ETSI GR ZSM 010 V1.1.1 (2021-07)

Zero-touch network and Service Management (ZSM); General Security Aspects

Disclaimer

The present document has been produced and approved by the Zero-touch network and Service Management (ZSM) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGR/ZSM-010_SecStudy

Keywords

countermeasures, security, threat analysis

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Zero-touch network and Service Management (ZSM).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Security consideration is critical to commercially deploy ZSM framework based solutions. The present document covers security threat and risk analytics on ZSM framework based on assets of ZSM framework and attack mechanism defined in Common Attack Pattern Enumeration and Classification (CAPEC) project of MITRE (see [i.4]).

Several key security issues are identified according to risk analysis result, and solutions were proposed to mitigate the risks, which include:

- Trust issue of cross domain service management and build relationship between multiple management domains.
- Potential security risk caused by vulnerability of management function and security assurance of ZSM management function.
- Security isolation and security requirement fulfilment in multi-tenancy environment of ZSM Framework.

- Access control for management service provided by multiple domain service producers of ZSM framework.
- Leverage existing security specifications to identify security risk of AI/ML model and protect AI/ML models in ZSM framework.

1 Scope

The present document studies the security aspects of the ZSM use cases, framework and solutions, identifies potential security threats and mitigation considerations to be covered in ZSM standardization activities. It aims to outline a list of security controls (aka security countermeasures) in order to raise awareness of security aspects that could be considered in ZSM specifications. The present document will explore the relationship between security controls and technology-specific solutions.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ISO/IEC 27005:2011: "Information technology - Security techniques - Information security risk management".

[i.2] NIST Special Publication 800-30 (Revision 1): "Guide for Conducting Risk Assessments".

[i.3] Recommendation ITU-T X.805 (10/2003): "Security architecture for systems providing end-to-end communications".

[i.4] MITRE Common Attack Pattern Enumeration and Classification (CAPEC) project.

NOTE: Available at https://capec.mitre.org/.

[i.5] MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) project.

NOTE: Available at https://attack.mitre.org/.

[i.6] General Data Protection Regulation (EU GDPR) definitions.

NOTE: Available at https://gdpr-info.eu/art-4-gdpr/.

[i.7] GSMA Network Equipment Security Assurance Scheme (NESAS).

NOTE: Available at https://www.gsma.com/security/network-equipment-security-assurance-scheme/.

[i.8] ETSI TR 133 916 (V15.1.0): "Universal Mobile Telecommunications System (UMTS); LTE; Security Assurance Methodology (SCAS) for 3GPP network products (3GPP TR 33.916 version 15.1.0 Release 15)".

[i.9] Adversarial ML Threat Matrix.

NOTE: Available at https://github.com/mitre/advmlthreatmatrix/blob/master/pages/adversarial-ml-threat-matrix.md#structure-of-adversarial-ml-threat-matrix.

[i.10] ETSI GR SAI 004 (V1.1.1): "Securing Artificial Intelligence (SAI); Problem Statement".

[i.11] ETSI GR SAI 005 (V1.1.1): "Securing Artificial Intelligence (SAI); Mitigation Strategy Report".

[i.12] ISO/IEC TR 24028:2020: "Information technology - Artificial intelligence - Overview of trustworthiness in artificial intelligence".

[i.13] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.14] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.15] ETSI GS ZSM 002: "Zero-touch network and Service Management (ZSM); Reference Architecture".

[i.16] ETSI GS ZSM 007: "Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM".

[i.17] NIST 800-39: "Managing Information Security Risk".

NOTE: Available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

[i.18] ETSI GS ZSM 001: "Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

access control: framework and procedures that authenticate and authorize a management service consumer, and trace the activities of the consumer according to SLA and other policies or regulations

control or countermeasure: technique that puts into place to mitigate (reduce) the potential risk

information system: management functions and management services used in the present document

qualitative risk analysis: risk analysis technique that uses a scale of qualifying attributes to describe the magnitude of potential consequences (e.g. Low, Medium and High) and the likelihood that those consequences will occur

NOTE: An advantage of qualitative analysis is its ease of understanding by all relevant personnel while a disadvantage is the dependence on subjective choice of the scale.

quantitative risk analysis: risk analysis technique that uses a scale with numerical values (rather than the descriptive scales used in qualitative risk analysis) for both consequences and likelihood, using data from a variety of sources

