Security Protection and Potential of Network Digital Twins

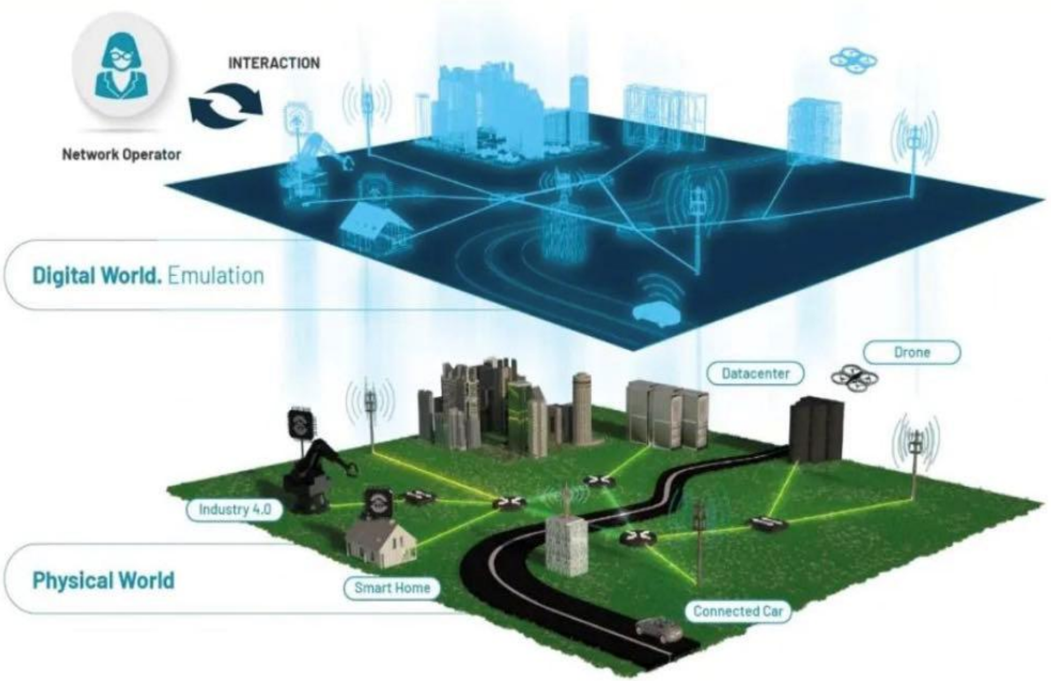
Ke WANG

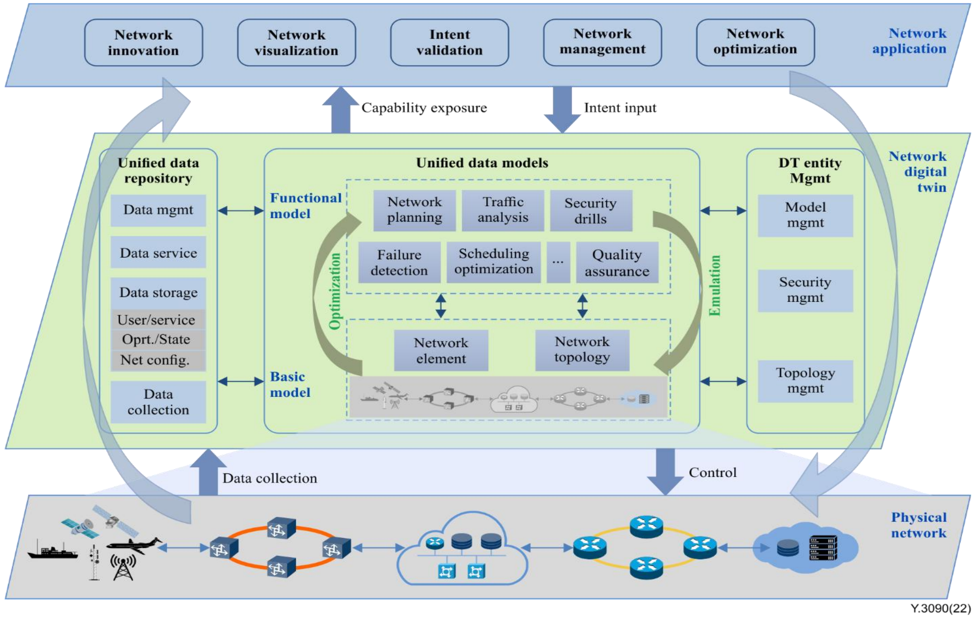
wangkeyj@chinamobile.com

2025.4

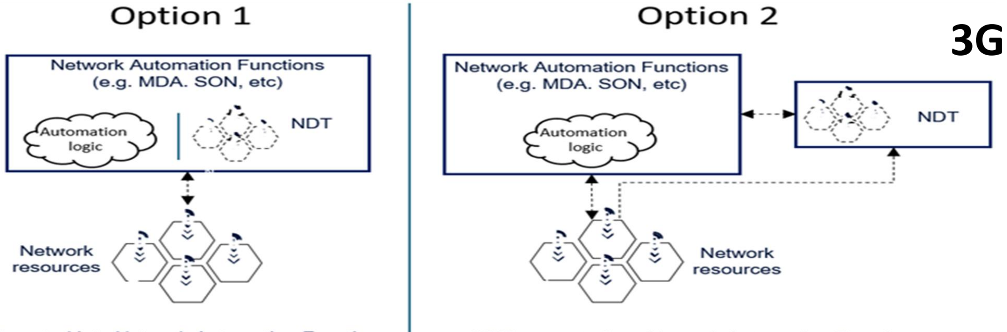
Network Digital Twin

- **Network Digital Twin (NDT)**: virtual replica of mobile network or part of one, that captures its attributes, behaviour and interactions
- NDT can serve as Testbed to accomplish **automation** functionality with **High similarity, Real-time synchronization, High Verifiability**
- NDT can help the network realize **low-cost trial, intelligent decision-making, efficient innovation and predictive maintenance**





ITU



Option 1
Network Automation Functions (e.g. MDA. SON, etc)
Automation logic
NDT
Network resources
Option 2
Network Automation Functions (e.g. MDA. SON, etc)
Automation logic
NDT
Network resources

