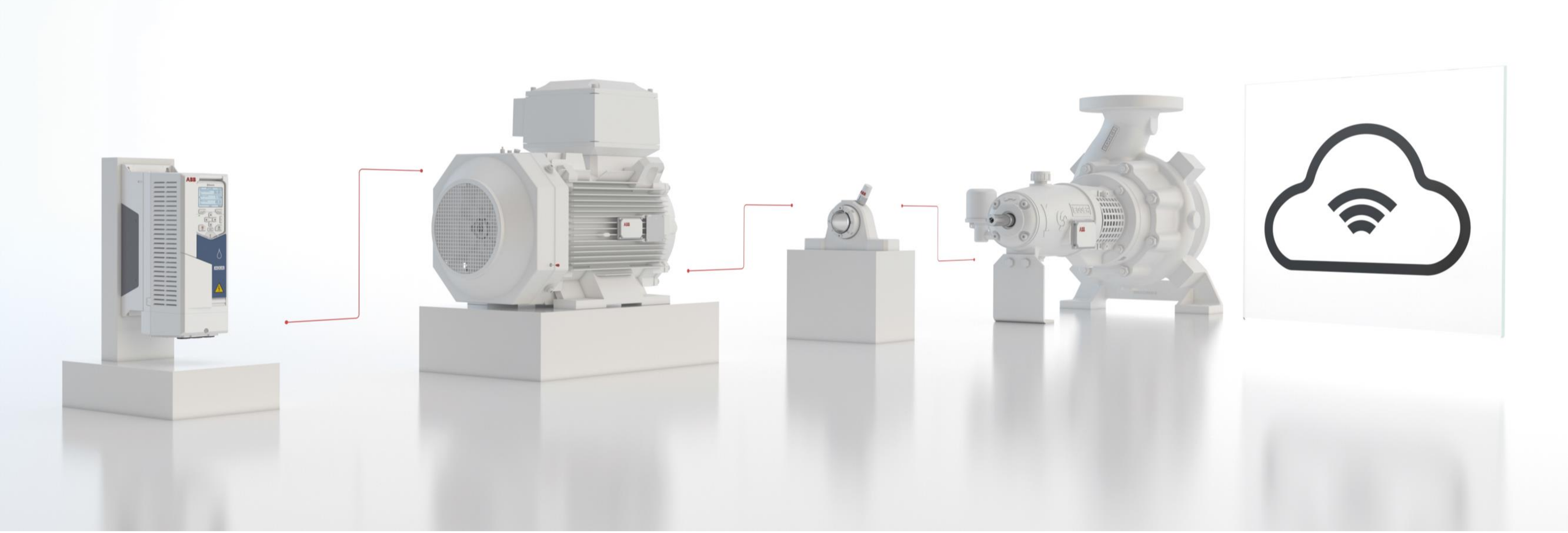
DISCLAIMER: this presentation is just my research findings and personal opinions as a researcher for academic discussions. It doesn't intend to present ABB's official roadmap or strategy in these areas.



2022-10-19

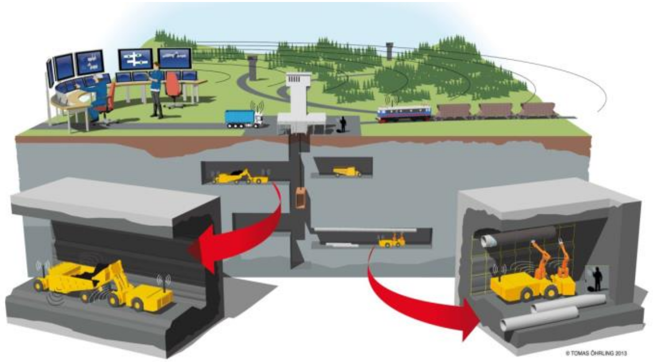
5G communication and computing for industrial control systems: where we are and directions

Zhibo Pang, Senior Principal Scientist, ABB Corporate Research Sweden (pang.zhibo@se.abb.com) / Adjunct Professor, KTH Royal Institute of Technology (zhibo@kth.se)

