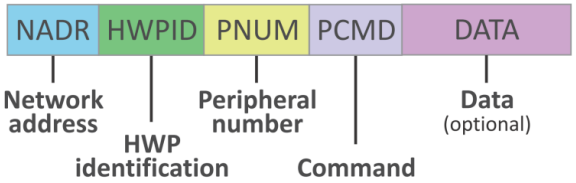
Smarter wireless. Simply.

Interoperability simplifies design and enables global cooperation

Interoperability

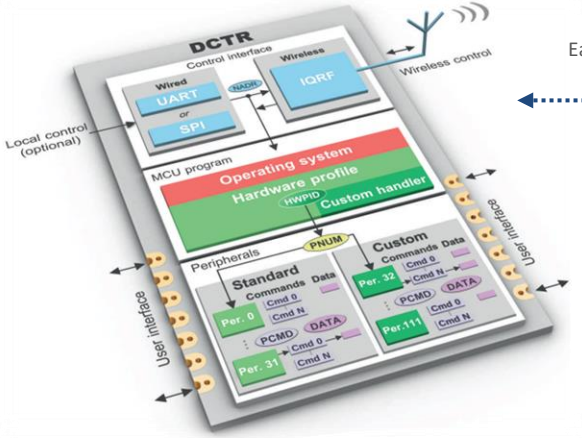
Simple integration

IQRF® DPA Command



- IQRF® OS is built-in at each IC/TR
- IQRF® DPA is available as a SW plugin
- DPA plugins are Plug & Play
- DPA plugins are free of charge
- Further customizable via Custom handler
- **Dramatically shorten development phase**

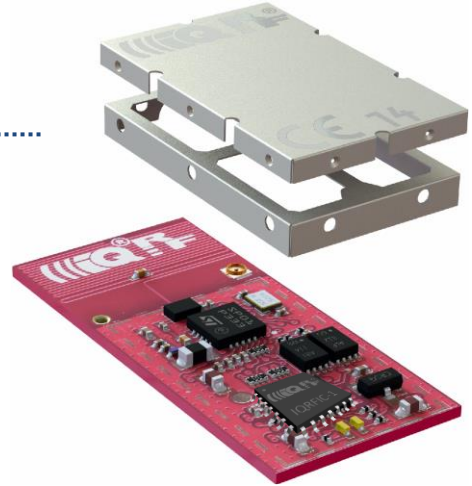
IQRF Data Controlled Transceivers®



Each peripheral / service on any device is simply available by sending of DPA Commands, **without programming.**

Physical interoperability 2022+

1. DCTR modules
2. IQRF® ICs with PHY
3. IQRF® PHY SW stacks for major MCU platforms
3. IQRF® open standard



IQRF Data Controlled Transceivers® dramatically shorten development phase. This results in huge savings and products come to the market much earlier.

Smarter wireless. Simply.

What is the IQRF®, its **Positioning** and **Why** to adopt it

Industrial Reliability and protocols behind: IQMESH®, FRC®

IQRF True Low Power® and protocols behind: beaming + offline FRC + local FRC

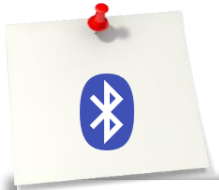
Interoperability / Simple integration: IQRF Data Controlled Transceivers®

Ultimate security: every single detail matters

Open and fully documented: … simply visit www.iqrf.org

So, where is the IQRF® going to?

SECURITY is a must and an added value for IoT



IoT Goes Nuclear:
Creating a ZigBee Chain Reaction

Eyal Ronen(✉)*, Colin O'Flynn†, Adi Shamir* and Achi-Or Weingarten*
*Weizmann Institute of Science, Rehovot, Israel
{eyal.ronen,adi.shamir}@weizmann.ac.il
†Dalhousie University, Halifax, Canada
coflynn@dal.ca

PART OF A ZDNET SPECIAL FEATURE: SECURING YOUR MOBILE ENTERPRISE

Security flaws put billions of Bluetooth phones, devices at risk

It's thought to be the most widescale set of vulnerabilities based on the number of devices affected, hitting Windows desktops, Android devices, older iPhones and iPads, and smart devices.