NDT integrated into Network Automation Functions

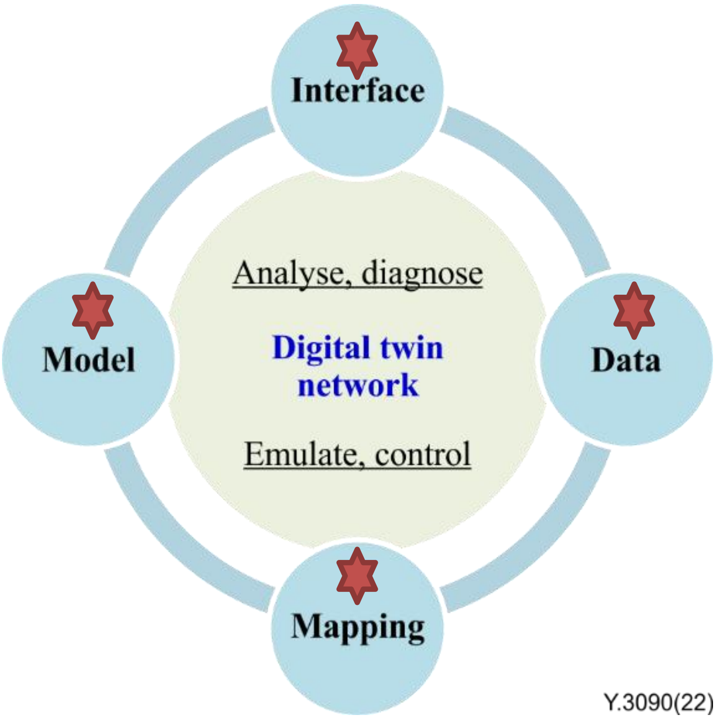
NDT separate from Network Automation Functions

3GPP

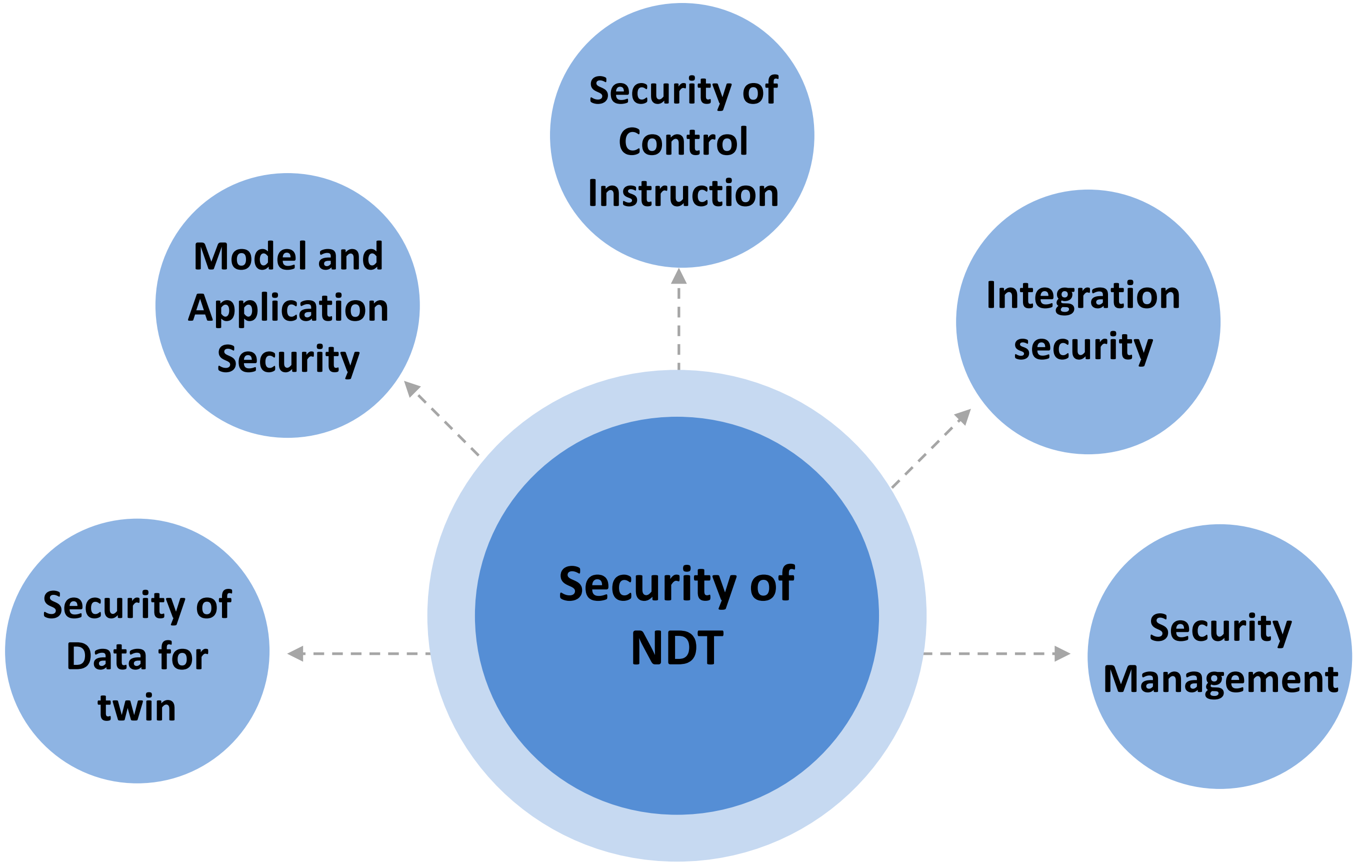
- **Advantages and potentiality**:
- High similarity： it can form the twin of network elements and networks,
- Real-time synchronization: get data from the existing network,
- High accuracy: can simulate attacks directly, quickly, accurately and dynamically.

Security Protection of NDT

- Data, model, interfaces and mapping of **NDT face security threats**
- Security threats need to be addressed in the operation of the **digital twin as part of network**, and the security mechanisms need to **meet the twin characteristics**.



Y.3090(22)



Security of Control Instruction
Model and Application Security
Integration security
Security of NDT
Security of Data for twin
Security Management

Protection of Data for twinning

- Leakage of data or unauthorized access by applications may lead to the leakage of privacydata -》 confidentiality and privacy protection requirements
- Tampered or untrustworthy data can not be used for modelling and analysis in NDT -》 data trustworthiness.
- The security requirements of data sources, models, network are complex, diverse, and changeable, -》 dynamic and differentiated security protection mechanisms.

