

Recommendation

ITU-T Y.3060 (09/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Future networks

Autonomous networks – overview on trust



ITU-T Y-SERIES RECOMMENDATIONS

**Global information infrastructure, Internet protocol aspects, next-generation networks,
Internet of Things and smart cities**

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
General	Y.100-Y.199
Services, applications and middleware	Y.200-Y.299
Network aspects	Y.300-Y.399
Interfaces and protocols	Y.400-Y.499
Numbering, addressing and naming	Y.500-Y.599
Operation, administration and maintenance	Y.600-Y.699
Security	Y.700-Y.799
Performances	Y.800-Y.899
INTERNET PROTOCOL ASPECTS	Y.1000-Y.1999
General	Y.1000-Y.1099
Services and applications	Y.1100-Y.1199
Architecture, access, network capabilities and resource management	Y.1200-Y.1299
Transport	Y.1300-Y.1399
Interworking	Y.1400-Y.1499
Quality of service and network performance	Y.1500-Y.1599
Signalling	Y.1600-Y.1699
Operation, administration and maintenance	Y.1700-Y.1799
Charging	Y.1800-Y.1899
IPTV over NGN	Y.1900-Y.1999
NEXT GENERATION NETWORKS	Y.2000-Y.2999
Frameworks and functional architecture models	Y.2000-Y.2099
Quality of Service and performance	Y.2100-Y.2199
Service aspects: Service capabilities and service architecture	Y.2200-Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250-Y.2299
Enhancements to NGN	Y.2300-Y.2399
Network management	Y.2400-Y.2499
Computing power networks	Y.2500-Y.2599
Packet-based Networks	Y.2600-Y.2699
Security	Y.2700-Y.2799
Generalized mobility	Y.2800-Y.2899
Carrier grade open environment	Y.2900-Y.2999
FUTURE NETWORKS	Y.3000-Y.3499
CLOUD COMPUTING	Y.3500-Y.3599
BIG DATA	Y.3600-Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800-Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	Y.4000-Y.4999
General	Y.4000-Y.4049
Definitions and terminologies	Y.4050-Y.4099
Requirements and use cases	Y.4100-Y.4249
Infrastructure, connectivity and networks	Y.4250-Y.4399
Frameworks, architectures and protocols	Y.4400-Y.4549
Services, applications, computation and data processing	Y.4550-Y.4699
Management, control and performance	Y.4700-Y.4799
Identification and security	Y.4800-Y.4899
Evaluation and assessment	Y.4900-Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3060

Autonomous networks – overview on trust

Summary

Recommendation ITU-T Y.3060 provides an overview on trust for autonomous networks. It introduces the background and necessities of trust study in areas of network autonomy and network intelligence. The concepts of trust for autonomous networks are explained and defined in context. Basic principles are also explained and described in detail. In addition, an overall workflow model for a trusted autonomous network is introduced.

Use cases of trust for autonomous networks are also provided in the appendix.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.3060	2023-09-29	13	11.1002/1000/15638

Keywords

Autonomous networks, basic principles, concepts, trust, workflow.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2023

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere.....	1
3.2 Terms defined in this Recommendation.....	1
4 Abbreviations and acronyms	2
5 Conventions	2
6 Introduction	2
6.1 Background of trust topic in areas of network autonomy and network intelligence	2
6.2 Necessity of trust for AN.....	3
7 Concepts	3
8 Basic principles of trusted AN.....	3
8.1 Accountability	4
8.2 Equitability	4
8.3 Explainability	4
8.4 Robustness.....	5
8.5 Safety.....	5
9 Developing a trusted AN	5
9.1 Workflow model for a trusted AN.....	5
9.2 Initiation of trust for a trusted AN.....	6
9.3 Continuous trust for a trusted AN	7
9.4 Consideration of basic principles while developing a trusted AN	7
Appendix I – Use cases of trust for autonomous networks.....	8
I.1 Trust for operation, administration and maintenance of an autonomous network.....	8
I.2 Trust for knowledge exchange of ANs.....	9
I.3 Trust for AI relevant technologies for network automation in an AN	10
Bibliography.....	12

Recommendation ITU-T Y.3060

Autonomous networks – overview on trust

1 Scope

This Recommendation mainly focuses on the overview on trust for autonomous networks.