By Zack Whittaker for Zero Day | September 12, 2017 -- 13:00 GMT (14:00 BST) | Topic: Securing Your Mobile Enterprise

Wired Equivalent Privacy (WEP)

Many security flaws

Wi-Fi Protected Access (WPA)

PSK + TKIP

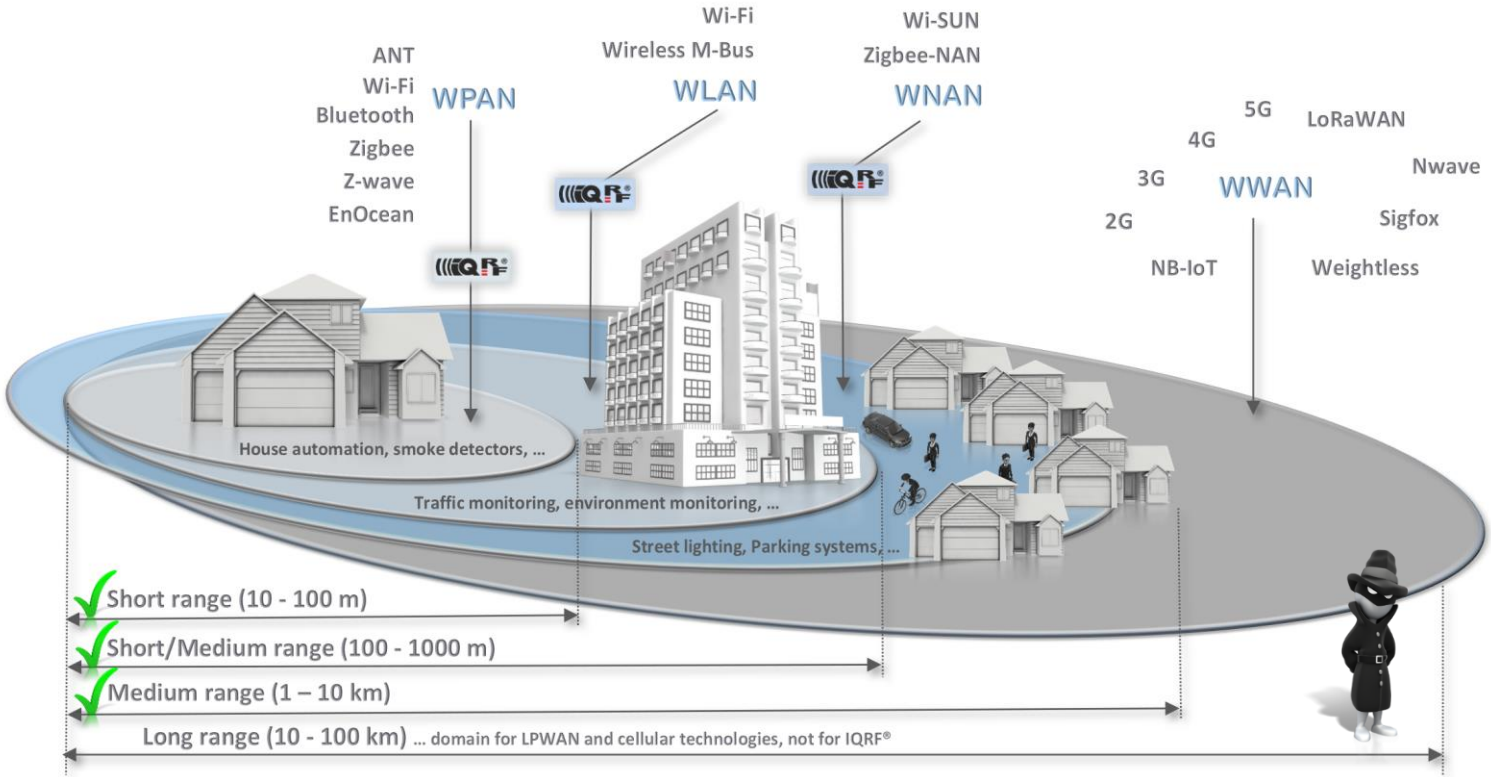
Wi-Fi Protected Access version 2 (WPA2)

AES encryption added

Wi-Fi WPS vulnerability (2011)