Diversified security requirements from data sources

Comprehensive representation and precise expression of the network involve collection of various types of data from network

Diversified security requirements from models and applicaitons

Application models with multiple classed, scales and levels may have different security restrictions and requirements

Diversified non-security requirements

Digital twins need to track the state changes of the real network. the tolerance levels for the time overhead and information loss of the data security mechanisms used vary

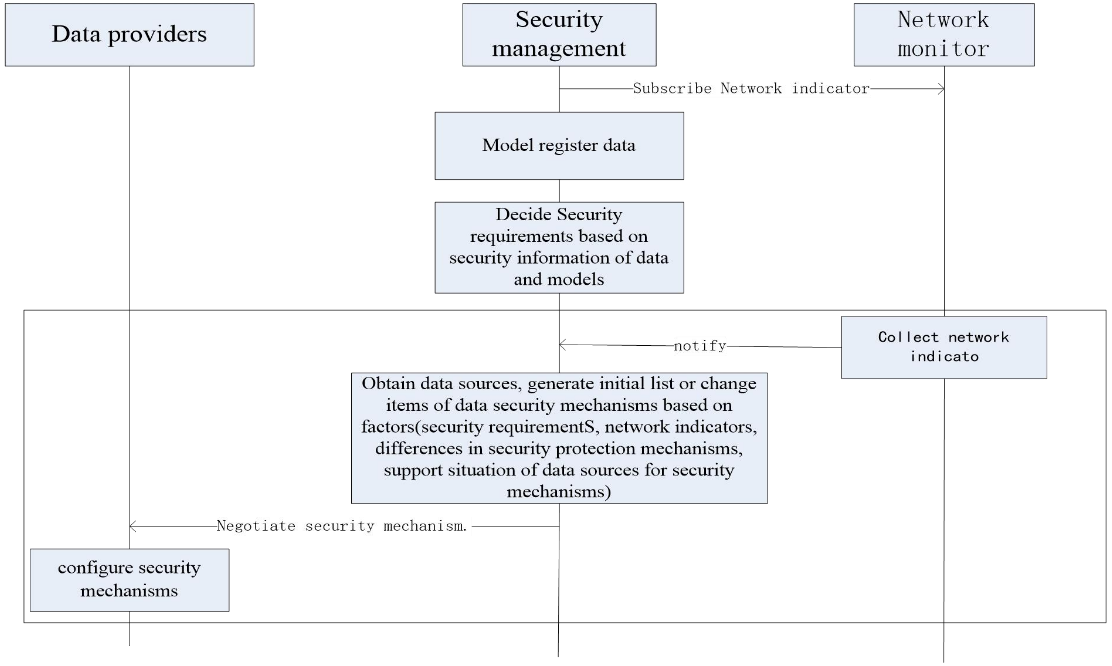
Dynamically changing network status

Content of the collected twin data may change dynamically according to factors like network bandwidth conditions, faults, and security attacks, so as to achieve a balance among real-time performance, accuracy, and overhead.

Protection of Data for twinning

	Confidentiality	Privacy	Trust	Real-time
Diversified Requirements	- None - Visible/Invisible for Data Depository/Channel/Models - Traceable	- With/Without privacy protection	- high level/ Basic trustworthyness	- real-time - no need
Diversified Measures	- access control: ACL/block and allow list/token/DLT - channel encryption - data encryption in repository - end-to-wnd attribute-based encryption mechanisms	- data collectin consent - declassification - security computing	- Trustworthiness of data source identity (optional): authentication, identity in DLT - Trustworthiness of data source behavior (optional): TEE, zero trust, attack awareness - Trustworthiness of data transmission and storage (mandatory): Integrity check: hash, digital signature - Trustworthiness of data ownership (mandatory): Logs, data identity on the blockchain	- not activated - high-speed - basic

Adaptive selection and adjustment of security mechanisms



Data providers

Security management

Network monitor

Subscribe Network indicator

Model register data

Decide Security requirements based on security information of data and models

notify

Collect network indicato

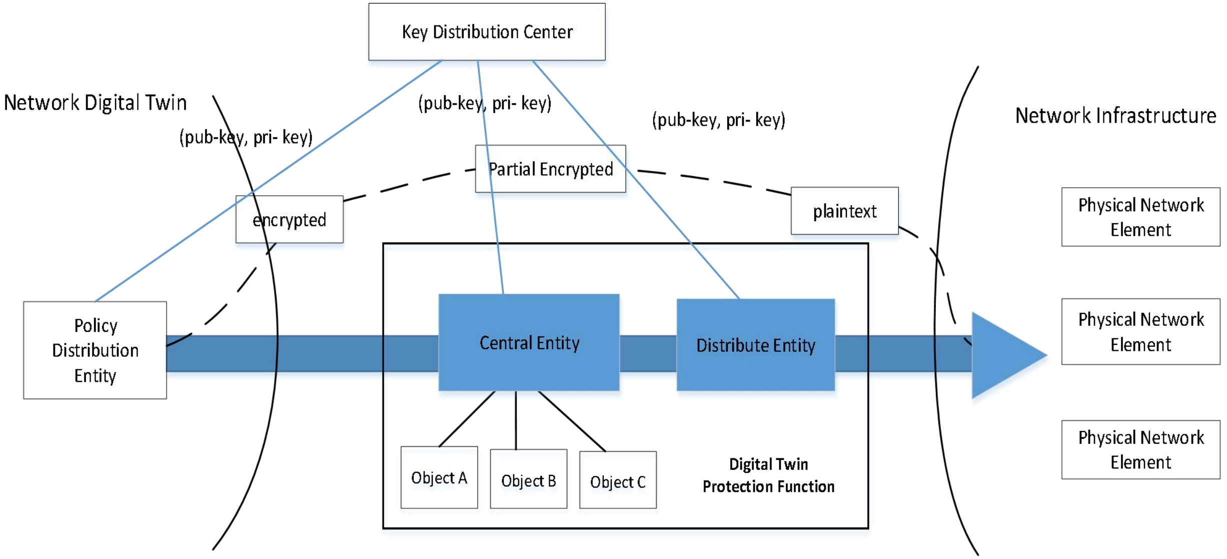
Obtain data sources, generate initial list or change items of data security mechanisms based on factors(security requirementS, network indicators, differences in security protection mechanisms, support situation of data sources for security mechanisms)

Negotiate security mechanism.

configure security mechanisms

Protection of Control Interaction

- Attacks on the twin may pose a threat to the personal safety, equipment security, and business security in the physical network
- It is necessary to design a security mechanism to ensure the security of the control issuing interface from the twin network to the physical network
  - Confidentiality and Integrity Requirements
  - Stability Rquirements
  - Unforgeability Requirements



□ **DTPF(Digital Twin Protection Function)** :

Central Entity （CE)

Distribute Entity(DE)

□ **Security Technologies:**

① **Cross-domain security classification**：Provide different security services according to the security requirement levels of the physical network;

② **Minimize Privacy Design**：CE can only partially decrypt the required information.

