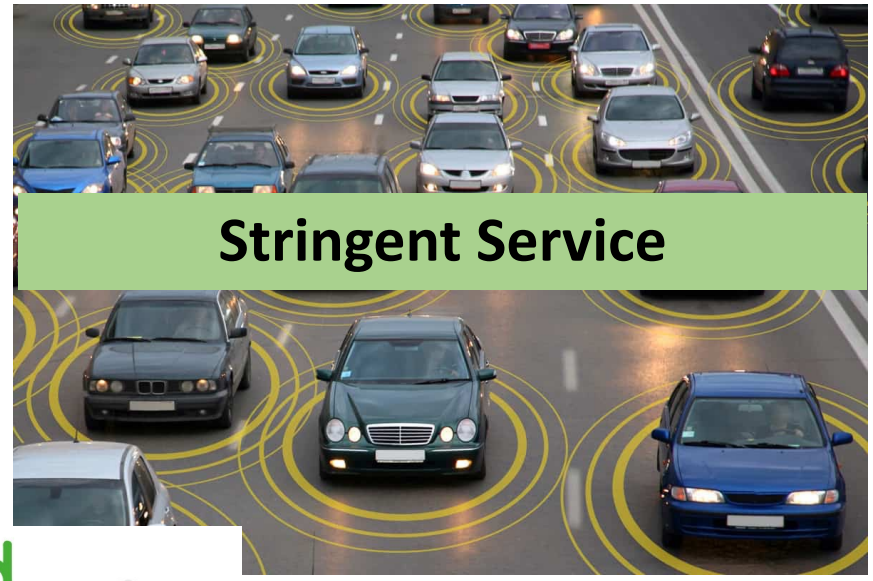
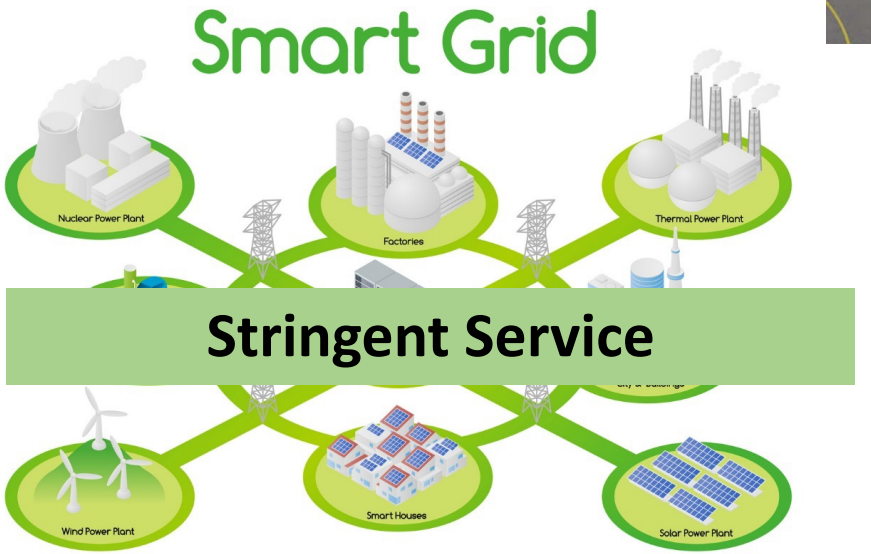
Operation and Control Networks - Problem Statement

This problem statement is in the context of Industrial systems, particularly Industry 4.0. However, some scenarios related to generalized future networks are highlighted to show a wider requirement of OCN networks.

Future Networks' Requirements

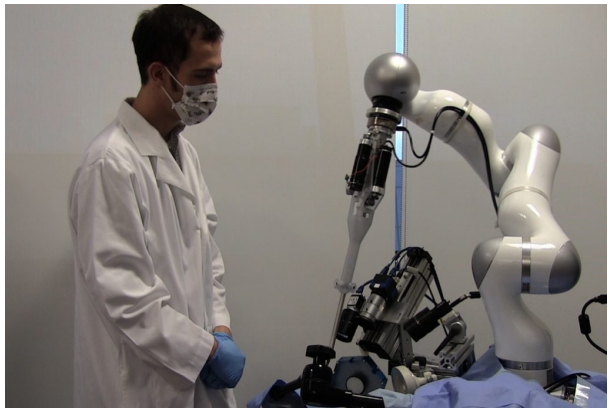
- Differentiated Services
- **Massive** number of devices (e.g., IoT)
- Stringent Services are **not always required**

