frontiers in Energy Research

BRIEF RESEARCH REPORT
published: 08 February 2022
doi: 10.3389/fenrg.2021.796257

Power 5G Hybrid Networking and Security Risk Analysis

Yu Jiang[1,2,3]*, *Yang Cong*[1] *and Aiqun Hu*[1,2,4]

[1]School of Cyber Science and Engineering, Southeast University, Nanjing, China, [2]Purple Mountain Laboratories, Nanjing, China, [3]Key Laboratory of Computer Network Technology of Jiangsu Province, Nanjing, China, [4]State Key Laboratory of Mobile Communication, Southeast University, Nanjing, China

5G communication technology provides strong support for the power Internet of Things, and it also introduces new security challenges in the application process of the power industry. Starting from the analysis of the power 5G business requirements, this article proposes five 5G enterprise networking construction plans based on different collaborative processing relationships, and conducts a comparative analysis in security, delay, independence, cost, and staffing. According to the analysis of power business requirements and enterprise networking mode, a hybrid networking architecture of 5G and power communication network is proposed, and the 5G network slicing architecture is re-segmented according to different business scenarios. Finally, the new risks and challenges introduced by 5G technology are analyzed in detail from the four parts of terminal access, edge computing, network channel, and core network. Two important risks pointed are specified through a security risk assessment algorithm. In the future, it is also necessary to further study key technologies such as lightweight authentication algorithms and network slice security isolation to realize the real security use of 5G network in the power industry.

Keywords: 5G, network slicing, hybrid networking, security risk, cyber security

OPEN ACCESS

Edited by:
Sheng Huang,
Hunan University, China

Reviewed by:
Xueping Li,
Hunan University, China
Yinpeng Qu,
Hunan University, China
Feifan Shen,
Hunan University, China

***Correspondence:**
Yu Jiang
jiangyu@seu.edu.cn

Specialty section:
This article was submitted to Smart Grids, a section of the journal Frontiers in Energy Research

Received: *16 October 2021*
Accepted: *20 December 2021*
Published: *08 February 2022*

Citation:
Jiang Y, Cong Y and Hu A (2022) Power 5G Hybrid Networking and Security Risk Analysis. Front. Energy Res. 9:796257. doi: 10.3389/fenrg.2021.796257

INTRODUCTION

5G technology is the future development direction of mobile communication technology (Shafi et al., 2017). The features of low latency and high reliability (Jaber et al., 2016) make it possible to "wirelessly" control production control systems such as power monitoring systems. 5G network slicing technology (Ordonez–Lucena et al., 2017) can create customized "business private network" services for users in the power industry to better meet the differentiated needs of power grid services. The massive access capacity, high bandwidth, and edge computing capabilities of 5G provide strong support for acquisition, transmission, and on-site processing (Wang, 2018; Wang et al., 2019; Zhang et al., 2019).

5G has proposed newer and more secure standards in terms of access authentication, communication encryption, and so on. However, in the application process of the power industry, there are still many security issues that have not been resolved. While key technologies and brand-new network design, such as network slicing (Liu et al., 2020), core network sinking (Xiang et al., 2017), mobile edge computing (Arfaoui et al., 2018), and ultralow latency business bearer, better support diverse application scenarios, they also raise new challenges to the existing power network security protection system architecture in edge computing scenario, network access, business security, network management, and so on.

Starting from the demand analysis of the power 5G business, this article analyzes production consumption and business demand, in order to master the overall characteristics and typical

indicators of the power business. Then according to the requirements, five different 5G enterprise network deployment and construction plans are proposed, and we conduct comparative analysis on security, delay, independence, deployment cost, and staffing. Next, a hybrid networking architecture of 5G and power communication network is proposed, covering four levels of end, edge, pipe, and cloud. Due to the large differences in communication requirements for business scenarios of the power grid, the 5G network slicing architecture in the hybrid networking mode needs to be re-segmented under different business scenarios. Finally, from the four parts of terminal access, edge computing, network channel, and core network, the new risks and challenges introduced by 5G technology are analyzed in detail.

Based on the adaptability of the 5G communication and the power grid, we propose a hybrid networking architecture of 5G and power communication network, and consider the risks of four parts. In practical applications, on the one hand, the structure of the hybrid networking system is conceived from the perspective of "end, edge, pipe, and cloud" with the logical division of business slicing. On the other hand, it provides guidance for the security protection of weak links.