③ **Multi-dimensional policy validation**：Source verification, policy authenticity verification, target matching verification, etc.

Protection of Models

Confidentiality and Integrity Requirements

- It is required to support the integrity and confidentiality protection of the models and the data used.

- It is recommended to support building multiple twins for multiple network security domains and to collect data as the corresponding security requirements for each domain.

Access control Requirements

- It is required to allocate necessary privileges to the models with different purposes and security levels to access the data, other models and network functions (NFs).

- It is required for the model, or any other network function that may store the model, to be able to check that the entity (e.g., network applications or other models) is authorized to retrieve that model.

Model Detection and evaluation Requirements

- It is required to detect security vulnerabilities before a model is deployed to eliminate potential risks and damages in advance.

- It is required for a model to be auditable in order to evaluate the security of the model including whether the data is sufficient for twinning and simulation, the affected objects (e.g., NFs, services, users) of the control instructions and privilege of data used for models.

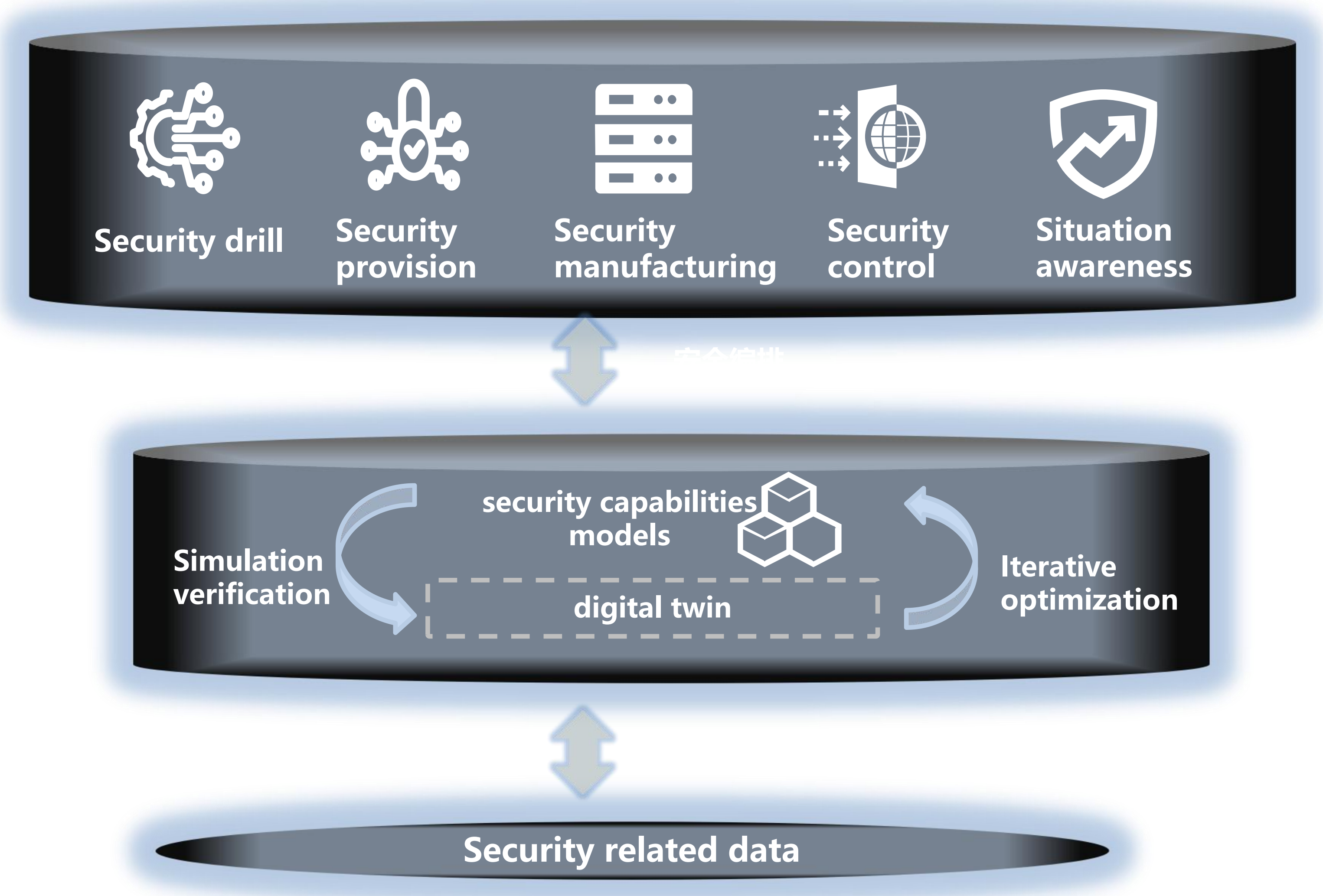
- It is recommended to provide mechanisms to ensure that the model is able to operate normally when facing abnormal data input and attacks.