Protocol flaw degraded combinations number from 10M to 11k

SECURITY is a must and an added value for IoT



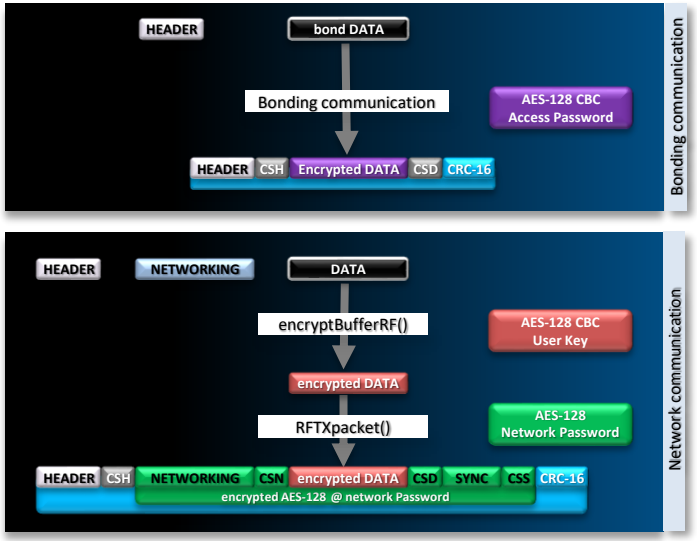
SECURITY is a must and an added value for IoT

Based on standards (AES-128, CBC)

IQRF® DPA OTA: configuration, updates

2004 – 2021: 0.5+ Mpcs devices running in the field

No golden keys, network passwords, multilayered security



- Multi-layer & forced security based on standards
- Complexity, understandability, simplicity
- Secure keys management
- System security local isolation

THREATS

Shared medium

Analyzing and hacking tools availability

~~Proprietary protocols~~

~~Not secure or not available updates~~

~~Green technologies are not proven~~

~~Inconsistences and compromises~~

~~Low complexity of the security design~~

~~Golden / fixed keys~~

What is the IQRF®, its **Positioning** and **Why** to adopt it

Industrial Reliability and protocols behind: IQMESH®, FRC®

IQRF True Low Power® and protocols behind: beaming + offline FRC + local FRC

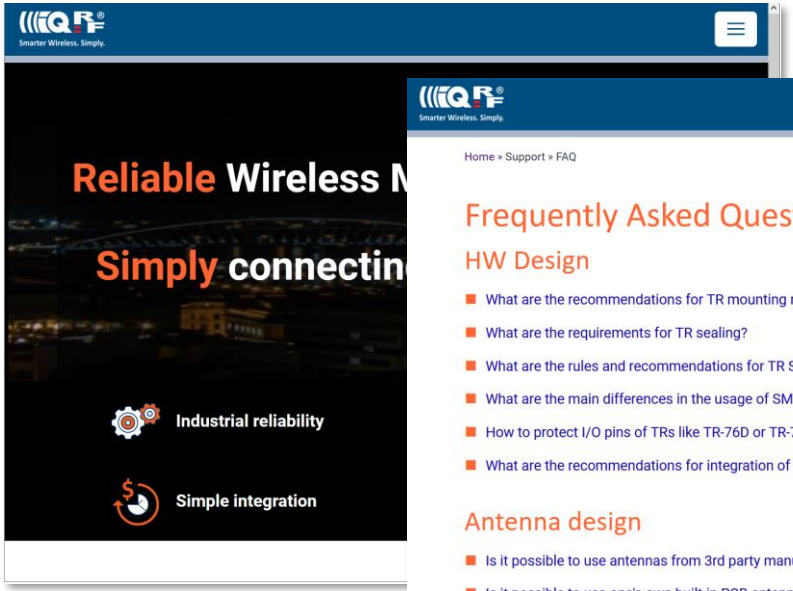
Interoperability / Simple integration: IQRF Data Controlled Transceivers®

