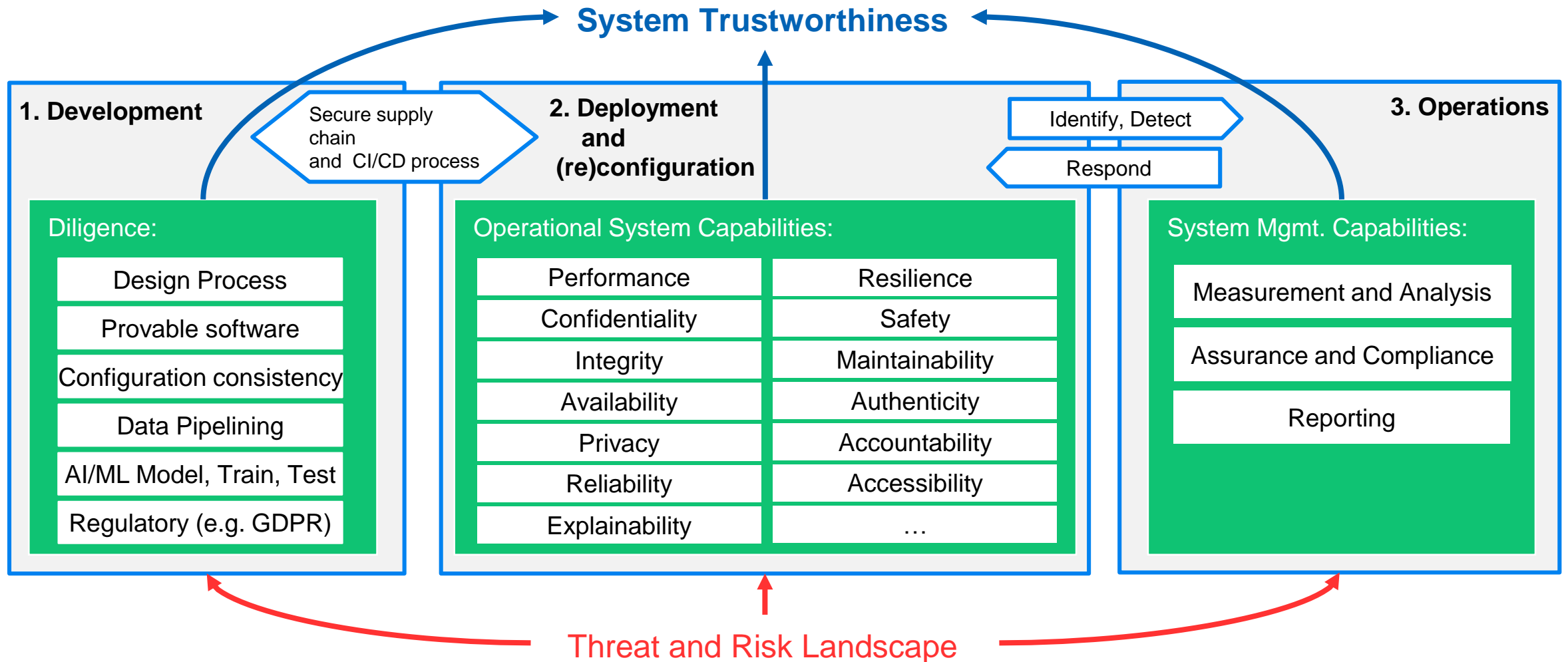
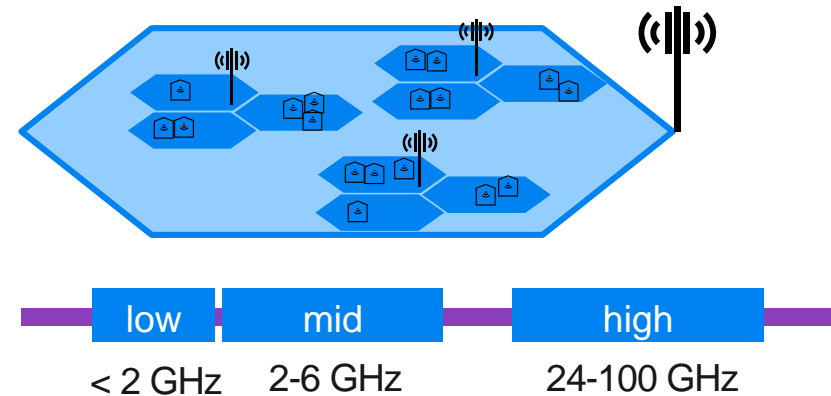