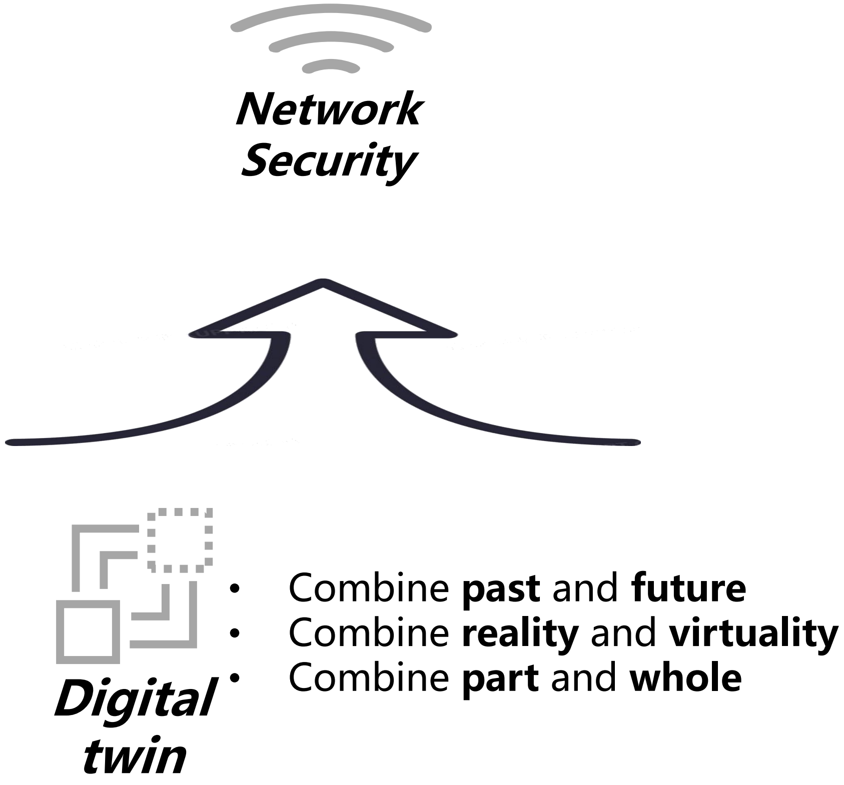
- It is required to support policy conflict detection. It is recommended to set different priorities for different models to ensure that the security control cannot be bypassed.

- It is recommended to support monitoring and alert of the consistency between the basic model and the physical network.

Security Potential of NDT

- Base on NDT, various network situations can be sensed; security risk or security devices could be simulated; different security strategies could be generated, tested, optimized and decided





- Combine **past** and **future**
- Combine **reality** and **virtuality**
- Combine **part** and **whole**

Benefits of using DTN to support network security applications

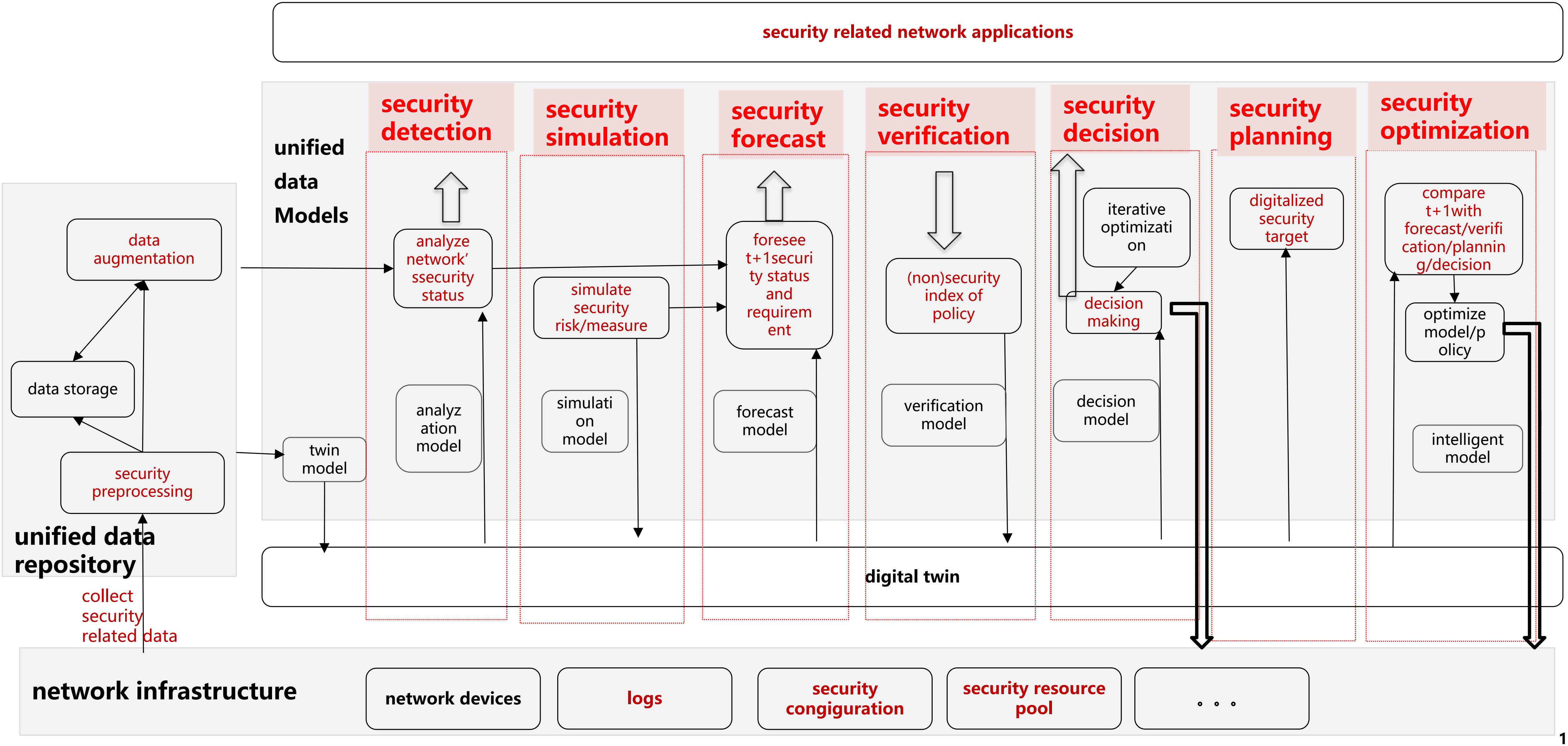
- **Verifiability**: DTN creates an accurate digital network simulation platform which can be used as a test bed. Security policy or new security devices can be fully tested without interrupting the running network before deployed in the physical network. Security attacks can be simulated in the twin to know the possibility which can help decide the security prevention plan.

- **Real-time**: DTN is defined to have the capability to represent the real state of the physical entity in real-time and support the synchronization of control information execution from a virtual entity to a physical entity within acceptable time delay range. So it can help sense and deal with security issues of the network in time.