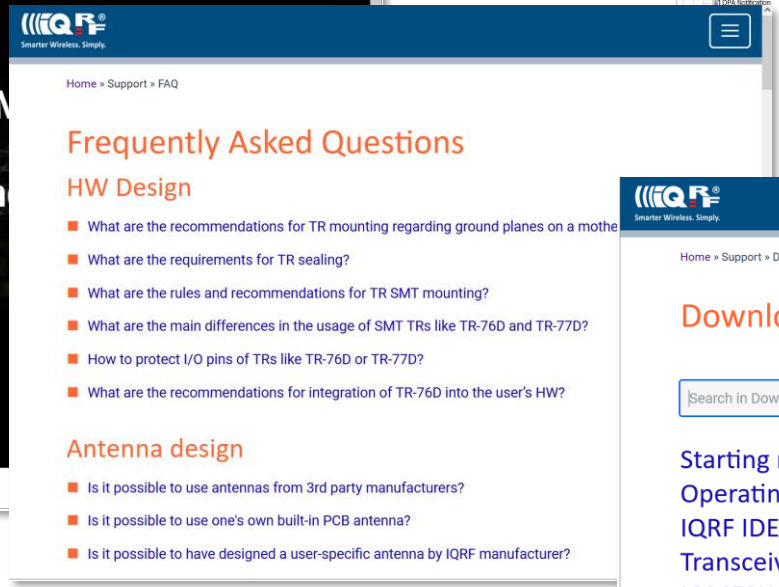
Ultimate security: every single detail matters

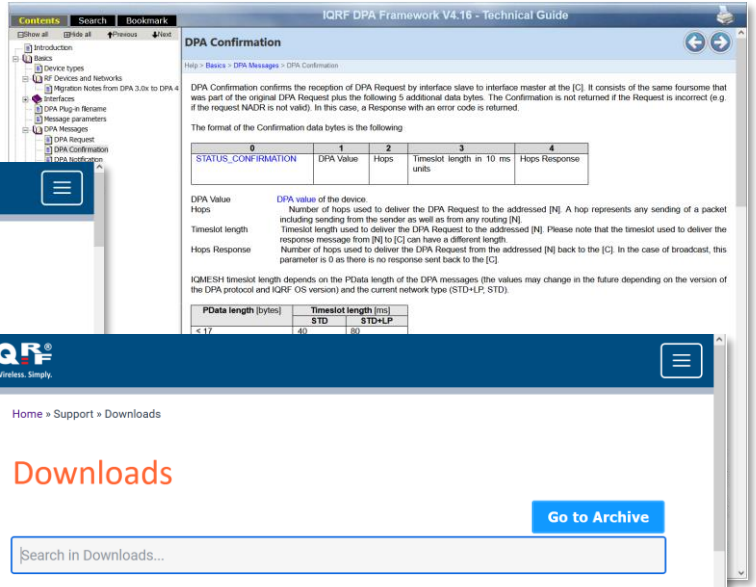
Open and fully documented: … simply visit www.iqrf.org

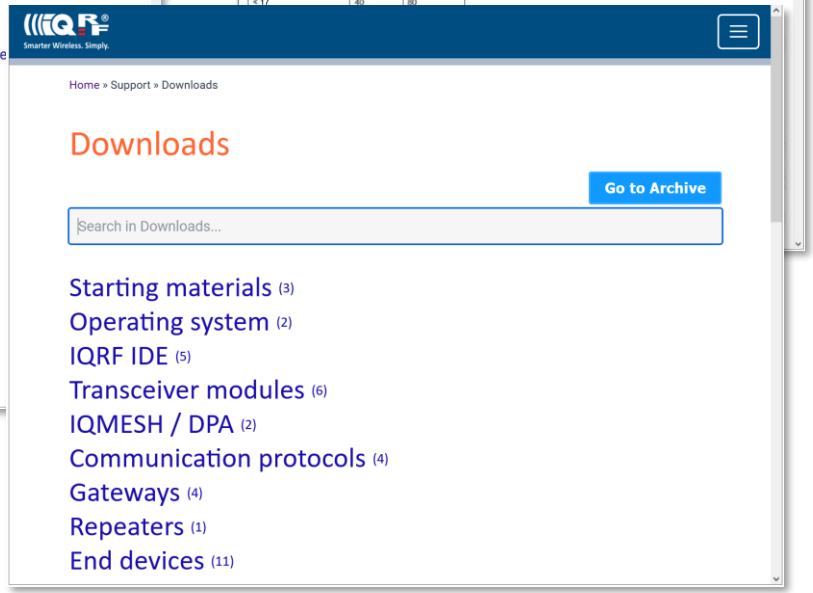
So, where is the IQRF® going to?

