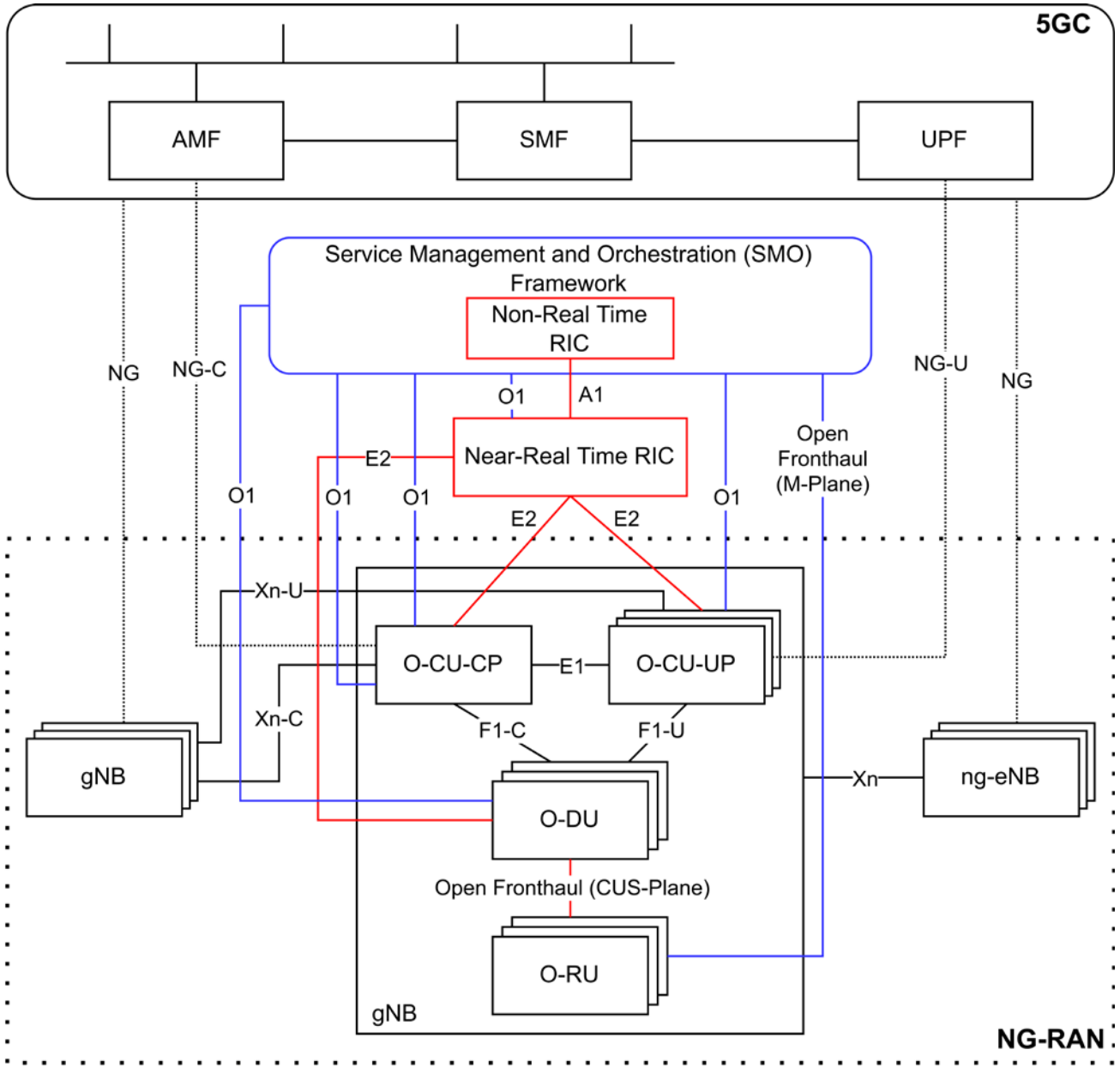
# Open RAN Risk Analysis and way forward

| | |
|---|---|
| Department | SZ - Standardization, Certification and Cybersecurity of Telecommunication Networks |
| Division | SZ 3 - Cyber Security in mobile Infrastructures and Chip Technology |
| Section | SZ 31 - Infrastructure Security for Telecommunication Networks, 5G |

# BSI Motivation for Open RAN risk analysis in 2021

- Open RAN is a growing trend in the mobile industry (e.g. MoU of MNOs January 2021)
- O-RAN Alliance has the key role in Open RAN specification
- Both opportunities and risks arise with Open RAN
  → Many political statements in public discussion
  → Need for factual analysis of current security level

# Excursus: O-RAN architecture (functional + management)



# Open RAN risk analysis

- Study commissioned by BSI
- Preparation by Barkhausen Institute
  (CEO Prof. Gerhard Fettweis; Dresden / Germany)
- Cooperation partners:
  - Advancing Individual Networks
  - secunet Security Networks AG
- Runtime: May – September 2021

# Methodology: Best/Worst Case Scenarios

- Risk analysis **solely based on specifications**/standards
  → no real-world implementations/operations considered
- Challenge: many security controls are only optional
- Solution:
  → Best-case: **all optional security controls are (correctly) in place**
  → Worst-case: **only required security controls considered**
- Independently **applied to 3GPP** standards and **O-RAN** specifications

# Open RAN Risk Analysis - Recommendations

**Conclusion:** „functionality first“ leads to many security risks

**Recommendations:**

- **Take „security/privacy by design/default“ serious**
- Consider minimal trust assumptions (buzzword: „zero trust“)
- Make optional security controls mandatory
- Disallow the usage of outdated/insecure cryptographic algorithms
- Implement fine-grained access control & rights management
- Consider denail-of-service attacks
- Consider untrusted O-Cloud operators

# Way forward

- German BSI and BNetzA (Federal Network Agency) continue to accompany Open RAN standardisation process in ETSI MSG
- BSI promotes Enhancements in 5G and Open RAN security as part of public funding programmes (see https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Foerderung_Projekte_220505.html )
- Networking with other funding programmes and researchers
- Co-operation in NIS and ENISA

→ Secure products and networks from the beginning

# Thank you for your attention!

Deutschland
Digital•Sicher•BSI•

**Heiner Grottendieck**

Section SZ 31
„Infrastructure Security for Telecommunications Networks, 5G“
referat-sz31@bsi.bund.de

Federal Office for Information Security (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de


Bundesamt
für Sicherheit in der
Informationstechnik