- **Crossing-time**: Based on the data repository, DTN can support network traceability from the history data. Based on the model and data, DTN can support network prediction through simulation.

- **Visualization**: DTN can support the visualization of the network changes through the digital twin which can help mining valuable security related information hidden in the network. DTN is also defined to have the capability to display the process of network simulation and optimization. This can help the users to better understand the security policy and status of network they are using.

How can NDT support security related network applications



security related network applications

unified data Models

security detection

analyze network’ ssecurity status

analyzation model

security simulation

simulate security risk/measure

simulation model

security forecast

foresee t+1security status and requirement

forecast model

security verification

(non)security index of policy

verification model

security decision

iterative optimization

decision making

decision model

security planning

digitalized security target

security optimization

compare t+1with forecast/verification/planning/decision

optimize model/policy

intelligent model

data augmentation

data storage

security preprocessing

twin model

unified data repository

collect security related data

digital twin

network infrastructure

network devices

logs

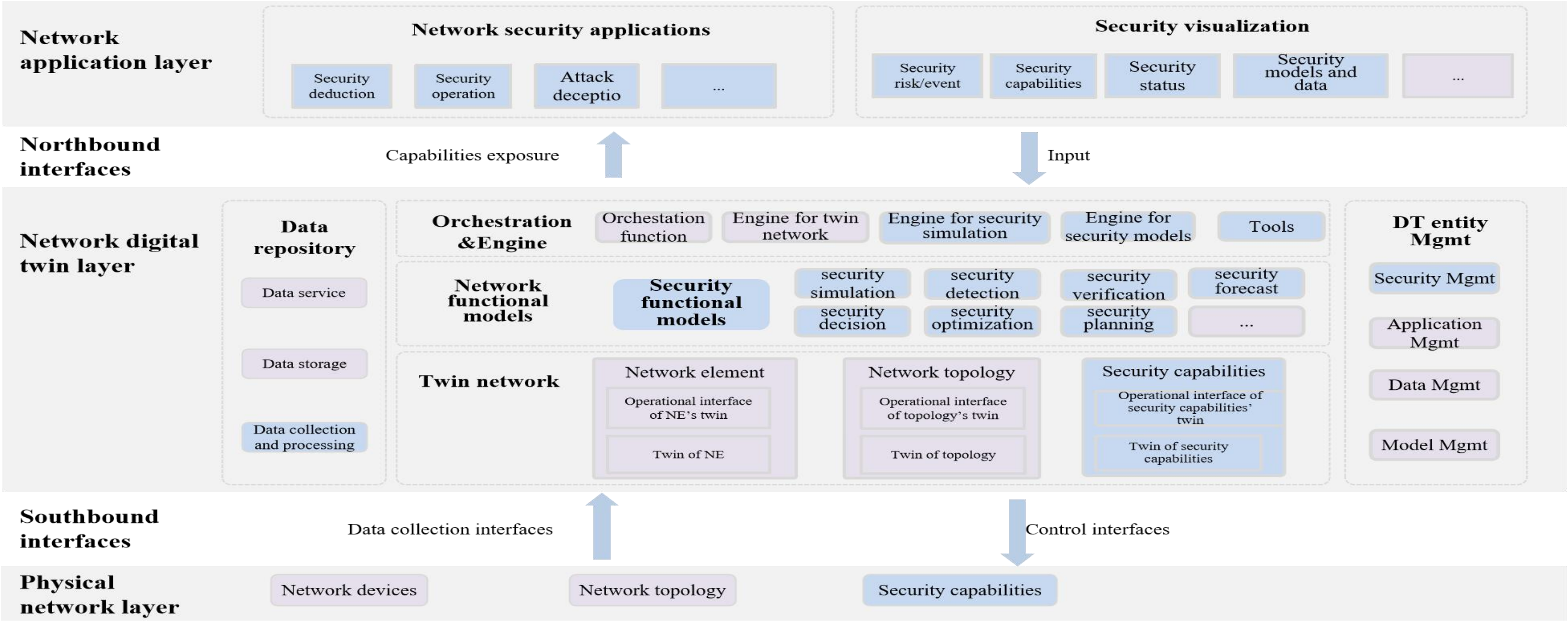
security congiguration

security resource pool

。。。

Architecture of NDT supporting security applications

- Standardization is needed to attain unification and standardization of the interoperability.
- ITU-T Y.2090, X.2011, X.dtns, X.fr-vsasi, 3GPP 28561 and so on



Network application layer

Network security applications

Security deduction

Security operation

Attack deceptio

...

Security visualization

Security risk/event

Security capabilities

Security status

Security models and data

...

Northbound interfaces

Capabilities exposure

Input

Network digital twin layer

Data repository

Data service

Data storage

Data collection and processing

Orchestration &Engine

Orchestration function

Engine for twin network

Engine for security simulation

Engine for security models

Tools

Network functional models

Security functional models

security simulation

security detection

security verification

security forecast

security decision

security optimization

security planning

...