NOTE: The quality of the analysis depends on the accuracy and completeness of the numerical values and the validity of the models used.

risk: likelihood of a threat source exploiting a vulnerability and the corresponding business impact

risk analysis: process that comprehends the nature of risk and determines the level of risk

security assurance: processes and functionalities that evaluate and assess security of a management product

security baseline: set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system

NOTE: Source: [i.2].

tenant: representation of user/group of users/organization that obtained access to the shared application

threat: any potential danger that is associated with the exploitation of a vulnerability

trust model: model that describes ways in which organizations can obtain the levels of trust needed to form partnerships, collaborate with other organizations, share information, or receive information

vulnerability: weakness in a system that allows a threat source to compromise its security

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication, Authorization and Account/Audit
AI	Artificial Intelligence
ANAS	Authentication Administration Service
API	Application Programming Interface
APT	Advanced Persistent Threat
ARAS	Authorization Administration Service
ATT	Adversarial Tactic and Technique
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
BSS	Business Support System
CAPEC	Common Attack Pattern Enumeration and Classification
CDANA	Cross-Domain Authentication Administration/decision
CDANAS	Cross-Domain Authentication Administration Service
CDARA	Cross-Domain Authorization Administration/decision
CDARAS	Cross-Domain Authorization Administration Service
CDIF	Cross-Domain Integration Fabric
CI/CD	Continuous Integration/Delivery
CN	Core Network
CVE	Common Vulnerabilities and Exposures
DAC	Discretionary Access Control
DANA	Domain Authentication Administration/decision
DANAS	Domain Authentication Administration Service
DARA	Domain Authorization Administration/decision
DARAS	Domain Authorization Administration Service
DIF	Domain Integration Fabric
DoS	Denial of Service
DSS	Data Security Standard
EU	European Union
FM	Fault Management
GDPR	General Data Protection Regulation
GPU	Graphic Processing Unit
GSMA	Global System for Mobile communications Association
IAM	Identity and Access Management
IP	Intellectual Property
ISO	International Organization for Standardization
ISV	Independent Software Vendor
IT	Information Technologies
KPI	Key Performance Indicator
LS	Liaison Statement
MAC	Mandatory Access Control
MFA	Multi-Factor Authentication
ML	Machine Learning
NESAS	Network Equipment Security Assurance Scheme
NFV	Network Function Virtualisation
NGFW	Next Generation Firewall
OSINT	Open Source Intelligence
OWASP	Open Web Application Security Project
PCI	Payment Card Industry

PKI	Public Key Infrastructure
PM	Performance Management
RAN	Radio Access Network
SAI	Securing Artificial Intelligence
SAP	Service Access Point
SCAS	Security Assurance Specifications
SDO	Standard Development Organization
SECAM	Security Assurance Methodology
SLA	Service Level Agreement
SLS	Service Level Specification
SSO	Single Sign On
TLS	Transport Layer Security
TM	Trace Management
TRA	Threat and Risk Analysis
TTPs	Tactics, Techniques and Procedures
UEBA	User and Entity Behavior Analytics
VM	Virtual Machine

4 Threat and risk assessment/analysis

4.1 Methodology of threat and risk analysis

4.1.1 General approach of ZSM threat and risk analysis

The present document refers NIST 800-30 [i.2], ISO/IEC 27005 [i.1] and Recommendation ITU-T X.805 [i.3] for security Threat and Risk Analysis (TRA) of ZSM framework and solutions. Qualitative or Semi-Quantitative Assets/Impact-oriented were proposed in the present document and the following aspects would be covered during TRA:

- Define scope of TRA for ZSM. The present document analyses the risk of ZSM framework, use cases, requirements and solutions in E2E service point of view and use top-down approach to assess impacted assets.
- Identify and categorize ZSM assets. The assets include management/managed service, management function, management/managed data, managed resource, etc.
- Identify threats that are relevant to the assets. Threat natural, human or machine origin, accidental or deliberate, internal or external. Threats include destruction, corruption or modification of service or function, theft, removal or loss of data, violation of regulation, etc.
- Identify vulnerabilities and threat surfaces that could be exploited by threat agent. Vulnerabilities includes out of date or mis-designed or mis-configured architecture, software, hardware, etc., as well as deficient management process, policies, etc.
- Identify the existing controls and their effect on the vulnerabilities and threats identified. In the first stage of the present document, no existing security control is considered. The present document can be iteratively updated based on new controls adopted.