The scope of this Recommendation includes:

- Introduction of trust in areas of network autonomy and network intelligence;
- Relevant concepts of trust for autonomous networks;
- Basic principles of trusted autonomous networks;
- Developing trusted autonomous networks.

The appendix describes several use cases of trust for autonomous networks.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3052] Recommendation ITU-T Y.3052 (2017), *Overview of trust provisioning in information and communication technology infrastructures and services*.

[ITU-T Y.3101] Recommendation ITU-T Y.3101 (2018), *Requirements of the IMT-2020 network*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 autonomous network [b-3GPP TS 28.100]: Telecommunication system (including management system and network) with autonomy capabilities which is able to be governed by itself with minimal to no human intervention.

3.1.2 IMT-2020 [ITU-T Y.3101]: Systems, system components, and related aspects that provide far more enhanced capabilities than those described in [b-ITU-R M.1645].

3.1.3 trust [ITU-T Y.3052]: The measurable belief and/or confidence which represents accumulated value from history and the expecting value for the future.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 trusted autonomous network: An autonomous network which is trustworthy enough (i.e., able to work correctly as intended) for the network to be authorized to work partly or completely autonomously.

3.2.2 trust in an autonomous network (TiAN): A measurable and quantifiable degree of trustor's confidence in an autonomous network to govern itself with minimal to no human intervention.

3.2.3 trustor in an autonomous network: One who/which has the authority to authorize a network and/or a relevant entity to govern itself with minimal to no human intervention.

3.2.4 trustee in an autonomous network: A network or network relevant entity with autonomous capabilities which can be authorized to govern itself with minimal to no human intervention.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AI	Artificial Intelligence
AN	Autonomous Network
FPGA	Field Programmable Gate Arrays
ICT	Information and Communication Technologies
IS	Information Society
ML	Machine Learning
OAM	Operation, Administration and Maintenance
SoC	System-on-Chip
SVM	Support Vector Machine
TiAN	Trust in Autonomous Network

5 Conventions

None.

6 Introduction

6.1 Background of trust topic in areas of network autonomy and network intelligence

As a decision-making behaviour, trust is affected by past experience and associated predictions for the future. Previously, the study of trust in automated systems has been a topic of psychology; however, in the development and evolution of technologies, artificial intelligence (AI) poses unique challenges: the AI user has to trust AI, changing the interaction between a user and a system into a relationship. Trust itself is a complexity-reduction mechanism, whose importance increases the less that is known about the technology or technologies. In information and communication technologies (ICT), trust has been studied and discussed since the application or usage of machine intelligence. For communication networks, with the development of network systems and evolution of AI technology applications, operators are recommended to gradually hand over their work and duties to autonomous and intelligent network systems which have self-X properties (the abilities to monitor, operate, recover, heal, protect, optimize and reconfigure themselves), also known as autonomous networks (ANs), and which are applied in areas of network planning, network deployment, network operation, network optimization, network service provisioning and assurance, etc.

Trust relevant topics have been studied and discussed worldwide since intelligent and autonomous technologies were gradually studied and applied. [ITU-T Y.3052] defines trust as "the measurable belief and/or confidence which represents accumulated value from history and the expecting value for the future", and trust can be one of the critical words to identify features of the future information society and its infrastructure.

6.2 Necessity of trust for AN

During the development and evolution of AN, the following serious problems and challenges may occur: AN solutions including reliable ones and risky ones are difficult to distinguish and may not be applied in real/commercial networks due to the lack of trust or confidence from operators; especially when operators are facing the pressure of network quality assessment and market competition, traditional but more familiar solutions may be preferred. On the other hand, a lack of sufficient trust and confidence on the part of operators will mean it cannot get enough application opportunities in the real/commercial network, thus, loses the chance to learn and evolve to a more advanced level. Trust in an AN is essential for its commercial deployment, usage and application, and it is also important for its evolution; in other words, trust is crucial to AN(s).

7 Concepts

The trust concept itself is a complicated notion with different meanings depending on the participators and situations, and it is influenced by both measurable and unmeasurable factors. There are various kinds of trust definitions and this brings great difficulties to establish some common and general notation which holds regardless of personal dispositions or differing situations. Generally, trust is considered a computational value depicted by a relationship between trustor and trustee, described in a specific context, measured by trust metrics and evaluated by a mechanism [b-ITU-T TR Trust].