Twin network

Network element

Operational interface of NE's twin

Twin of NE

Network topology

Operational interface of topology's twin

Twin of topology

Security capabilities

Operational interface of security capabilities' twin

Twin of security capabilities

DT entity Mgmt

Security Mgmt

Application Mgmt

Data Mgmt

Model Mgmt

Southbound interfaces

Data collection interfaces

Control interfaces

Physical network layer

Network devices

Network topology

Security capabilities

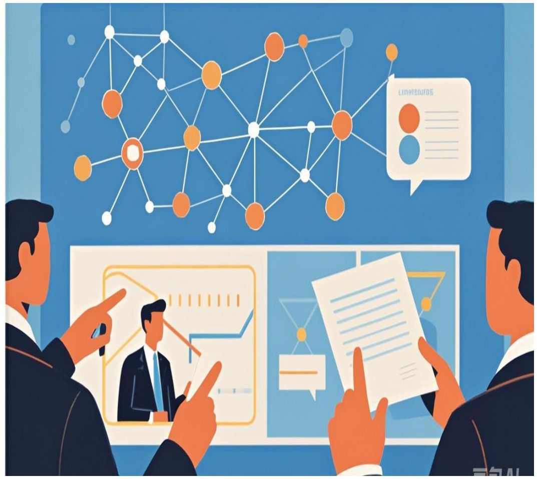
Security drill using NDT

Test in production network

Advantages:
accurate

Drawbacks:
impact the users and services using the network

Security analysis



Advantages:
low cost, convinient

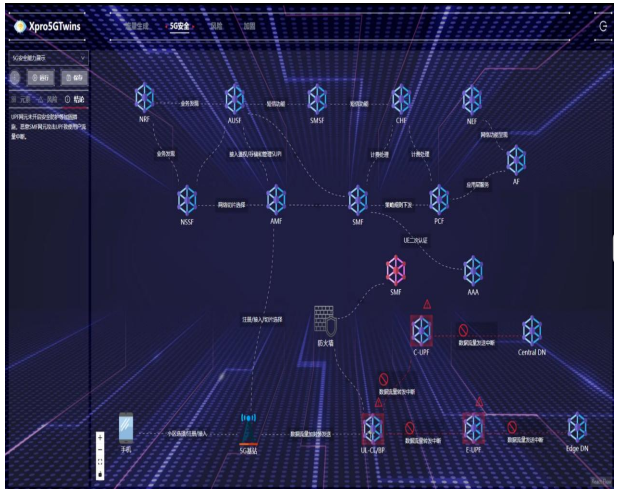
Drawbacks:
inaccurate, hard to deal with complex situation

Security drills on simulated environment

Advantages:
High-degree simulation, High accuracy

Drawbacks:
Higher cost, Limited network environment, outdated network data

Security drills on NDT



UPF网元未开启安全防护等加固措施，恶意SMF网元攻击UPF致使用户流量中断。

Advantages:
Real-time and High-degree simulation, High accuracy, Low cost

Drawbacks:
Need integration with network

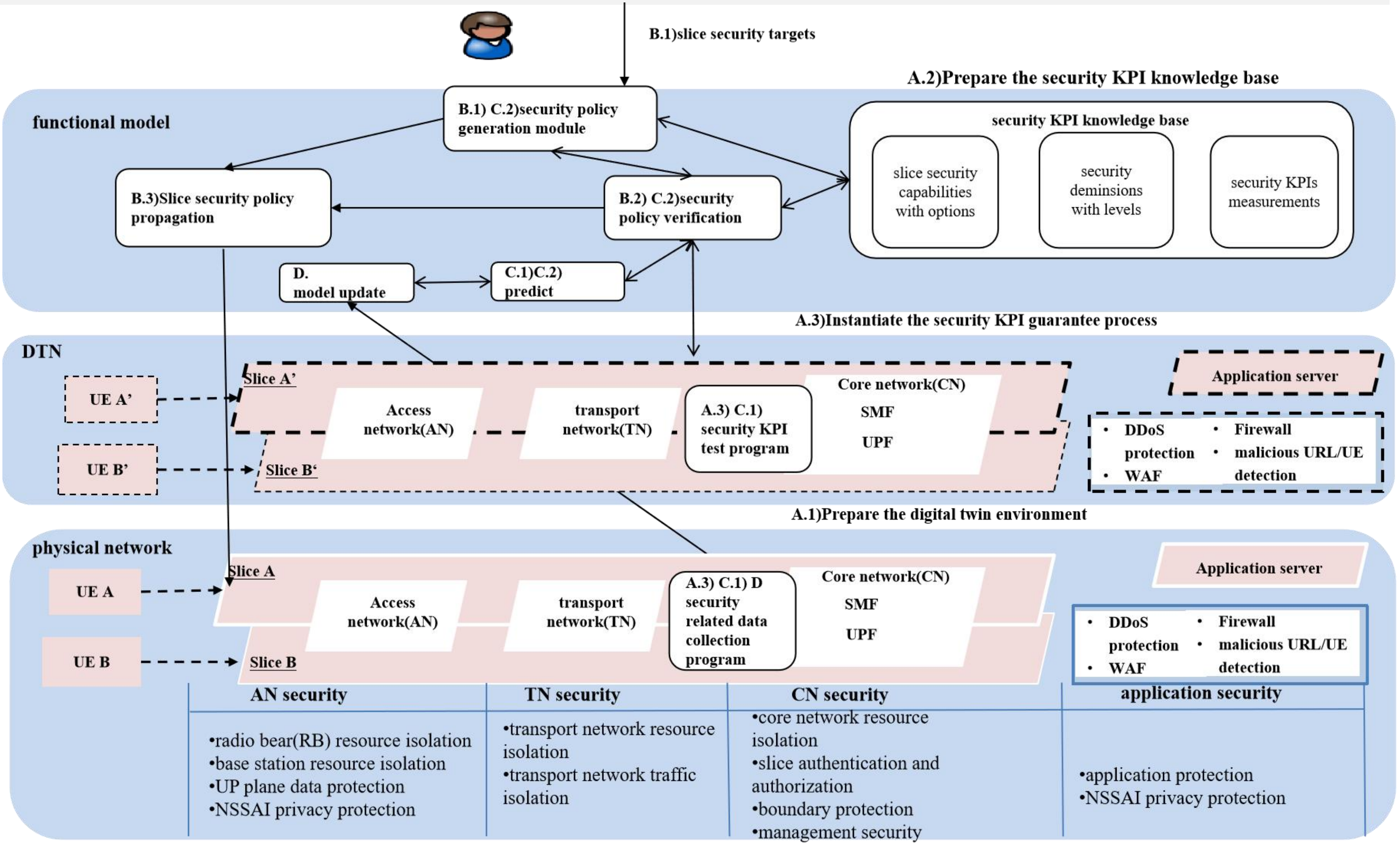
Security provisioning and guarantee using NDT

- The diverse forms of networks and businesses require differentiated security guarantees. By utilizing NDT, digital twin based slice security provisioning and service guarantees can fully leverage the advantages of expert experience and implementation verification, promoting precise matching between industry demand and network security capabilities

□ **Intent driven slice security provision**

□ **Differentiated slicing security capability selection for vertical industries**

□ **Slice security service guarantee**



B.1)slice security targets

A.2)Prepare the security KPI knowledge base

functional model

B.1) C.2)security policy generation module

B.3)Slice security policy propagation

B.2) C.2)security policy verification

security KPI knowledge base

slice security capabilities with options

security deminsions with levels

security KPIs measurements

D. model update

C.1)C.2) predict

A.3)Instantiate the security KPI guarantee process

DTN

Slice A'

UE A'

UE B'

Slice B'

Access network(AN)

transport network(TN)