ANALYSIS OF POWER 5G BUSINESS REQUIREMENTS

From the perspective of production and consumption, the power business mainly covers the five main links of the power grid: generation, transmission, transformation, distribution, and usage. At present, with the wide-ranged power distribution points, optical fiber coverage construction costs are high, and operation and maintenance and deployment are difficult (Chen, 2015; Luo et al., 2017). 5G networks are mainly used in power distribution and power consumption scenarios with ubiquitous wide-area coverage requirements.

From the perspective of business needs, the 5G power communication network mainly involves three types of business including production control area, information management area, and Internet area. The specific subdivision business mainly includes distribution differential protection, synchronous phasor measurement (PMU), intelligent distribution automation, power load demand side response, intelligent inspection, facility operation status monitoring, and so on.

1) Overall characteristics: ultralow delay, high security isolation, high reliability, and ultrahigh precision timing requirements. The production control category involves high-reliability and low-latency communications (uRLLC), the information collection category involves enhanced mobile broadband (eMBB), and a small number of applications involve the integration of uRLLC and eMBB.
2) Typical indicators: strict isolation is required between production control and information collection business. Power distribution differential protection and power distribution automation services present deterministic low-latency requirements with two-way delay requirements of 2–5 ms and business bandwidth requirements greater than 2 Mbps. Therefore, there is a demand for small particles and low delay load. The PMU business presents the bearer requirement of ultrahigh-precision timing. For example, the 5G base station air-to-air timing is used for PMU terminals as a backup for GPS/Beidou satellite synchronization, and the precision of precise timing needs to reach hundreds of nanoseconds.

POWER 5G HYBRID NETWORKING DESIGN

Analysis of 5G Enterprise Networking

To realize 5G applications, 5G networks need to be built and deployed first. The deployment of 5G networks mainly includes two parts: the radio access network (RAN) and the core network (Zhu and Xiang, 2016; Wang et al., 2017). Currently, 5G network deployment methods can be roughly divided into five categories: enterprise self-built, licensed spectrum, shared base station, unique user plane management (UPF)/MEC, and network slicing (Ahmad, 2019; Li et al., 2021). In order to meet the needs of communication networks and reduce construction costs, different deployment and construction plans are proposed according to the actual situation. The following is a detailed analysis of five 5G enterprise networking modes.

1) Self-built 5G private networks by enterprises: It needs to independently apply for private spectrum and establish a completely private local area network.
2) Exclusive operator-built isolated 5G private networks: Similar to (1), the difference is that the company exclusively enjoys the operator's 5G network infrastructure, and the operator licenses part of the spectrum to the company.
3) Enterprise private network sharing public network RAN: The user plane management (UPF), 5G core network control panel (5 GC CP), unified data management (UDM), and MEC are deployed in the enterprise and are physically isolated from the public network. Only the 5G base station of the public network is shared between the private network and the public network.
4) Enterprise private network sharing public network RAN and control plane: Enterprise-specific UPF and MEC are built into the enterprise, and the 5G base station and control plane of the public network are shared. The control plane functions (identity verification, mobility, *etc.*) of enterprise private network equipment and public network equipment are performed by 5 GC CP and UDM in the operator's network.
5) Enterprise private network sharing all the 5G network facilities of the public networks: The enterprise private network uses network slicing to share the public network, and logically separates the 5G RAN and core network.

Table 1 compares the analyses from the above five schemes in terms of security, delay, independence, deployment cost, and staffing.

TABLE 1 | Analysis of 5G enterprise networking mode.

Mode	Security	Low latency	Indepen-dence	Deployment cost
(1) Self-built 5G private networks by enterprises	Good, physically isolated from the public network, data managed in the enterprise	Yes	Good	High
(2) Exclusive operator-built isolated 5G private networks	Good, completely private 5G LAN	Yes	Good	High
(3) Enterprise private network sharing public network RAN	Fair, data offloaded at the base station	Yes	Average	Fair
(4) Enterprise private network sharing public network RAN and control plane	Fair, data offloaded at the base station with mixed transmission	Yes	Fair	Fair
(5) Enterprise private network sharing all the public 5G network facilities	Poor, data flow must pass through the operator's edge cloud	No	Poor	Low