8 Basic principles of trusted AN

To achieve authorization(s) from a trustor in AN, it is necessary to clearly determine whether the AN is trustworthy and even how much it can be trusted; besides, at the very beginning of relevant standardization work, clear and explicit descriptions for the basic principles of trusted AN are necessary. It is suggested that the basic principles of trusted AN be taken into consideration and met before one or more trustors in AN carries out authorization. The basic principles are as follows:

- **Accountability** requires an AN and its provider(s) or vendor(s) to explain, justify and take responsibility for any decisions and actions made by the AN; at the same time, it is required to be auditable throughout the whole life cycle of the AN.
- **Equitability** requires an AN and its provider(s) or vendor(s) to take deliberate steps – in the AN life-cycle – to avoid intended or unintended bias and unfairness which would inadvertently cause harm, damage or loss.
- **Explainability** is the ability to describe how an AN works, i.e., how an AN is making decisions and carrying out actions. Explanations are supposed to be produced regarding both the procedures followed by the AN (i.e., their inputs, methods, models, algorithms and outputs) and the specific decisions and actions taken. These explanations are recommended to be accessible to people with varying degrees of expertise and capabilities, including to the general public.

NOTE – For the explainability principle to take effect, the AN engineering discipline is supposed to be sufficiently advanced such that technical experts possess an appropriate understanding of the technology, development processes and operational methods of its AN systems, including the ability to explain the sources and triggers for decisions through transparent, traceable processes and auditable methodologies, data sources and design procedures and documentations.

- **Robustness** refers to the stability, resilience, adaptability, timely, performance, etc. of an AN system dealing with changing ecosystem(s). An AN is recommended to work robustly throughout its life cycle and it is recommended to continually assess and manage potential risks.
- **Safety** of an AN is recommended to be tested, assessed and ensured across the entire life cycle within an explicit and well-defined domain of usage. In addition, any AN will be

designed to also safeguard the data, infrastructures, relevant hardware and software which are impacted.

None of the above basic principles has higher priority than any other, and all are related to each other.

8.1 Accountability

It is the provider/vendor of trustee in an AN who provides/offers/supplies solutions, software, hardware or relevant entities for an AN. In order to achieve trust from the trustor in an AN, the provider/vendor of the trustee in the AN is recommended to take accountability/responsibility for what has been provided, including but not limited to the AN entity, the whole process, actions and decisions throughout the life cycle of an AN.

- The trustee(s) in an AN, i.e., any data, algorithms, methodologies, actions, documentation, executions, are recommended to be auditable.
- Governance processes, functions or structures are recommended to be set in an AN. Accountability requires solid evidence and a clear division of responsibilities; at the same time, well-defined roles, responsibilities and a line of authority are necessary for governance.
- A clearly predetermined division of responsibilities by provider(s)/vendor(s) is necessary, before the trustee in an AN is delivered.
- Before the authorization(s), TiAN evaluation(s) are necessary.

NOTE – In order to make TiAN measurable and quantifiable, the evaluating metrics are recommended to be defined and the evaluation methodologies are also supposed to be explored and described.

8.2 Equitability

As machine intelligence related technologies are being widely and deeply used in ANs, there are serious concerns about biases or unfairness which may be caused by AI or other machine intelligence related technologies, whether intentionally or unintentionally. Through the whole life cycle of an AN, it is necessary to avoid intentional or unintentional biases or unfairness which may cause any harm, damage or loss.

- For an AN, machine intelligence related technologies are recommended to be without any bias or unfairness throughout the whole AN life cycle, i.e., from the beginning of designing to the end of delivering.
- The provider/vendor of an AN system/component is recommended to take accountability/responsibility for the whole execution process. If there is any bias or unfairness found, the provider/vendor may be warned or penalized, etc.

8.3 Explainability

ANs are becoming more and more complex and can be likened to a black box when the machine intelligence or automation related technologies take effect, during which time the trustor in the AN cannot know what has happened within it. Explanations are essential and they are necessary to handover to the trustor in an AN with understandable terminology or expressions that can be understood at least by a specialist/expert who possesses an appropriate understanding of the technology, development processes and operational methods of the AN system. Explainability includes the ability to explain the sources and triggers for any decisions or actions through transparent, traceable processes and auditable methodologies, data sources, design procedure and documentation.