ABB

Wireless networks for time-critical control applications

Not just replacing cables but enabling more values

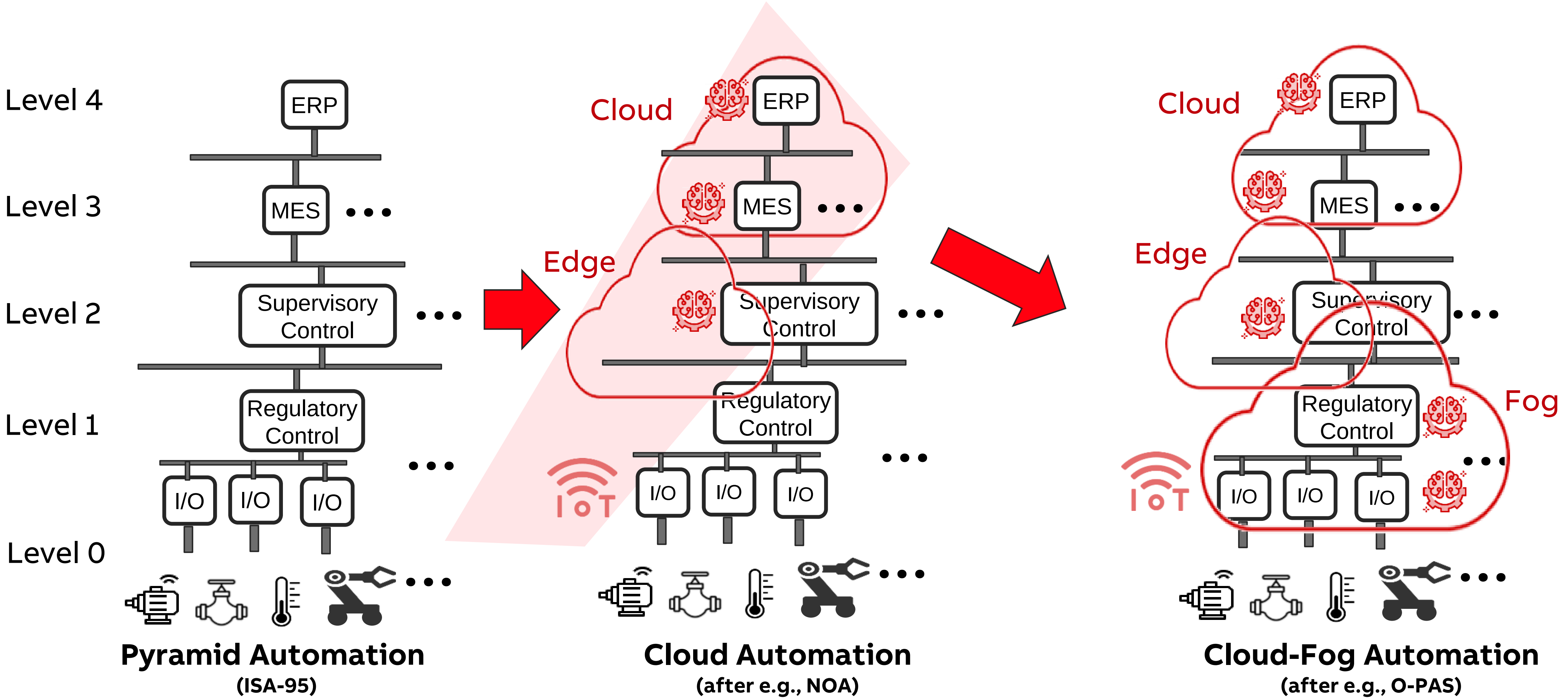







Towards the vision of Could-Fog Automation (CFA)

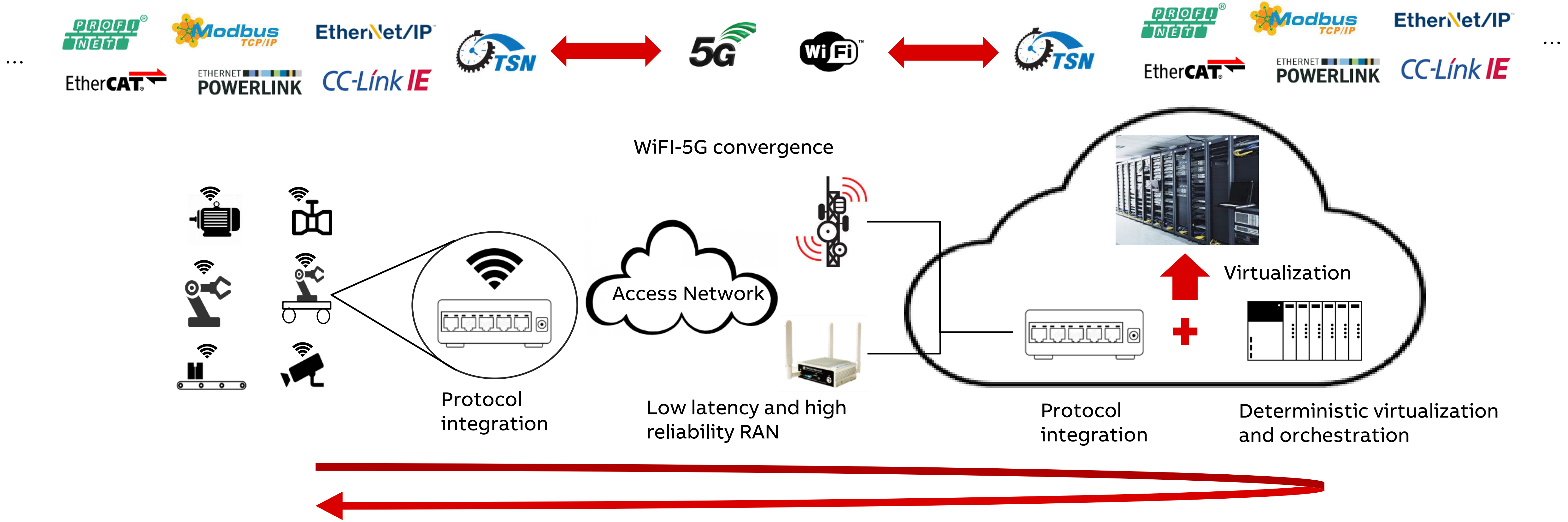
A realistic pathway: from monitoring & optimization to critical control, from add-on to replacement