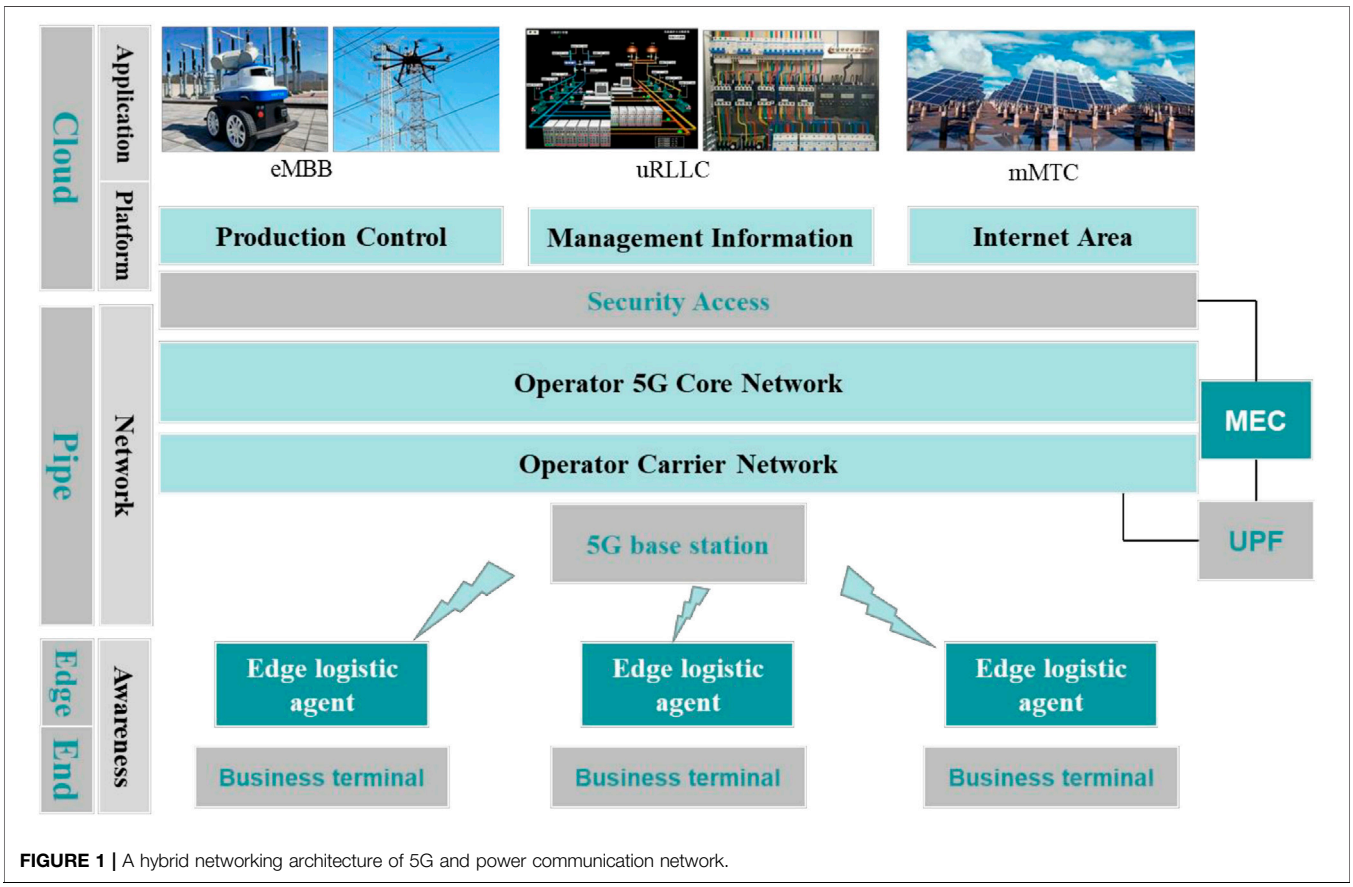

FIGURE 1 | A hybrid networking architecture of 5G and power communication network.

It can be seen from **Table 1** that the independent construction of 5G network infrastructure adopted by modes 1 and 2 has a relatively high deployment cost. Due to the national wireless spectrum resource allocation policy, it will be more difficult for companies to build their own 5G private networks or lease operator's spectrum. Options 3 and 4 adopt the mode of shared base station and dedicated MEC. While ensuring the low latency of data transmission, it guarantees the privacy of the data, which is suitable for the application requirements of the power grid production control or information management business. Option 5 shares the public network 5G infrastructure, which is suitable for the application requirements of the power grid Internet business.

Hybrid Networking Architecture of 5G and Power Communication Network

Based on the typical business of the three major regions of the power grid, this section first proposed a hybrid networking architecture of 5G and power communication network, as shown in **Figure 1**.