- Self-explaining systems are recommended to be used to detect anomalous behaviour which requires explanations and generates explanations accordingly. On this basis, combining this detection with behaviour classification to classify behaviours into categories with similar causes can reduce the search space for interpretation. Self-explaining systems can enable an AN to self-interpret, detect and classify abnormal behaviours.

- The trustee in an AN is recommended to be able to (self-)explain what has happened in the AN blackbox, including but not limited to any actions, decisions, processes, methodologies, data resources and documentation.
- Understandability is one of the essential factors of explainability for a trustee in an AN to be trusted, so proving itself trustworthy in an understandable way is necessary and key for the trustee in an AN.
- The explanations from the trustee in an AN are recommended to be output as terminology that is understandable at least to specialists/experts. Actually, the explanations maybe in some machine languages, which may be difficult to understand by the trustor in an AN, so the AN development discipline is recommended to be sufficiently advanced that technical experts possess an appropriate understanding of the technology, development processes and operational methods of its AN systems.
- TiAN is supposed to be evaluated. Interpretability is recommended to be one of the essential metrics/indicators for TiAN evaluation and the degrees of transparency, translatability, understandability, explanation accuracy, explanation integrity and explanation of reproduction may directly impact the result of interpretability.
- Transparency of data (resource), algorithm, procedure design, methodology, etc. is recommended to be one of the essential requirements for explainability.

8.4 Robustness

For a trustworthy system, robustness is one of the basic requirements and principles. In order to be trusted, the trustee in an AN is recommended to function robustly throughout its life cycle and it is necessary to continually assess and manage potential risks.

- Robustness is the ability of an AN system to maintain its performance and accuracy when it is applied under highly variable conditions; at the same time, explainability, transparency and security are also the important properties to robustness.
- Stability, resilience, adaptability, timeliness, and performance of an AN are among the attributes of robustness; all of them are recommend to be the metrics/factors of TiAN.

8.5 Safety

It is recommended to ensure safety for an AN, including but not limited to privacy, security, compliance and controllability.

- The Trustee in an AN is recommended to ensure the fulfilment of all the security considerations to be trusted, including (physical) environment and life security, software and algorithm security, information and data security, and attack defence.
- The trustee in an AN is required to be always under control and to be able to be taken over at any time in any condition if necessary.
- Privacy is required to take user privacy, data privacy and algorithm privacy into consideration, so that an AN system/solution can remain safe and trusted.

9 Developing a trusted AN

9.1 Workflow model for a trusted AN

Trust itself can be divided into the objective part and the subjective part. For an AN, trust is recommended to be considered for the subjective part from the trustor's perspective and the objective part from the trustee's perspective. For a trusted AN, both initiation of trust and continuation of trust are essential and necessary for networks working and evolving normally, during which all the basic

principles are required to be considered and satisfied. An overall workflow model for trusted ANs is illustrated in Figure 1.