A.3) C.1) security KPI test program

Core network(CN)

SMF

UPF

Application server

- DDoS protection
- WAF
- Firewall
- malicious URL/UE detection

A.1)Prepare the digital twin environment

physical network

Slice A

UE A

UE B

Slice B

Access network(AN)

transport network(TN)

A.3) C.1) D security related data collection program

Core network(CN)

SMF

UPF

Application server

- DDoS protection
- WAF
- Firewall
- malicious URL/UE detection

AN security

•radio bear(RB) resource isolation
•base station resource isolation
•UP plane data protection
•NSSAI privacy protection

TN security

•transport network resource isolation
•transport network traffic isolation

CN security

•core network resource isolation
•slice authentication and authorization
•boundary protection
•management security

application security

•application protection
•NSSAI privacy protection

Enhance the certainty of network security using NDT

- The next generation mobile communication network is developing towards larger scopes, more complex architectures, supporting more business types
- There will be more security risk, attack paths, and security capabilities in future networks, which will result in a huge challenge to evaluating and measuring security risks and security desicions

Scenarios	Usecases	Security risks
Immersive Communication	immersive XR, remote multi-sensory telepresence, and holographic communications	• The key rate used for encryption and integrity protection of ultra-high-speed data streams is difficult to match the communication rate • Multi-modal sensing data transmission bring privacy issues due to the irreversibility of human biometric data
Hyper Reliable and Low-Latency Communication	communications in an industrial environment for full automation, control and operation	• Whether availability and reliability of network services can still be maintained facing attacks • Whether security issues can be protected, detected, responded and recovered in time
Massive Communication	smart cities, health, energy, agriculture, and those requiring a variety of IoT devices without battery or with long-life batteries	• Signalling storm • Large amount of encryption and difficult management of authentication key distribution on the network side. High complexity and insufficient security strength on the terminal side
Ubiquitous Connectivity	Air-Space-Ground、IoT and mobile broadband communicatio	• Open enviroment, complex structure and weak node processing of SAGIN make vulnerabilities easier to exploit • Integration and interworking of heterogeneous networks and diversified terminal environments bring cross-domain security issues
Artificial Intelligence and Communication	Distributed computing, AI applications, digital twin	• Security risks of new technologies itself: AI- data imbalance, algorithm deviation, DTN- unreliable data, vulnerabilities in models, etc. • Automatic detection and disposal based on new technologies: AI- threat feature extraction, malware identification, self-adaptive arrangement of security policies, etc. DTN- security simulation, deduction, testing, etc
Integrated Sensing and Communication	Wide-area multi-dimensional perception provides spatial information about equipment, its movement and environment.	• Wireless environment is more vulnerable to communication information eavesdropping, deceptive interference attacks, denial of service, and perceived privacy disclosure. • Location privacy issues

Thanks

Security KPIs

Access control
Authentication
Non-repudiation
Data confidentiality
Communication security
Data integrity
Availability
Privacy

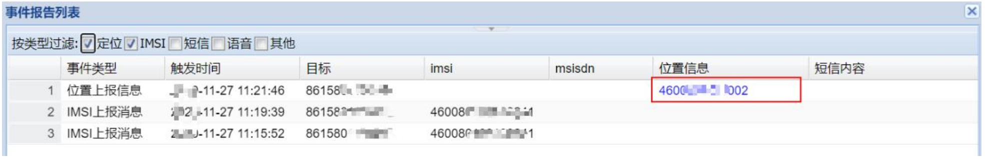
KPI-Communication security

Capabilities	*Boundary protection*		***Application service protection***		***Communication security***	***cost***	***latency***
Options	on	off	on	off			
Combinations	off		off		base	low	low
	off		on		midum	midum	midum
	on		off		midum	midum	midum
	on		on		high	high	high

Security KPI measurements

test	**security capabilities**	**measurement**	**level**
Attackers use traffic meters to launch DDoS attacks on the exposed assets of the 5G network, such as SYN Flood, UDP Flood, etc	reduce exposure to network assets	only reduce attacks on some assets	low
	deploy anti-ddos device and	can prevent DDoS attacks	high
Send the SS7 location query request to the target user's network through the signaling instrument to obtain the user's current location information	no FW	obtain user's location information	low
	deploy signal FW and SS7 interception strategy	can identify attack signals	high

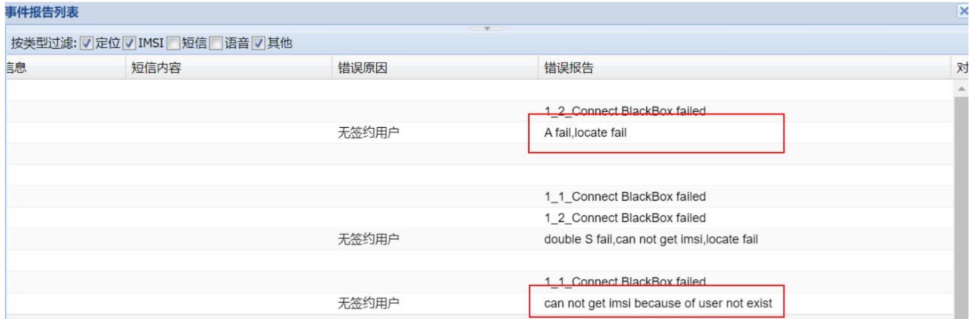
e.g., effect of SS7 interception



事件报告列表

按类型过滤: ☑定位 ☑IMSI □短信 □语音 □其他

	事件类型	触发时间	目标	imsi	msisdn	位置信息	短信内容
1	位置上报信息	[redacted]-11-27 11:21:46	86158[redacted]			4600[redacted]002	
2	IMSI上报消息	[redacted]-11-27 11:19:39	86158[redacted]	46008[redacted]			
3	IMSI上报消息	[redacted]-11-27 11:15:52	861580[redacted]	46008[redacted]1			



事件报告列表

按类型过滤: ☑定位 ☑IMSI □短信 □语音 ☑其他

信息	短信内容	错误原因	错误报告	对
		无签约用户	1_2_Connect BlackBox failed A fail,locate fail	
		无签约用户	1_1_Connect BlackBox failed 1_2_Connect BlackBox failed double S fail,can not get imsi,locate fail	
		无签约用户	1_1_Connect BlackBox failed can not get imsi because of user not exist	