The hybrid networking architecture of 5G and electric power communication network covers 4 levels: end, edge, pipe, and

cloud. The terminals in the three regions of the "end" layer are connected to the edge IoT agent equipment through the northbound. The edge IoT agent equipment of the "edge" layer are connected to the 5G base station through the air interface. Some power business in the "pipe" layer are offloaded on the 5G edge side UPF and terminated at the MEC, or preprocessed by MEC and connected to the "cloud" layer application system through the dedicated line of the city. Other business in the "pipe" layer enter the "cloud" layer application system through the power communication network connected to the 5G bearer network.

The perception layer includes the "end" and "edge" parts of the original 4G network architecture, and some terminals directly support 5G communication through transformation. Under the original edge IoT agent, the terminals of the "end" and "edge" layer can meet the access function requirements by adding 5G communication functions to the edge IoT agent.

The network layer forms the "pipe" part of the network architecture, including the operator's network, enterprise-deployed MEC equipment, as well as the dispatching data network of the production control area and the data communication network of the management information area.

The platform layer and the application layer together constitute the "cloud" part of the network architecture, including production control area, management information area, and the Internet area. In the "cloud-pipe-edge-end" system, 5G introduces new technologies to the hybrid networking architecture, which is mainly reflected in MEC equipment and network slicing.

The following focuses on the analysis of the changes in the business processing process that MEC brings to the hybrid networking of 5G and power grids. According to different types of business, MEC/UPF is deployed in two different locations. One is the MEC/UPF deployed in the core network, which is mainly responsible for processing low-bandwidth non–real-time business in the Internet area and management information area. And the other is the MEC/UPF deployed at the power grid plant and station side, mainly responsible for processing high-bandwidth, low-latency, and high-reliability business in the production control area and the management information area.

In the two scenarios of MEC/UPF deployment, three business flows are formed.

1) Local processing of MEC/UPF at the plant and station: From the "end" and "edge," the perception layer business enters the local plant UPF through the access network and bearer network for traffic offloading, and then sends it to the MEC equipment for localized processing in order to realize business interaction. The MEC in the production control area is recommended to be self-built, and the MEC in the management information area is self-built or leased by operators.
2) Connected to the enterprise intranet after local processing of MEC/UPF at the plant and station: From the "end" and "edge," the perception layer business enters the local plant UPF through the access network and bearer network for traffic offloading, and then sends it to the MEC equipment for localized processing, entering the intranet to realize business interaction. The regulation business is preprocessed on the MEC and directly connected to the production control area through the city's dedicated line. The collection business is preprocessed on the MEC and then enters the management information area through the data communication network and the secure access.
3) Access to the corporate intranet through the UPF of the operator's core network: From the "end" and "edge," the perception layer business enters the local plant UPF through the access network and bearer network for traffic offloading, and then sends it to the MEC equipment for localized processing, entering the intranet to realize business interaction. The regulation business connected to the production control area through the dispatch data network and the secure access. The collection business is connected to the management information area through the data communication network and the secure access.

Power 5G Business Deployment Architecture

The 5G end-to-end network slicing system is driven by business. 5G network slicing technology logically divides the basic physical network to share the same set of physical infrastructures through cloud and virtualization technologies, thereby providing customized network services for business applications with different performance requirements. In view of the large differences in communication requirements in different business scenarios of the power grid, the 5G network slicing architecture in the hybrid networking mode should be re-segmented according to business scenarios, which is shown in **Figure 2**.

As shown in the figure, the production control area and the management information area/Internet area are first isolated, and then the power grid business is classified according to the three major application scenarios of 5G into eMBB, uRLLC, and mMTC slices. eMBB slices are mainly large video applications of smart grids, including substation inspection robots, transmission line drone inspections, integrated video monitoring of power distribution rooms, mobile site construction control, and emergency site–integrated autonomous applications. uRLLC slices mainly include intelligent distribution automation and power load demand side response services. mMTC slices are mainly distributed energy regulation and advanced metering. On the basis of the three major network slicing, according to the sub-slices of different business in the same slice scenario, it realizes reliable end-to-end slicing from the power terminal to the station system by connecting with various business platforms of the power grid.