NOTE: Vulnerabilities, threats and controls can be changed continuously, and identification of vulnerabilities, threats and controls could be interleaved. E.g. Security controls could reduce threat surface caused by vulnerabilities, therefore the vulnerabilities would not be exploited by threat.

- Determine the likelihood that the identified threat would incur security incident and damage the asset. It can be e.g. very likely, likely, possible, not likely, etc.
- Determine the adverse impacts on the assets from the exploitation of vulnerabilities by threat, and consequence of the provider and consumer of the assets. It can be e.g. Disastrous, Damaging, Harmful, Annoying, etc.
- Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation.

4.1.2 ZSM threat and risk analysis framework

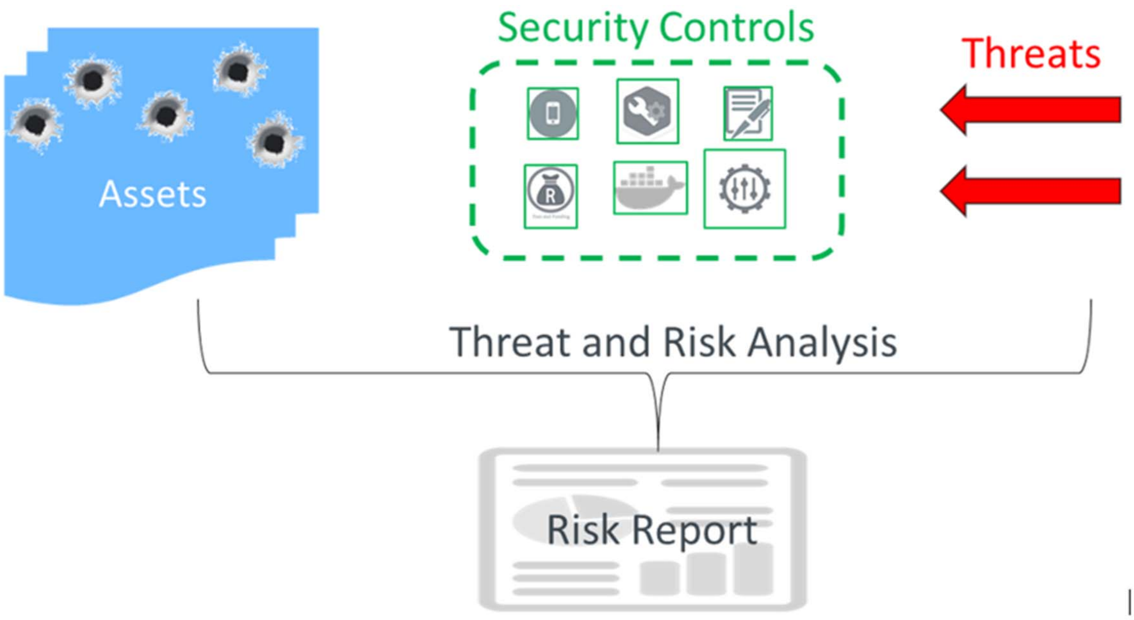

Figure 4.1.2-1: ZSM threat and risk analysis framework

4.1.3 Risk score and priority

There are various methods to calculate risk scale with either qualitative or quantitative scale, or mixture of both. For example, a quantitative risk scale is defined according to quantitative asset value and qualitative threat vulnerability levels. In some other example, a quantitative or qualitative risk scale is defined based on qualitative likelihood of an incident scenario and qualitative estimated business impact against the impact. In yet another example, a quantitative risk scale is calculated with quantitative consequences (asset value) and quantitative likelihood of threat occurrence (taking account of vulnerability aspects).

Considering difficulty to evaluate asset value independently, the present document proposes that the quantitative or qualitative risk scale is calculated based on qualitative likelihood of an incident and Business Impact caused by the incident. Refer to table E.1 b) of ISO/IEC 27005:2011(E) [i.1].

The likelihood of an incident scenario is given by a threat exploiting a vulnerability with a certain likelihood. It depends on the attractiveness of the asset and its susceptibility of the vulnerability to exploitation, as well as the ease of conversion exploiting the vulnerability of the asset into reward and the technical capabilities of the threat agent.