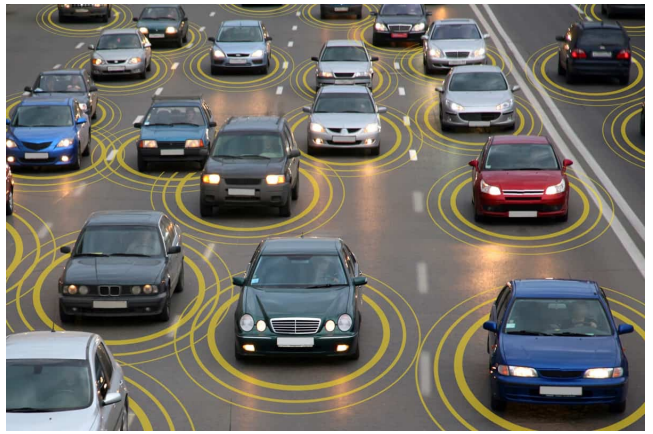




Service differences from general-purpose to control systems

- **Best-Effort Connection** (e.g., checking non-urgent email)
- **Bounded-Latency Connection** (e.g., car braking)
- **Hard-Service Connection** (e.g., autonomous surgery)



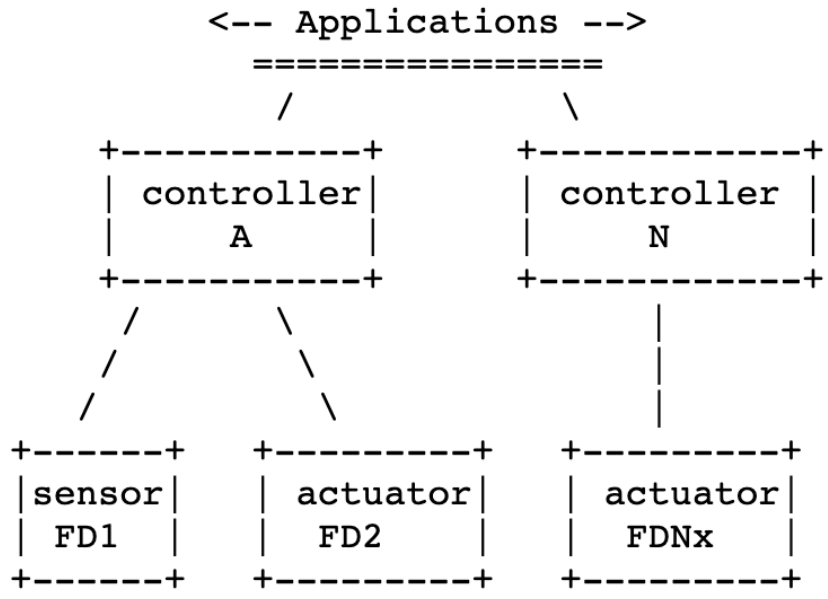


Limitations, Complexities and Requirements in Control Networks

- **High Precision Data Delivery**
  - Different types of commands require different latency delivery
  - Varying characteristics such as bounded latency, periodicity, message urgency on per command basis
  - Packet loss avoidance and/or faster detection – can lead to a missed command to an appliance
- **Computational Abilities**
  - Complex Process automation programs require computational abilities which are absent in sensors etc.
- **Use of AI/ML Technologies**
  - Predicting maintenance windows, general wear and tear of equipment requires feeding real-time data to ML models -- Connectivity to offsite server farms with such capabilities

- **Traffic Distribution**
  - Different types of commands require different latency delivery
  - Varying characteristics such as bounded latency, periodicity, message urgency on per command basis
  - Packet loss avoidance and/or faster detection – this could lead to a missed command to an appliance.
  - Well-engineered behaviour – all the anomalies must be managed
  - Ordering – should be support at network layer
  - Per-packet expectations – some packets will be prioritised
  - Congestion Control – congestion needs to managed at end-points
- **Accountability (can be through DLT)**
- **Cyber-Security Threats**
  - Protection against different threats such as taking over the role of sensor to send incorrect readings, taking control over an actuator to execute different behavior or jamming the network with burst of sensor data.
  - **Safety and Reliability** -- only correct data should be sent by devices

- **Control Loops**
  - Need to be supported from cloud
  - A network between controller and field devices (of course, within the physical link capabilities)
- **Communication model**
  - Can be generalized



Conclusion

- **Diversity in Service Quality** – different types of latency constraints for different types of messages. Control networks present challenges in terms of differentiated and reliable service requirements
- **Connected Sensors and Actuators** – to execute control loops over networks
- **Control network design** should be able to support diversified services (both stringent and non-stringent services)