In accordance with the partition isolation requirements of the power grid business, the FlexE hard slicing technology is used to hardly isolate the production control area and the management information area/the Internet area. eMBB, uRLLC, and mMTC slices are isolated in the areas for secure communication requirements to meet the differences in business functions. At the same time, the operator's network realizes the open sharing of terminals and network information through the capability opening

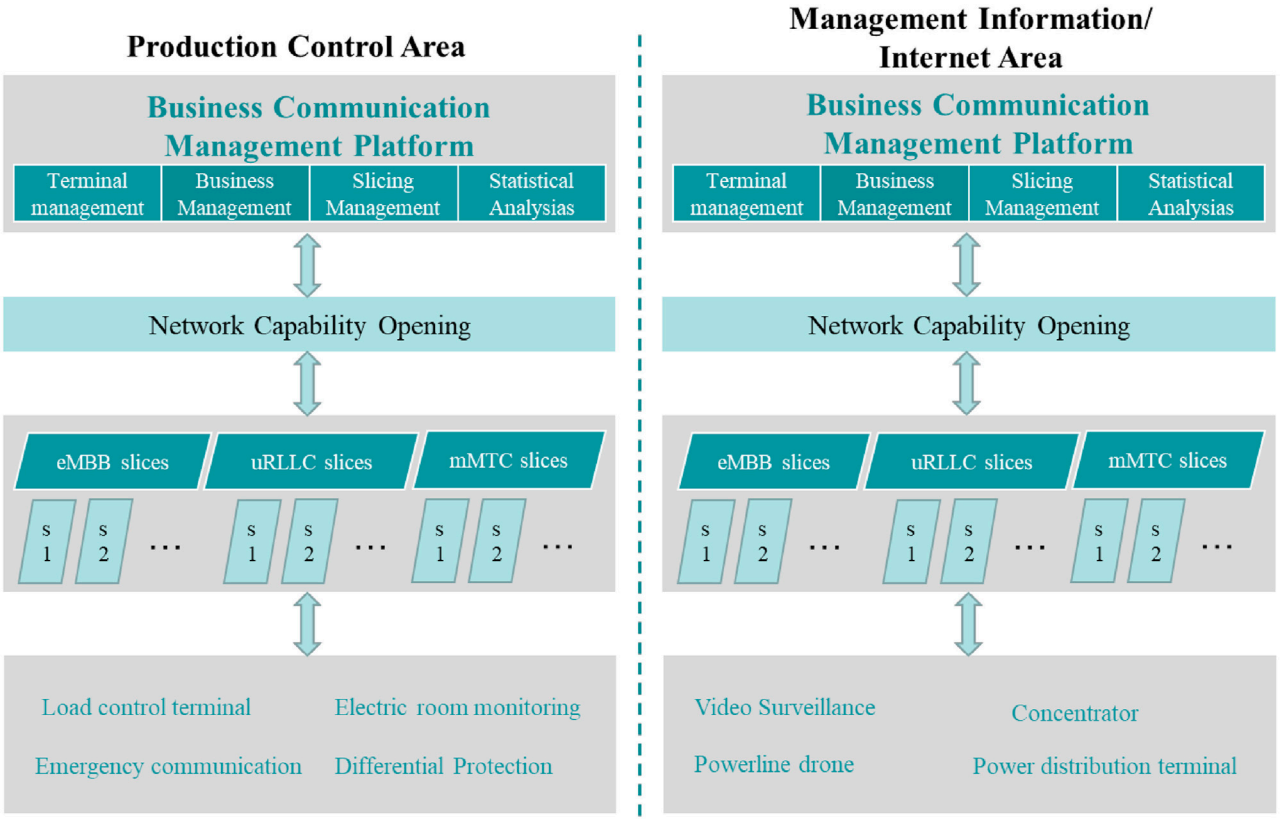

FIGURE 2 | Power 5G service deployment architecture.

platform, thereby providing the power industry with statistical analysis and configuration management of network slicing.

SECURITY RISK ANALYSIS OF POWER 5G HYBRID NETWORKING

The new security risks and challenges of 5G mainly include terminal access risks, edge computing risks, network channel risks, and core network risks. The risks introduced in the four parts are analyzed in detail below.

Terminal Access Risks Brought by Multiple Business Scenarios

When using smart terminals, there are inevitably threats such as malicious programs, firmware loopholes, eavesdropping, and tampering with user information. In addition, 5G scenarios of high concurrency, high traffic, and low latency put forward different requirements for the access authentication protocol. Simply using a general access authentication protocol cannot achieve the expected goals of the three application scenarios (Wojciech et al., 2020; Zou et al., 2021).