The business impact caused by the incident scenario can be a violation of legal and regulatory obligations, financial loss, disruption of activities, loss of services, incompliance of organizational policies, loss of reputations, unsatisfaction of contract or agreement with a customer, etc.

The table maps likelihood incident scenario against the business impact to quantitative risk score. The resulting risk is measured on a scale of 0 to 8 that can be evaluated against risk acceptance criteria. This risk scale could also be mapped to a simple qualitative risk rating, for example:

- Low risk: 0-2
- Medium Risk: 3-5
- High Risk: 6-8

4.1.4 Typical threat categories considered in ZSM

4.1.4.0 Description

Threats may be deliberate or accidental which may result in, for example, leak of information, damage of services or loss of properties, etc. The business or reputation can also be impacted because of threat of regulation incompliance. The present document lists typical threats may be relevant to ETSI ZSM framework and solutions.

4.1.4.1 Deliberate threat

This table lists potential deliberate threats on ZSM. It is expressed as Adversarial Tactic and Technique (ATT). Adversarial Tactic for ZSM is catalogued in table 4.1.4.1-1. Adversarial Technique could be various on different assets, it will be described in threat analysis for concrete assets.

Table 4.1.4.1-1: List of potential Deliberate threat on ZSM

Threat Cat Id	Adversarial Tactic	Description	Threat Source
D1	Engage in deceptive interactions	Attack patterns within this category focus on malicious interactions with a target in an attempt to deceive the target and convince the target that it is interacting with some other principal and as such take actions based on the level of trust that exists between the target and the other principal. These types of attacks assume that some piece of content or functionality is associated with an identity and that the content/functionality is trusted by the target because of this association. Often identified by the term "spoofing", these types of attacks rely on the falsification of the content and/or identity in such a way that the target will incorrectly trust the legitimacy of the content. For example, an attacker may modify a financial transaction between two parties so that the participants remain unchanged but the amount of the transaction is increased. If the recipient cannot detect the change, they may incorrectly assume the modified message originated with the original sender. Attacks of these type may involve an adversary crafting the content from scratch or capturing and modifying legitimate content.	Individual • Outsider • Insider Organization • Competitor Nation-State
D2	Abuse Existing Functionality	An adversary uses or manipulates one or more functions of an application in order to achieve a malicious objective not originally intended by the application, or to deplete a resource to the point that the target's functionality is affected. This is a broad class of attacks wherein the adversary is able to alter the intended result or purpose of the functionality and thereby affect application behavior or information integrity. Outcomes can range from information exposure, vandalism, degrading or denial of service, as well as execution of arbitrary code on the target machine.	Individual • Outsider • Insider Organization • Competitor Nation-State
D3	Manipulate Data Structures	Attack patterns in this category manipulate and exploit characteristics of system data structures in order to violate the intended usage and protections of these structures. This is done in such a way that yields either improper access to the associated system data or violations of the security properties of the system itself due to vulnerabilities in how the system processes and manages the data structures. Often, vulnerabilities and therefore exploitability of these data structures exist due to ambiguity and assumption in their design and prescribed handling.	Individual • Outsider • Insider • Trusted Insider • Privileged Insider Organization • Competitor • Supplier • Partner • Customer Nation-State