1. Kang B. Lee, Richard Candell, Hans-Peter Bernhard, Dave Cavalcanti, Zhibo Pang, Inaki Val, "Reliable, High-Performance Wireless Systems for Factory Automation", *NIST Interagency/Internal Report (NISTIR)*, No. 8317, September 18, 2020

CFA over wireless communication and computing infrastructure

Challenges: latency, reliability, protocol integration, virtualization, security, safety



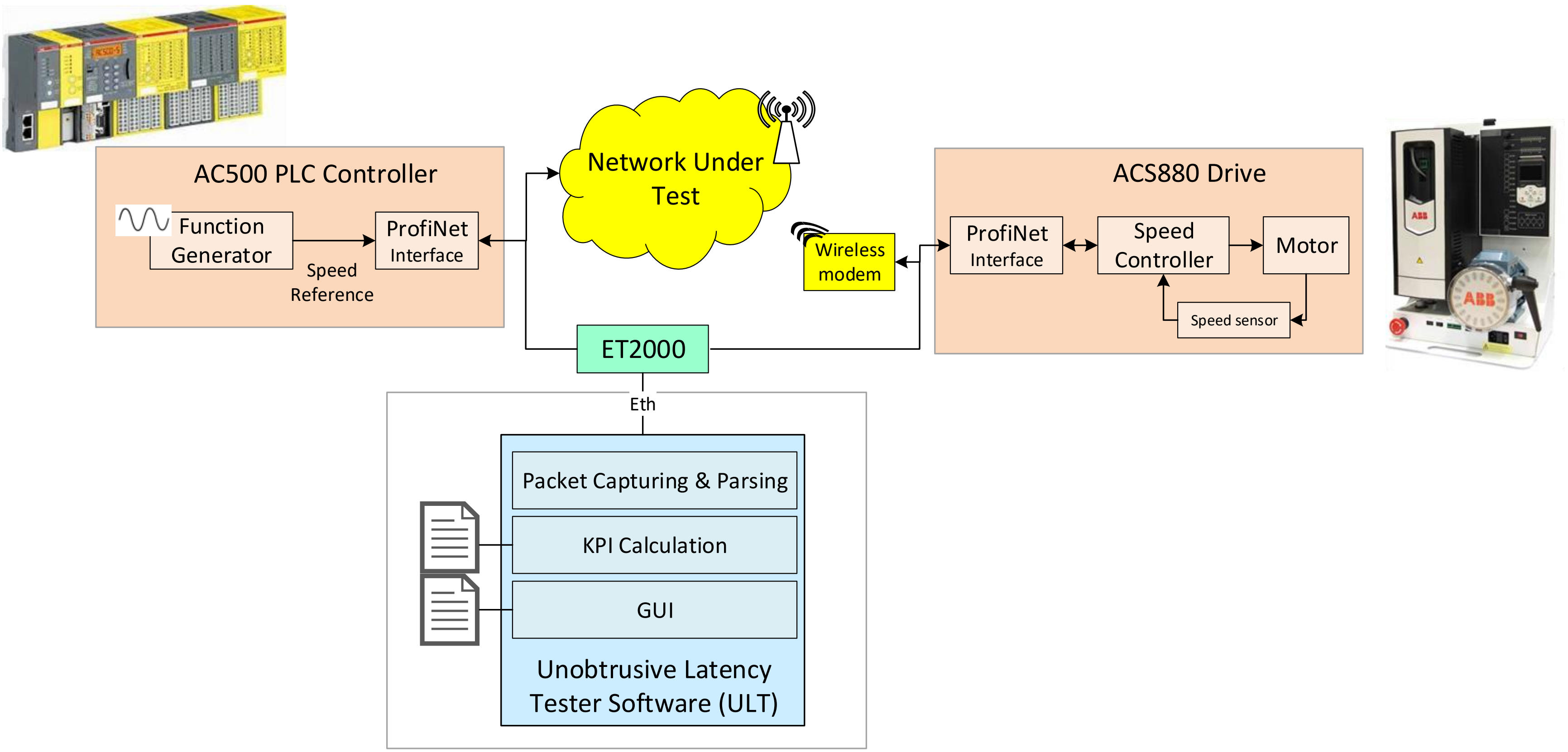
End-to-end latency <1~100ms, availability > 99.999%, depending on the equipment under control.
OT cybersecurity (e.g., IEC 62443), and functional safety (e.g., IEC61508, ISO 13849)