1) In the eMBB scenario, the transmission rate is high, and more user privacy and sensitive information are involved. Different business in the same application scenario also has different security requirements. Therefore, a higher level of authentication and information integrity protection must be implemented when the terminal is accessed, and at the same time, a high-rate encryption capability must be ensured.
2) In the mMTC scenario, the number of terminals connected to the network is huge, of which the security capabilities are weak and power consumption is limited. If the terminals continue to use the traditional access method, a signaling storm may cause network congestion. In the case of an access failure, the terminal continuously tries to re-access the network to initiate authentication, which will accelerate its battery consumption. Therefore, the access authentication protocol in this scenario mainly needs to be lightweight, efficient, reliable, and low cost.
3) uRLLC applications have higher requirements for communication reliability and low latency. However, enhancing the network security protection mechanism will inevitably come at the expense of network performance and reduced network efficiency. The realization of ultralow latency requires a series of mechanism optimizations in each link of end-to-end transmission.

Edge Computing Risks Caused by Business Traffic Offloading

1) The Risk of UPF Traffic Offloading

Once the business traffic passes through the local offloading edge node, it is difficult to effectively monitor and manage it. If the

UPF configuration is improper, there may also be the risk of offloading UPF traffic to other MEC platforms. The attacker unloads a large number of computing tasks or malicious transition to a specific MEC server, resulting in an oversupply of workload resources between the servers in the MEC, which may cause other users to time out and exhaust computing resources.

2) The Risk of MEC Data Offloading

The business data processed by the MEC application have the risk of data leakage for the confidentiality of data transmission and storage. In terms of data transmission, the lack of encryption and integrity verification mechanisms in the process of virtual machine migration or inter-platform transmission can lead to the risk of data being tampered or eavesdropped on by attackers, which is difficult to be tampered with. In terms of data sharing, there is a risk of sensitive data leakage caused by unauthorized third-party data dissemination and failure to use hierarchical classification and desensitization.

Network Channel Risks Brought by Networking Slicing

1) The Risk of Network Slicing Being Attacked

In logically isolated bearer network slices, overloading of one slice may cause other virtual slices in the same physical pipeline to work abnormally. The attacker actively uses the controlled slice as a springboard to attack other slices.

2) The Risk of Network Slice Access

When accessing a slice, an attacker may consume the resources of other slices, resulting in insufficient resources. DoS attacks may be launched on other slices. Attackers can also conduct cross-slice side-channel attacks.

3) The Communication Risk Between Slices

Communication is required between different network slices, RAN network slices, and core network slices. In all inter-network slice communication, the interfaces between network slices may be attacked. In addition, attacking the user plane can damage or maliciously transfer user data, thereby affecting one or more UEs.

Core Network Risks Brought by Network Capability Opening

5G adopts a new business-oriented architecture to split core network business into relatively independent network elements. The isolation and interfaces between network elements introduce new security risks. It is proposed that the opening of business capabilities will further break the closed state of networks and blur the security boundary with faster spread threats, easier attack, and harder defense. The comprehensive cloudification and ITization bring new challenges to the security of networks and information (Dutta and Hammad, 2020).

1) Network capability opening opens up information and data from the closed platform inside the operator. Operators have weakened data management and control capabilities, properly facing security risks such as unauthorized access and use and data leakage. Attackers can use the API provided by the 5G network capability open architecture to conduct denial of service attacks.
2) With the development of cross-industry applications, it is necessary to openly share corresponding data information, and the risk of data leakage increases. The network capability opening provides more attack surfaces for external opponents, making the infrastructure configuration easy to be tampered with, and also easy to be maliciously used and tampered with by internal attackers.
3) Once a security incident such as user data leakage occurs in the process of cross-industry data sharing, it will face unclear division of responsibilities between subjects, which increases the difficulty of data security supervision.
4) The network capability opening interface adopts the general Internet protocol, which will further introduce the existing security risks of the Internet to the 5G network.

TABLE 2 | Risk assessment grading standrads.

R	Risk grading results
[7,10]	Critical
[5–7)	High
[3,5)	Medium
[1,3)	Low

Risk Assessment of Power 5G Hybrid Networking

The calculation of security risk assessment is performed on each risk analyzed above, which is divided into the risk probability assessment P_n and the risk impact assessment E_n. The security risk assessment is based on the square root of the product of the two parts (Batalla et al., 2020). The calculation formula is

$$\mathbf{R} = \sqrt{\sum_{n=1}^{3} a_n \mathbf{P}_n \times \sum_{n=1}^{2} b_n \mathrm{E}_n}, \tag{1}$$

where R is the security risk assessment. The risk probability is determined by the physical intervention difficulty P_1, the implementation difficultyP_2, and the time consumption P_3, and the risk impact is determined by the business data impact E_1 and the business equipment impact E_2. Correspondingly, a_n and b_n are the weights of the weighted calculation, which are given in **Table 2**. For each P_n and E_n, the possible values from high to low are {10, 6, 3, 1}.