Threat Cat Id	Adversarial Tactic	Description	Threat Source
D4	Manipulate System Resources	Attack patterns within this category focus on the adversary's ability to manipulate one or more resources in order to achieve a desired outcome. This is a broad class of attacks wherein the attacker is able to change some aspect of a resource's state or availability and thereby affect system behavior or information integrity. Examples of resources include files, applications, libraries, infrastructure, and configuration information. Outcomes can range from vandalism and reduction in service to the execution of arbitrary code on the target machine.	Individual • Outsider • Insider • Trusted Insider • Privileged Insider Organization • Competitor • Supplier • Partner • Customer Nation-State
D6	Employ Probabilistic Techniques	An attacker utilizes probabilistic techniques to explore and overcome security properties of the target that are based on an assumption of strength due to the extremely low mathematical probability that an attacker would be able to identify and exploit the very rare specific conditions under which those security properties do not hold.	Individual • Outsider • Insider Organization • Competitor Nation-State
D7	Collect and Analyse Information	Attack patterns within this category focus on the gathering, collection, and theft of information by an adversary. The adversary may collect this information through a variety of methods including active querying as well as passive observation. By exploiting weaknesses in the design or configuration of the target and its communications, an adversary is able to get the target to reveal more information than intended. Information retrieved may aid the adversary in making inferences about potential weaknesses, vulnerabilities, or techniques that assist the adversary's objectives. This information may include details regarding the configuration or capabilities of the target, clues as to the timing or nature of activities, or otherwise sensitive information. Often this sort of attack is undertaken in preparation for some other type of attack, although the collection of information by itself may in some cases be the end goal of the adversary.	Individual • Outsider • Insider • Trusted Insider • Privileged Insider Organization • Competitor • Supplier • Partner • Customer Nation-State
D8	Subvert Access Control	An attacker actively targets exploitation of weaknesses, limitations and assumptions in the mechanisms a target utilizes to manage identity and authentication as well as manage access to its resources or authorize functionality. Such exploitation can lead to the complete subversion of any trust the target system may have in the identity of any entity with which it interacts, or the complete subversion of any control the target has over its data or functionality. Weaknesses targeted by subversion of authorization controls are often due to three primary factors: 1) a fundamental dependence on authentication mechanisms being effective; 2) a lack of effective control over the separation of privilege between various entities; and 3) assumptions and over confidence in the strength or rigor of the implemented authorization mechanisms.	Individual • Outsider • Insider Organization • Competitor • Supplier • Partner • Customer Nation-State
NOTE: This table mainly refers to MITRE Common Attack Pattern Enumeration and Classification (CAPEC) for ZSM specific attack patterns.			

4.1.4.2 Accidental threat

It is used for grouping threats that can accidentally damage information assets.

Table 4.1.4.2-1: List of potential accidental threats on ZSM

Threat Id	Threat Name	Threat Description
A1	Spill sensitive information	Authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
A2	Mishandling of critical and/or sensitive information by authorized users	Authorized privileged user inadvertently exposes critical/sensitive information.
A3	Incorrect privilege settings	Authorized privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low.
A4	Mis-configuration	Administrator erroneously configure a system, e.g. enable a vulnerable port, disable security function, etc.
A5	Communications contention	Degraded communications performance due to contention.
A6	Introduction of vulnerabilities into software products	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.
A7	Disk error	Corrupted storage due to a disk error.
A8	Pervasive disk error	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.
A9	Natural disaster	Loss of data or damage of service caused by the regional disaster.
A10	Infrastructure Failure/Outage	Loss of data or damage of service caused by outage of infrastructure.
A11	Infrastructure Incapability	Degraded security assurance because unexpected limitation of infrastructure.

4.1.4.3 Regulation noncompliance threats

It is used for grouping threats caused by violation of regulatory laws.

Table 4.1.4.3-1: List of potential threats of regulatory incompliance

Threat Id	Threat Name	Regulation Type	Regulation Requirement
R1	Privacy	Regional/Industry Regulation	Privacy of user
R2	Data Exfiltration	Regional Regulation	Boarder control of data
R3	Service Exfiltration	Regional Regulation	Service in specific area
R4	Leak sensitive information	Industry Regulation	Confidentiality of data
R5	IP or license compromising	Regional Regulation	License of Cryptographic or other algorithm

4.1.5 Threat analysis and assessment template

4.1.5.0 Description

There are several threat models defined in security industry, some models categorize threats based on impaction caused by the incident (e.g. description, corruption, disclosure, interruption, etc., defined in ITU-T), some models group threats according to domain of targets (e.g. software, hardware, communication, etc. defined in CAPEC project of MITRE), or attack mechanism (e.g. Deceptive Interaction, Abuse functionality, Manipulate resource, etc. defined in CAPEC project of MITRE), and some models classify threats for different phases of Advanced Persistent Threat (APT) (e.g. Initial Access, persistent, lateral movement and exfiltration, etc., defined in ATT&CK project of MITRE (see [i.5])).

The present document proposes ZSM threat analysis and assessment based on assets of ZSM framework and classifies threats according to attack mechanism defined in CAPEC project of MITRE.

Following pattern will be adopted as template of threat and risk report.

4.1.5.1 Asset description

This clause describes the functionality and value of the asset in general, the construction of the asset (e.g. software, hardware, etc.), the potential owner and supply chain of the asset, external and internal interface of the asset, technologies used in the asset, and potential lifecycle of the asset and possible deployment area of the asset, etc.

Furthermore, this clause identifies vulnerabilities of the asset which may be exploited by a threat agent.