Unobtrusive evaluation of 5G R15 eMBB in a representative control system

The testing tools:
- Inserting delay < 1 us
- Latency accuracy: 40ns
- Verifiable reliability: > 99,9999% (six-9)

The 5G under test:
- 5G R15 eMBB
- 1-hop 5G,
- In lab, 2m distance between UE and BS
- no obstacle, no competing traffics

The application
- PROFINET IO
- 16ms cycle time
- 60B Ethernet frame (PNIO in GRE in Eth),



Latency Distribution over Time and Mask of Latency Distribution

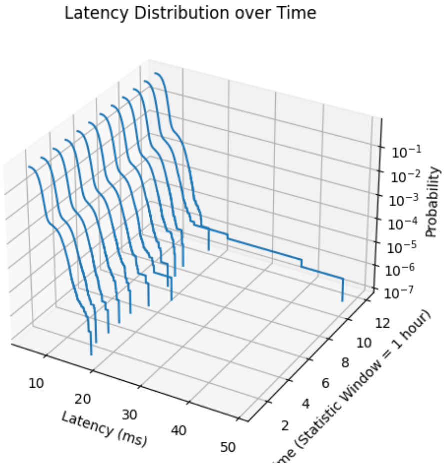
Results from the test in Feb 2022

Definition

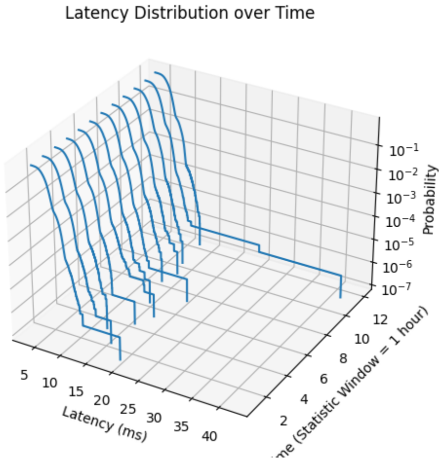
- **Latency distribution :**
  - CCDF (Complementary Cumulative Distribution Function)
  - Y is the probability of the packets with a longer latency than the X (ms).
- **Upstream**: traffic from device to controller
- **Downstream**: traffic from controller to device