For the assessment of each risk, **Table 2** gives the risk grading standards.

The expert team of the power system and cyber security analyzed each risk factor in detail, and assigned values to each risk factor. **Table 3** shows the specific content of each risk and their corresponding risk evaluation assignment, evaluation calculation, and grading results.

TABLE 3 | Risk assessment of power 5G hybrid networking.

Risk	P_n			E_n		R	Grading result
	P_1	P_2	P_3	E_1	E_2		
	30%	50%	20%	75%	25%		
Sensitive information leakage in eMBB scenarios	6	3	3	6	1	4.30	Medium
High concurrency access in mMTC scenarios	6	6	3	3	3	4.02	Medium
Low protection capabilities in uRLLC scenarios	3	6	3	10	3	6.09	High
UPF traffic offloading	1	3	1	3	3	2.45	Low
MEC data offloading	1	1	1	6	1	2.29	Low
Network slice being attacked	3	6	6	3	3	3.91	Medium
Network slice access	3	10	10	6	10	7.44	Critical
Communication between slices	3	6	3	6	6	5.20	High
API denial of service attack	3	6	6	6	3	5.17	High
Cross-industry data breach	6	6	3	6	3	5.32	High
Internet interface protocol	3	6	3	6	3	4.86	Medium

Judging from the risk assessment scores and grading results in **Table 3**, the risk in uRLLC scenarios and the risk of network slice access need to be paid attention to.

Once a low-latency service in uRLLC scenarios is attacked, the consequences will be quite serious. While it is difficult to enhance network, security protection mechanisms are limited by network performance requirements. The security protection of uRLLC scenarios relies on an efficient and reliable access authentication protocol, and further research is needed on technologies such as lightweight authentication algorithms and low-latency multilevel encryption.

Due to the large differences in the security levels of power grid services in different areas, it will have a great impact on the business system when the isolation of network slices is being broken. In order to solve the risks of network slice access, it can rely on network slice security isolation and resource allocation technology in the future.

CONCLUSION

This article proposes a hybrid networking architecture of 5G and power communication network, and analyzes the risks brought by 5G technology to the power grid with a security risk assessment algorithm. Starting from the analysis of the power 5G business needs, five 5G network deployment and construction plans are proposed, and they are compared in terms of security, delay, independence, cost, and staffing, in order to find a deployment mode suitable for the power grid with different security areas. On this basis, a 5G and power communication hybrid networking architecture is proposed, where the network slicing architecture should be re-segmented according to the business scenarios considering that the communication requirements of different business scenarios in the power grid differ from each other. After analysis of new risks and challenges introduced by 5G technology from the four parts of terminal access, edge computing, network channel, and core network, two important risks pointed are specified through a security risk assessment algorithm. It is also necessary to further research key technologies such as lightweight authentication algorithms, network slicing security isolation, and low-latency multilevel encryption to realize the real security use of 5G network in the power industry.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

YJ—main author, conceptualization, methodology, and writing—reviewing and editing. YC—author, formal analysis, visualization, and writing—original draft. AH—supervising professor, project administration, and supervision.

FUNDING

This work was supported in part by Jiangsu key R&D plan (BE2019109), the National Natural Science Foundation of China (61601114, 61602113, 61801115, 61941115, and 62001106), the Natural Science Foundation of Jiangsu Province (BK20160692, BK20200350, and BK20200352), and the Project of State Key Laboratory of Mobile Communication, Southeast University (2020B05).

ACKNOWLEDGMENTS

The authors also acknowledge Jiangsu Provincial Key Laboratory of Network and Information Security (BM2003201) and the Purple Mountain Laboratories.

REFERENCES

Ahmad, Rostami. (2019). "Private 5G Networks for Vertical Industries: Deployment and Operation Models," in 2019 IEEE 2nd 5G world Forum (5GWF), Dresden, Germany, 30 Sept.-2 Oct. 2019. doi:10.1109/5GWF.2019.891168

Arfaoui, G., Bisson, P., Blom, R., Borgaonkar, R., Englund, H., Felix, E., et al. (2018). A Security Architecture for 5G Networks. *IEEE Access* 6, 22466–22479. doi:10.1109/ACCESS.2018.28274110.1109/access.2018.2827419

Batalla, J. M., Andrukiewicz, E., Gomez, G. P., Sapiecha, P., Mavromoustakis, C. X., Mastorakis, G., et al. (2020). Security Risk Assessment for 5G Networks: National Perspective. *IEEE Wireless Commun.* 27 (4), 16–22. doi:10.1109/MWC.001.1900524

Chen, L. (2015). *Design and Implementation of Management Data Partition Transmission Scheme of Power Telecommunication Network*. Beijing, China: Beijing University of Posts and Telecommunications.