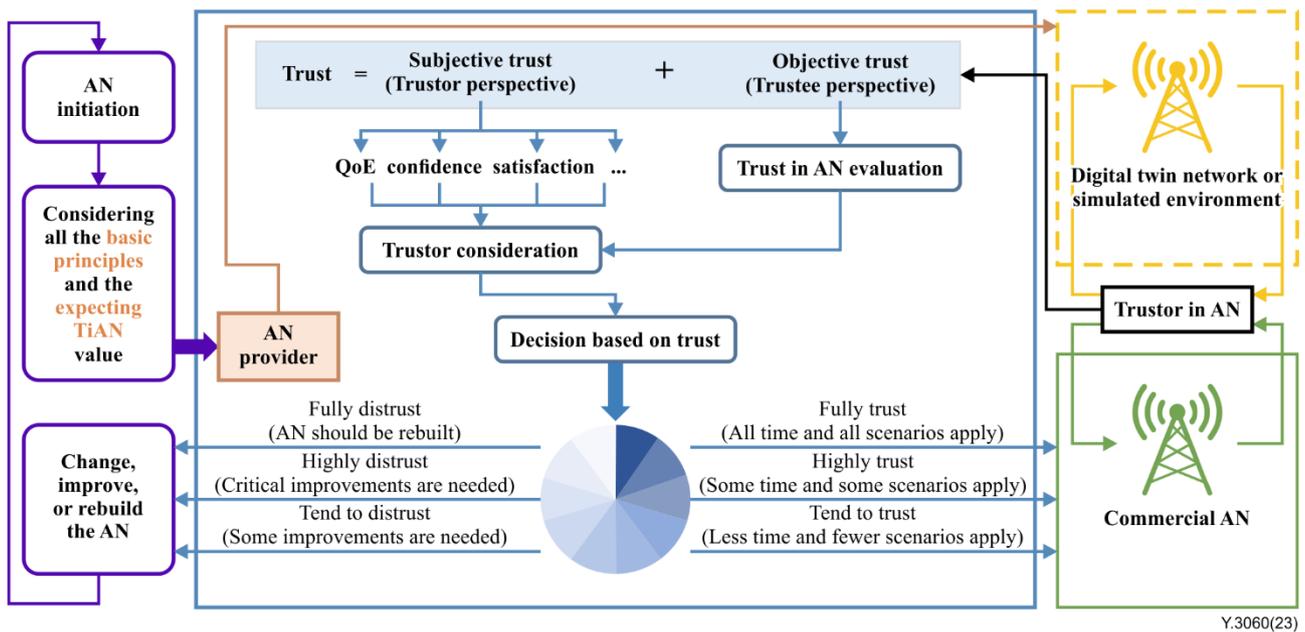


Figure 1 – An overall workflow model for trusted AN

9.2 Initiation of trust for a trusted AN

In order to initiate trust for a trusted AN, the trustor in the AN can give an order to trigger/start the evaluation of TiAN and the relevant process. After TiAN evaluation, the trustor in an AN can take the results into consideration to make decision(s).

- Trustor in AN is supposed to give some order or process to trigger the evaluation of TiAN for the trustee in AN.
- The quantified form of TiAN will depend on the specific scenario or use case; at the same time, a trustor in an AN can also decide the manner of TiAN quantification. The TiAN quantification can be in the form of a percentage, a score, levels, binary, etc.
- The trustor in an AN will take relevant TiAN into consideration, along with the subjective factors of trust, to make the following decision(s):
 - Fully trust: the commercial AN can be applied in all the scenarios all the time until the next evaluation.
 - Highly trust: the commercial AN can be applied in some scenarios in some specific time before next evaluation.
 - Tend to trust: the commercial AN can be applied just for a few scenarios in some specific time until the next evaluation.
 - Tend to distrust: the AN provider(s) should make some improvement(s) in the current AN in order to achieve higher TiAN and gain more trust from the trustor in later evaluations.
 - Highly distrust: the AN provider(s) should make some critical and essential improvements in the current AN, in order to achieve higher TiAN and gain more trust from the trustor in later evaluations.
 - Fully distrust: the AN provider(s) should rebuild the current AN in order to regain trust from the trustor.

- The evaluation of TiAN is recommended to take place in a commercial network environment if possible, and TiAN can also be evaluated in the digital twin network or some simulated environment which are both mirrored from commercial AN.

Trusted AN can be initiated when the trustor in an AN decides to trust, and then the trustee in an AN may be authorized to govern themselves with minimal or no human intervention.

9.3 Continuous trust for a trusted AN

After a trusted AN is initiated, it is recommended that periodic or sporadic TiAN evaluation(s) be permanently carried out to monitor the fluctuation of the TiAN, in order to provide reference to the trustor in the AN to adjust any relevant authorization decisions. AN providers are recommended to continuously improve ANs and relevant solutions, and AN may evolve, to earn trust to maintain the trusted AN.

9.4 Consideration of basic principles while developing a trusted AN

For a trusted AN, basic principles are important, necessary and essential for all the network processes and commercial usage scenarios. It is necessary to satisfy and guaranteed each of them, i.e., accountability, equitability, explainability, robustness and safety, must be guaranteed to some degree. As Figure 1 shows, the AN provider/vendor is recommended to take the basic principles seriously of and expected TiAN before delivering all the basic principles are preconditions for initiating and continuing a trusted AN.

Appendix I

Use cases of trust for autonomous networks

(This appendix does not form an integral part of this Recommendation.)