Trustworthiness and Process



Network Reliability, Availability, and Resilience (NRAR)



- Approaches to NRAR by 5G

- Node pooling, coverage redundancy, multiple bands
- Abundance of resources – trade off coverage with system capacity
- New 5GC features, e.g. network slicing, virtualized network functions, service-based architecture etc.

- New use cases \equiv New threat/risk surfaces

- Every new performance requirement is a potential risk
- 5G applied to critical communication needs emphasize reliability and latency for industrial applications

- Old risks remain

- Backward compatibility with 2G/3G/4G

- Physical layer resilience is aided by design for reliability
- Design for coverage, lean design, robust signaling channels, spatial diversity with MIMO and beamforming

- New features in 5G eliminate some vulnerabilities

- Integrity protection for signaling since 4G along with dynamic placement of signaling in 5G
- Dedicated signaling and control
- Subscriber privacy enhancements
 - Confidential PHY identities, e.g. SUCI
 - Paging identifier independence from permanent identities

How robust is the 5G radio link?



- Physical channels can be compromised with excessive interference power relative to signal power
 - AAS and channel coding provides some flexibility in being able to avoid interference
 - Signaling channels are designed for good coverage
 - Link budgets can provide coupling losses for each logical channel configuration with associated KPI
- Susceptibility analysis available in literature (Lichtman et al)
 - Prior work analyzes jammer operating in the energy limited region rather than power limited region
 - Power-limited operation is operationally relevant
- System configuration can aid more robust design and deployment
 - Strong recommendation to operators to initiate identity handling with SUCI
 - For NR-SA: Network slicing can improve robustness by preventing fallback to 4G and prior generations
 - Future releases may allow integrity protection for the data plane
- Mobile networks cannot be made totally resistant to jamming
 - Best we can expect is to increase complexity and maximize energy consumption by adversaries

Summary

- Trustworthiness largely derived from that part of trust that originates from evidence of compliance to well defined requirements and processes pertaining to security, reliability, privacy, safety and resilience.
- Resilience is derived from reliability and robustness and can involve system adaptability as a mechanism
- Physical layer resilience is achieved by design that focuses on
 - coverage,
 - exploits diversity and redundancy,
 - encrypting information and protects integrity, and
 - improving diversity modes
- Important to couple system observability through continuous measurement, analysis, and inference: this is an important area for application of machine learning





<https://www.ericsson.com/>

Abbreviations and further reading



Abbreviation	Description
5GC	5G Core
GDPR	General Data Protection Regulation
NRAR	Network Reliability, Availability, and Resilience
NR-SA	NR-Standalone
SUCI	Subscription Concealed Identifier

1. K.Balachandran, B. Smeets, M. Liljenstam, J. Ylitalo, and E. Fogelström, “Building trustworthiness into future mobile networks,” at <https://www.ericsson.com/4a1e32/assets/local/reports-papers/white-papers/ericsson-white-paper-building-trustworthiness-into-future-mobile-networks.pdf>.
2. P.K. Nakarmi, O. Ohlsson, and P. Hedman, “Fighting IMSI catchers: A look at 5G cellular paging privacy,” at <https://www.ericsson.com/en/blog/2019/5/fighting-imsi-catchers-5g-cellular-paging-privacy>.
3. K. Norrman and P.K. Nakarmi, “Protecting 5G against IMSI catchers,” at <https://www.ericsson.com/en/blog/2017/6/protecting-5g-against-imsi-catchers>.
4. M. Lichtman, R. Rao, V. Marojevic, J. Reed and R. P. Jover, "5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation," 2018 IEEE International Conference on Communications Workshops (ICC Workshops), 2018, pp. 1-6.