Dutta, A., and Hammad, E. (2020). "5G Security Challenges and Opportunities: A System Approach," in 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 10-12 Sept. 2020. doi:10.1109/5GWF49715.2020.9221122

Huan-huan, L., Wei-chun, G., Fan-bo, M., Qiang, G., Gui-ping, Z., Yi-ling, M., et al. (2017). "Research on Power Data Transmission Method Based on Monitoring System Combined with Optical Fiber and Wireless Communication Network," in 2017 IEEE Conference on Energy Internet and Energy System Integration, Beijing, China, 26-28 Nov. 2017. doi:10.1109/EI2.2017.8245223

Jaber, M., Imran, M. A., Tafazolli, R., and Tukmanov, A. (2016). 5G Backhaul Challenges and Emerging Research Directions: a Survey. *IEEE Access* 4, 1743–1766. doi:10.1109/ACCESS.2016.2556011

Li, X., Guimaraes, C., Landi, G., Brenes, J., Mangues-Bafalluy, J., Baranda, J., et al. (2021). Multi-Domain Solutions for the Deployment of Private 5G Networks. *IEEE Access* 9, 106865–106884. doi:10.1109/ACCESS.2021.3100120

Liu, J., Han, Y., and Liu, B. (2020). Research on 5G Network Slicing Security Model. *NetInfo Security* 20 (4), 1–11. doi:10.3969/j.issn.1671-1122.2020.04.001

Mazurczyk, W., Bisson, P., Jover, R. P., Nakao, K., and Cabaj, K. (2020). Challenges and Novel Solutions for 5G Network Security, Privacy and Trust. *IEEE Wireless Commun.* 27 (4), 6–7. doi:10.1109/MWC.2020.9170261

Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Munoz, J. J., Lorca, J., and Folgueira, J. (2017). Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges. *IEEE Commun. Mag.* 55 (5), 80–87. doi:10.1109/MCOM.2017.1600935

Shafi, M., Molisch, A. F., Smith, P. J., Haustein, T., Zhu, P., De Silva, P., et al. (2017). 5G: a Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice. *IEEE J. Select. Areas Commun.* 35 (6), 1201–1221. doi:10.1109/JSAC.2017.2692307

Wang, K. (2018). The Application of the Internet of Things in the 5G Era in the Power System. *Telecom Power Techn.* 35 (5), 187–188. doi:10.19399/j.cnki.tpt.2018.05.078

Wang, Q., Xie, P., Xiong, S., Wei, Y., Liu, Y., Li, W., et al. (2017). Key Technology and Standardization Progress for 5G. *Telecommunications Sci.* 33 (11), 112–122. doi:10.11959/j.issn.1000−0801.2017312

Wang, Y., Chen, Q., Zhang, N., Feng, C., Teng, F., Sun, M., et al. (2019). Fusion of the 5G Communication and Ubiquitous Electric Internet of Things: Application Analysis and Research Prospects. *Power Syst. Techn.* 43 (5), 1575–1585. doi:10.13335/j.1000-3673.pst.2019.0635

Xiang, H., Xiao, Y., Zhang, X., Piao, Z., and Peng, M. (2017). Edge Computing and Network Slicing Technology in 5G. *Telecom Sci.* 33 (6), 54–63. doi:10.11959/j.issn.1000-0801.2017200

Zhang, Y., Yang, T., and Meng, G. (2019). Review and prospect of Ubiquitous Power Internet of Things in Smart Distribution System. *Electric Power Construction* 40 (6), 1–12. doi:10.3969/j.issn.1000-7229.2019.06.001

Zhu, H., and Xiang, F. (2016). Architecture Design and Standardization Progress of 5G Network. *Telecommunications Sci.* 32 (4), 126–132. doi:10.11959/j.issn.1000-0801.2016127

Zou, Z., Chen, T., Chen, J., Hou, Y., and Yang, R. (2021). "Research on Network Security Risk and Security Countermeasures of 5G Technology in Power System Application," in 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 12-14 March 2021. doi:10.1109/IAEAC50856.2021.9390826

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.