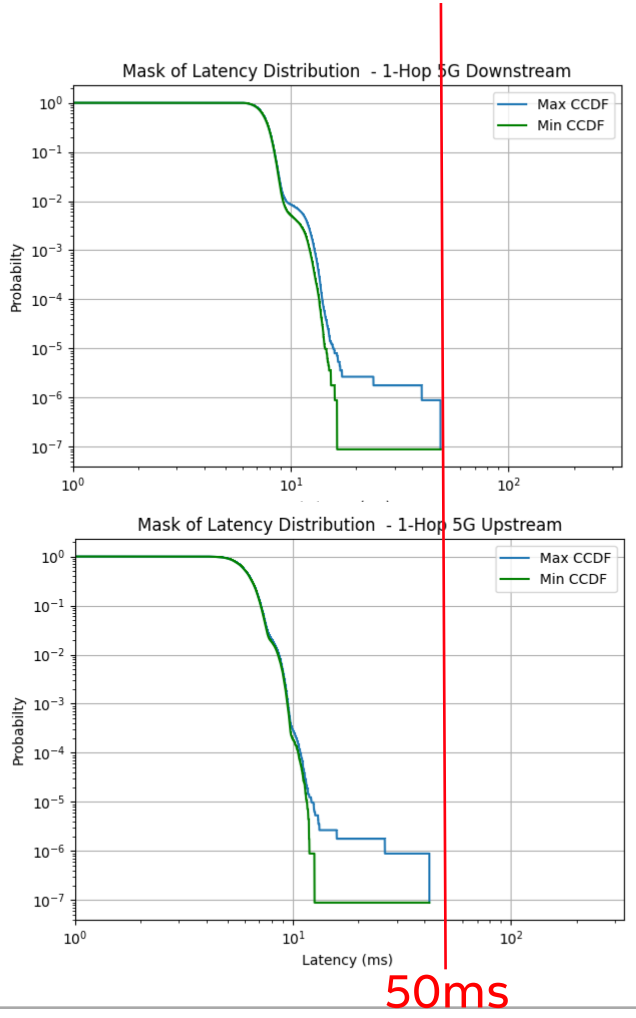
Statistic window: 5 hours

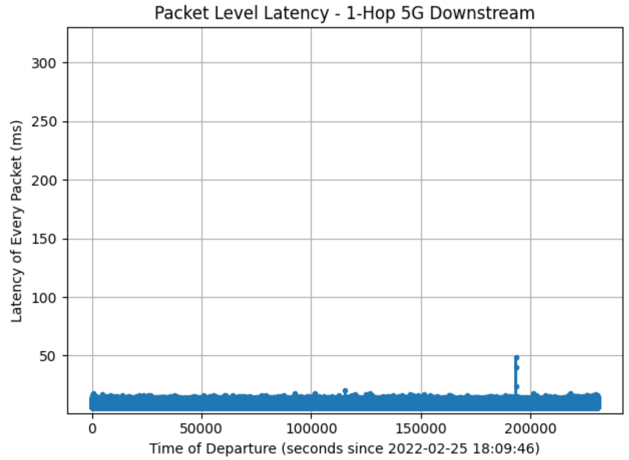
Downstream

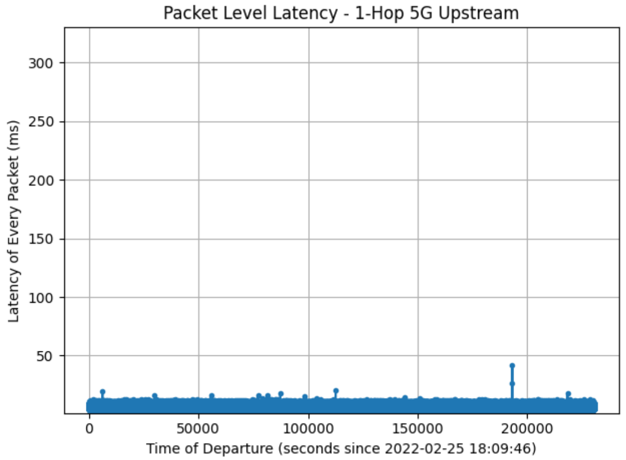


Upstream









Conditions: in lab, 1-hop 5G, 2m distance, no obstacle, no competing traffics, 16ms cycle time, 60B Ethernet frame (PNIO in GRE in Eth), when 5G system is stable, tested for 3 days, statistic window is 5-hour

Integration of 5G R15 with industrial network protocols

Known limitations (incomplete list)

- **It lacks support to Ethernet PDU :** IP Tunnelling (IPT) must be added to transmit non-IP traffics e.g. PROFINET, this is acceptable for customized case, instead of generic solution.
  - It breaks the compliance to standards, i.e., it cannot transmit the full length of PNIO packet as the IPT wastes 100+ bytes
  - This cannot be fully solved by IP fragmentation due to extra latency/reliability issues
  - When IP traffics and non-IP traffics are mixed, the IPT makes even more troubles (e.g., it puts IP packets in IP tunnel).
- **It lacks time synchronization for devices**: 5G R15 doesn't provide native time synchronization
  - It is complex or even infeasible to achieve PROFINET-RT grade time synchronization
  - It is NOT recommended for time-critical use cases, unless tailor-made solutions (e.g., PTP-like) are added in "gateway" or the application with lower accuracy than Ethernet-based.
- **It lacks support to IP/UDP multicast**: 5G R15 support only unicast of IP (internet protocol) packets
  - UDP multicast is important to get the benefits of the Pub-Sub feature of new generation automation network protocols like DDS and OPC-UA PubSub
  - Further investigation and customized solution is needed if UDP multicast is required in the application

New releases of 5G (R16/R17) are working on these issues, but products are to be delivered and verified.

Ethernet PDU (protocol data unit) is the layer 2 Ethernet packet which is commonly used in main-stream industrial ethernet protocols.
UDP: user defined protocol, a common way of realizing industrial communication protocols on top of IP (internet protocol).