I.1 Trust for operation, administration and maintenance of an autonomous network

<i>Use case name</i>	Operation, administration and maintenance (OAM) of autonomous network (AN)
<i>Use case description</i>	<p>The dynamic environment, network structure, user behaviour and user distribution drive of the network need to be monitored and optimized continually. Currently, this consumes a lot of experts' time and labour to discover problems, analyse root causes and then formulate solutions for the networks. Therefore, AI and big data technology is necessary to achieve full process automation and intelligent management of the wireless network. Some examples of autonomous management applicable to the OAM of wireless networks are real-time monitoring of data quality, quasi-real-time diagnosis, root cause analysis, recommended solutions and evaluation of impacts of recommended solutions in the radio network, as follows:</p> <ul style="list-style-type: none"> • Real-time monitoring of data quality: there is a need to collect real-time data from the IMT-advanced and IMT-2020 integrated network management, then to compare the consistency of the number of network elements from the collected data, and to achieve data quality monitoring and warning through a visualization panel. • Quasi-real-time diagnosis of abnormal condition in cells: using several categories of key performance indicators, a machine learning (ML) algorithm, e.g., support vector machine (SVM), is used to diagnose network elements in these categories of scenarios such as residential and colleges on a daily/weekly basis, and distribute them to front-line managers. • Root cause analysis and recommended solutions: through collecting tens of thousands of expert experiences, radio network knowledge bases have been established through knowledge graphs to develop intelligent recommendation algorithms and search engines, and to directly provide reasons and recommend solutions for each network element with abnormal condition to first-line experts, thus reducing troubleshooting time and error rate. • Evaluation of processing effects: through a mature evaluation system, the effectiveness of the solution to each abnormal condition is evaluated after the implementation, and then the knowledge base and recommendation algorithm are optimized and the intelligence level of the entire process is continuously improved.
<i>Identities of the AN in this use case</i>	<p>Trustor in the AN: authorizer(s) of the autonomous OAM entity/component(s) Trustee in the AN: autonomous OAM entity/component(s)/process(es)</p>
<i>Considerations of trust for this use case</i>	<p>Considerations of trust for autonomous and intelligent OAM:</p> <ul style="list-style-type: none"> • In the autonomous OAM process(es), the provider(s)/vendor(s) of the trustee in an AN is supposed to take responsibility for all the actions, decisions, procedures, etc. of the trustee in the AN. It is required that, prior to delivery of the AN solution, the division of responsibilities and the appointment of responsible entities are clearly documented. The whole process and life cycle of a trustee in an AN is expected to be auditable. • There is supposed to be no bias or unfairness intentionally or unintentionally throughout the autonomous OAM process.

<i>Use case name</i>	Operation, administration and maintenance (OAM) of autonomous network (AN)
	<ul style="list-style-type: none"> • Some function(s) or process(es) that self-explain the autonomous OAM process(es)/entities are supposed to be set; it is necessary that the explanations are understandable/translatable, transparent and comprehensive. • The trusted autonomous OAM process is supposed to be stable, resilient, adaptable and timely. • The whole autonomous OAM process is supposed to be safe, including but not limited to privacy, data security, compliance and control.
<i>Reference</i>	[b-ITU-T Y Suppl. 71] – Clause 7.6

I.2 Trust for knowledge exchange of ANs

<i>Use case name</i>	Knowledge exchange (import and export) of AN
<i>Use case description</i>	<p>Knowledge may include representation of data about the environment in which the autonomous system is operating, possible actions and consequences, key configuration options, possible measurement parameters and other elements of logic. This use case describes scenarios where knowledge is accessed and used by the actors involved in the AN to realize the use case.</p> <p>General use case scenarios comprise the following steps:</p> <ul style="list-style-type: none"> • Knowledge is imported from outside or peer entities of the AN components. • Knowledge is referred internally in the AN components, e.g., for driving evolution, driving exploration, configuration of automation loops. • Generate report for that is understandable and legible for a human. • Knowledge is stored and updated within the AN components. • Knowledge is exported from the AN components to outside or peer entities.
<i>Identities of the AN in this use case</i>	<p>Knowledge of the AN: a collection of resources (from internal or external) that help in solving a specific type of problem. For an AN, knowledge is supposed to include but not be limited to the intent, rules and experiences.</p> <p>Trustor in the AN: end points' authorizer(s) of knowledge exchange.</p> <p>Trustee in the AN: end points of exchange of knowledge.</p>
<i>Considerations of trust for this use case</i>	<p>Considerations of trust for knowledge exchange (including importing externally and exporting internally) of the AN:</p> <ul style="list-style-type: none"> • For the knowledge exchange of the AN, all the exchanging knowledge need to be auditable; at the same time, the resource(s) of knowledge need to be auditable, too. And the trustee in the AN is supposed to be responsible for the knowledge it offers. • Regarding the knowledge exchange, there is supposed to be no bias or unfairness during the whole process, and knowledge from different resource(s) will be treated equally. Furthermore, the trustee in the AN is supposed to take accountability for any biases and unfairness during the knowledge exchange. • Self-explaining is supposed to exist for the process of knowledge exchanging, to make the trustee in the AN explainable and understandable. • The whole process of knowledge exchange is supposed to be stable, resilient, adaptable and timely, i.e., robust. • Data security and privacy need to be taken seriously during the exchanging of knowledge, including import and export.
<i>Reference</i>	[b-ITU-T Y Suppl. 71] – Clause 7.1