OPEN and fully documented









https://www.iqrf.org

https://doc.iqrf.org

What is the IQRF®, its **Positioning** and **Why** to adopt it

Industrial Reliability and protocols behind: IQMESH®, FRC®

IQRF True Low Power® and protocols behind: beaming + offline FRC + local FRC

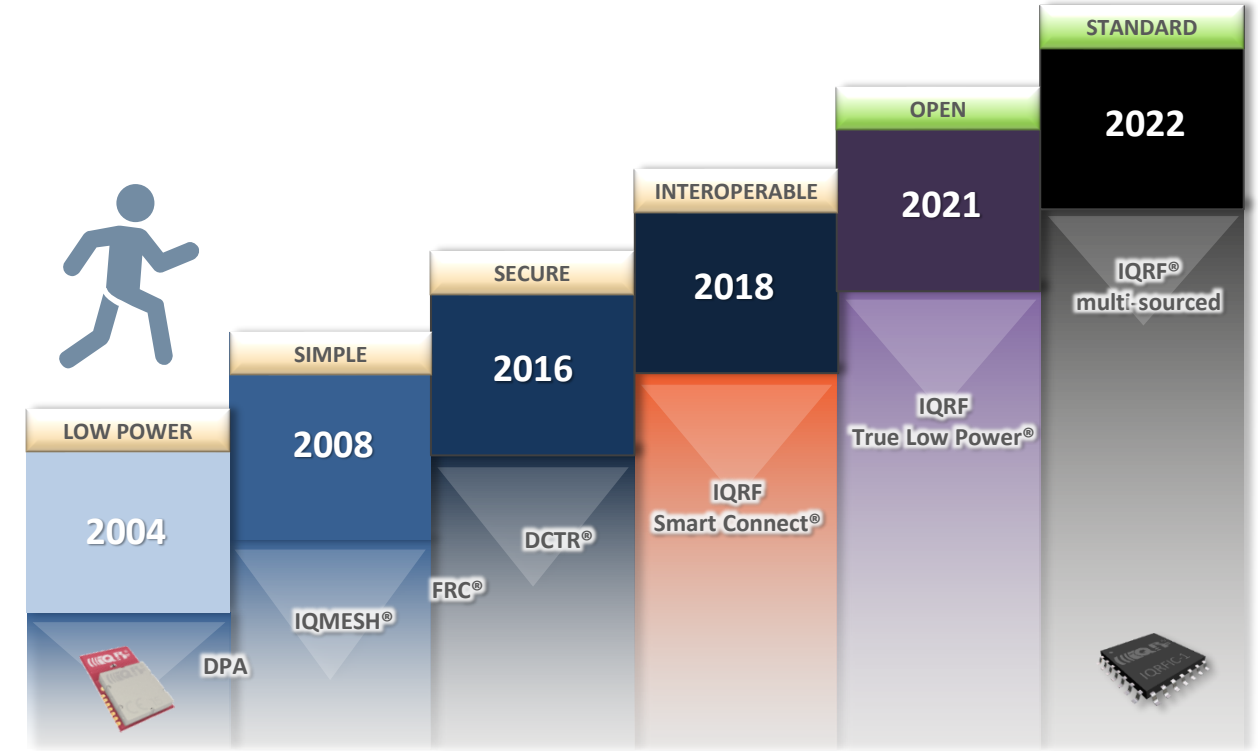
Interoperability / Simple integration: IQRF Data Controlled Transceivers®

Ultimate security: every single detail matters

Open and fully documented: … simply visit www.iqrf.org

So, where is the IQRF® going to?

Where is the IQRF® going to?



wireless mesh technology for IoT

BIG THANKS to

the IQRF team supporting our wireless mesh mission,

the IQRF Alliance members for joining our passion for the IQRF,

the Czech Ministry of Industry and Trade for financial support of the project FV40132

Thank you for your attention!

https://iqrf.org

https://iqrfAlliance.org

https://microrisc.com