Promise vs. delivery

5G ACIA
5G Alliance for Connected Industries and Automation

"For URLLC, the first release of **5G (Release 15)** already has the capability to achieve a latency of **1 ms** with a reliability of **99.999%** over the 5G radio interface."

-- the flagship White Paper[1]

- 5G has achieved big improvement than LTE, but the promised URLLC performances are not there yet
- Lab results are encouraging, but field tests are necessary:
  - Filed survivability
  - Scalability

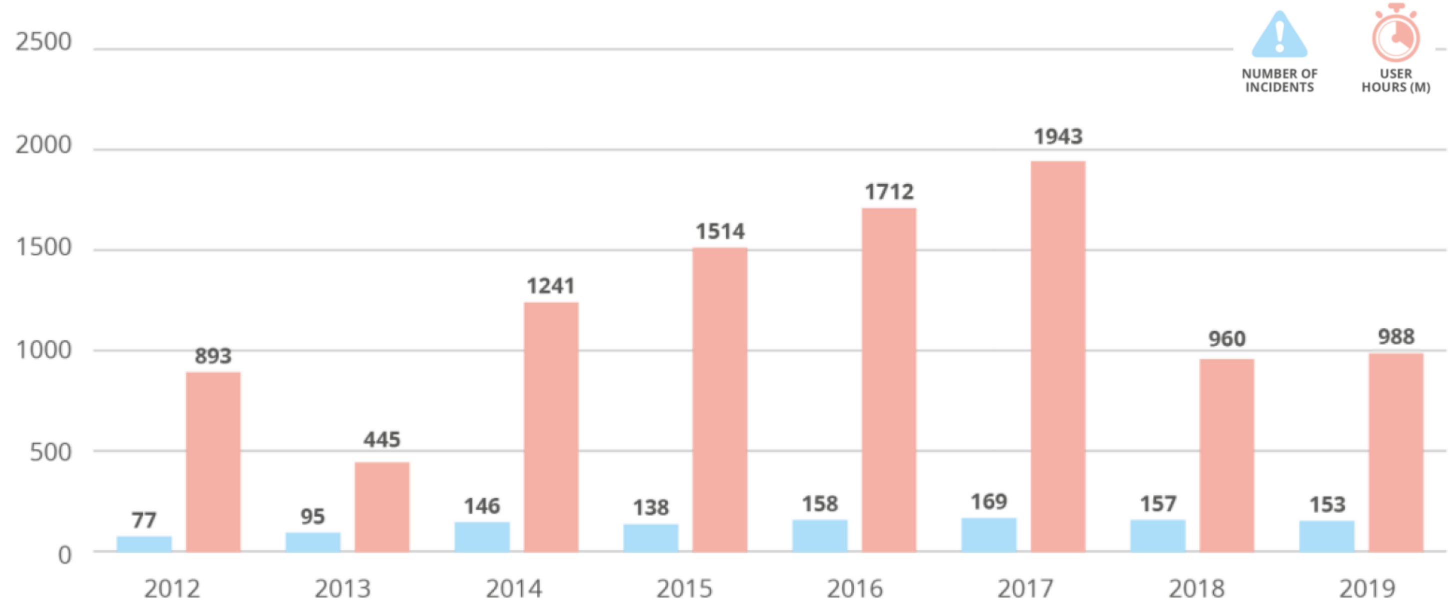
[1] 5G-ACIA White Paper 5G for Connected Industries and Automation, Second Edition, 28.02.2019. link

Security and long term availability of telecom services

Telecom Services Security Incidents 2019, European Union Agency for Cybersecurity (ENISA) [1]

- The 2019 annual summary reporting contains reports about **153 incidents** submitted by national authorities from the 26 EU Member States and 2 EFTA countries.
- The total user hours lost, multiplying for each incident the number of users and the number of hours was **988.12 Million User Hours**, i.e. roughly **0.026%** of the total user hours in a year using a basis of 500M (EU citizens) times 365 (days) times 24 (hours)..

Figure 1: Number of incidents and million user hours lost per year

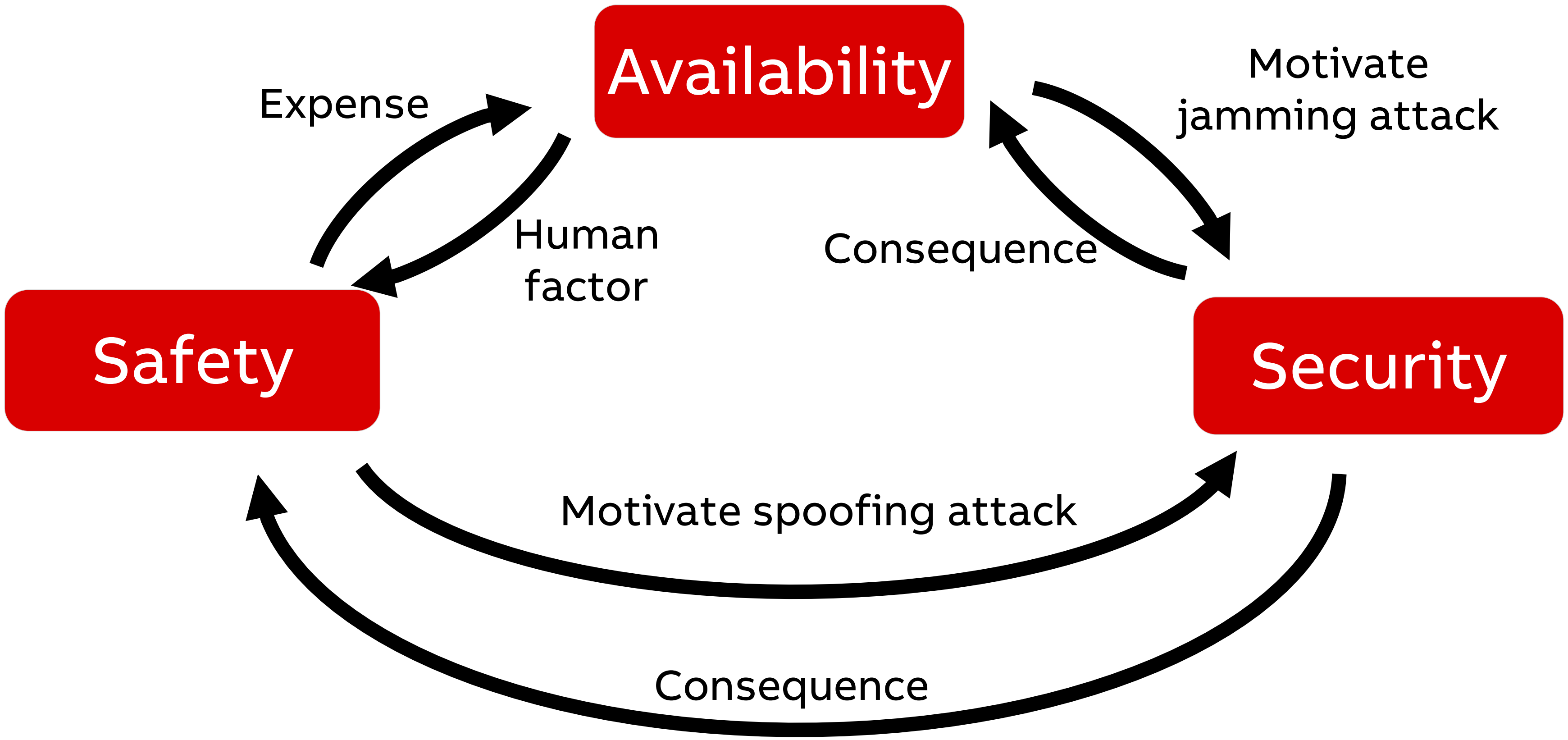


99.999% availability(=0.001% unavailability) was promised.
The actual unavailability, 0.026%, is 26 times worse than what was promised.

[1] European Union Agency for Cybersecurity (ENISA), "Telecom Services Security Incidents 2019 Annual Analysis Report", July 2020, link
ENISA: ultimately strives to serve as a centre of expertise for both member states and EU Institutions to seek advice on matters related to network and information security (--Wikipedia).

5G/wireless for safety critical and time deterministic applications

Relations between the 3 main aspects



- Jamming attack does affect safety, even though indirectly.

ABB

Take away messages

Cloud Fog Automation over wireless communication and computing for control applications will enable new values

5G R15 eMBB is evaluated in real-life testbed (ideal conditions):

- 50ms one-way latency with 99.9999% probability
- 99.9999% availability for 64ms cycle-time without tolerance, or 16ms cycle-time with strong tolerance in application

5G R15 eMBB has major functional gaps to support industrial network protocols

- Ethernet PDU session
- IP/UDP multicast
- Time synchronization

More tests are needed: field survivability, scalability

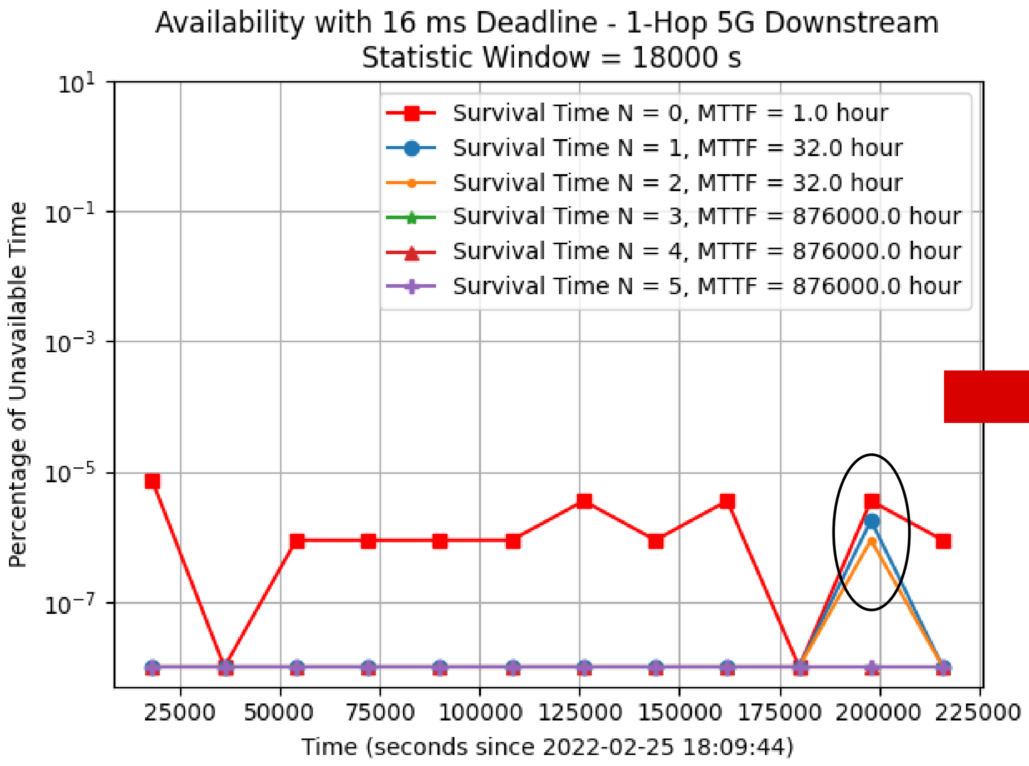
Security and long-term availability of telecom services are also of concern

Availability with and without packet loss/lateness tolerance in application

Results from the test in Feb 2022

Availability of 5G R15 **in good case** (2022-02-25)		
Deadline (one way)	99,999%	99,9999%
4ms	Never	Never
8ms	Never	Never
16ms	N=0	N=3
32ms	N=0	N=2
64ms	N=0	N=0
128ms	N=0	N=0
256ms	N=0	N=0

Obtained in a controlled environment (see the settings), results may vary depending on the actual deployment



The "Survival Time N" mechanism (→ time domain retransmission) is much less effective than the common assumption (e.g., in 3GPP [2]) to "cut the tail" of latency distribution when the probability is as low as e.g., 10^-4.

Communication service availability	Reliability (as defined in TS 22.261) 1 - p
99.999 9 %	99.9 %
99.999 999 %	99.99 %
99.999 999 99 %	99.999 %
99.999 999 999 9 %	99.999 9 %
99.999 999 999 999 %	99.999 99 %

[1] N: the number of consecutive packet loss or lateness that can be tolerated by the application.

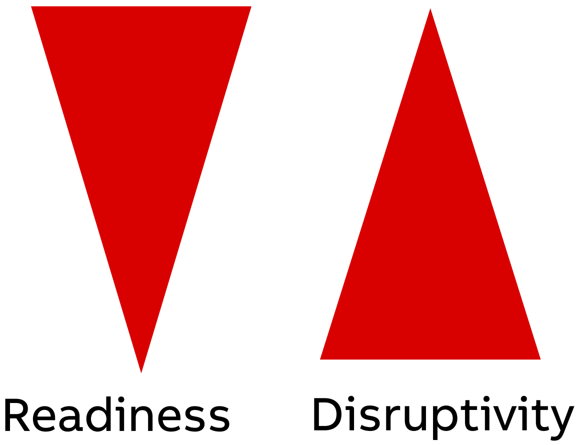
[2] 3GPP TS22.104, "Service requirements for cyber-physical control applications in vertical domains; Stage 1", V18.0.0 (2021-03)

“Killer applications” of 5G/WiFi6 and beyond

Best answers should come from business teams.

Personally, I have the following candidates:

- Wide area, long distance, flexibility
- Mobility of operator and machine
- Machine Intelligence (AI, vision)
- Automation/Control-as-a-Service



Some of them are being educated/inspired by 4G/WiFi5, but not really delivered with satisfaction.