I.3 Trust for AI relevant technologies for network automation in an AN

<i>Use case name</i>	AI relevant technologies (e.g., machine learning, federal learning) for network automation in an AN
<i>Use case description</i>	<p>It may be relevant to consider the following aspects for this specific use case:</p> <ul style="list-style-type: none"> • AI-enabled applications are increasingly being deployed at the edge. Low latency, low power consumption and small footprint are considerations for AI applications at the edge. Accelerated, AI-enabled applications at the edge are important enablers for future networks. • As AI technology evolves AI models evolve, and the acceleration platform must also be adaptable and at the same time satisfying the requirements above. Also, reduced time to market, development time and cost to reach production readiness are important factors influencing deployment decisions by network operators. Fully customized circuit board is no longer widely suitable due to the high cost. • Solutions that are pluggable into a larger edge application, providing both the flexibility of a custom implementation with the ease-of-use and reduced time to market of an off-the-shelf solution, are needed. • Adaptive computing includes hardware that can be highly optimized for specific applications such as field programmable gate arrays (FPGAs). In addition to FPGAs, new types of adaptive hardware such as adaptive system-on-chip (SoC) which contains FPGA fabric, coupled with one or more embedded CPU (central processing unit) subsystems, have been introduced recently. • Prebuilt platforms, APIs and software tools enable full customization of the adaptive hardware, enabling even more flexibility and optimization. This can be used to design highly flexible, yet efficient systems at the edge. • Exploiting the development and adoption of standards in interface and protocols at the edge, different AI-enabled edge applications can use similar hardware components. <p>Following are related steps in this use case scenario:</p> <ul style="list-style-type: none"> • Given an AI/ML model layered architecture, the following considerations need to be applied: (a) concurrency in processing of layers, (b) fragmentation/buffering between layers versus offloading of layers into compute, (c) precision versus performance and energy efficiency. • Given the specific goals and constraints of the AI/ML model, consider the trade-off between the complexity of target platform architecture and precision to explore the model architecture and layer compositions. • Transformation of an AI/ML model, going through the process of intermediate representation, optimization, hardware implementation, evaluation and back to training/modelling. • Derive feedback for hardware adaptation and design.
<i>Identities of the AN in this use case</i>	<p>Trustor in the AN: authorizer(s) of network entity/component(s)/process(es) Trustee in the AN: entity/component(s)/process(es) which applies to AI relevant technologies</p>

<i>Use case name</i>	AI relevant technologies (e.g., machine learning, federal learning) for network automation in an AN
<i>Considerations of trust for this use case</i>	<p>Considerations of trust for AI relevant technologies for network automation of the AN:</p> <ul style="list-style-type: none"> • In network automation with the usage/application of AI relevant technologies, firstly, it is necessary to be auditable for the whole process or life cycle of the trustee in the AN; secondly, a clearly predetermined division of responsibilities by the vendor(s) or provider(s) of the trustee in the AN is necessary; last but not the least, TiAN is supposed to be evaluated for the trustor in the AN to make the judgment before authorization(s). • As the usage of AI relevant technologies needs to prevent any intended or unintended biases and unfairness, it is necessary that the trustee in the AN be auditable to make sure that there are no biases or unfairness. • In order to achieve trust from the trustor in the AN, the trustee in the AN is supposed to self-explain or have some explaining process to make a series of relevant explanations to the trustor in the AN. Based on the explanation(s) from the trustee in the AN, it is also necessary for the explanation(s) to be understandable for the trustor in the AN with or without translation(s). • The process(es), including the function entities which make use or application of AI relevant technologies, are supposed be stable, resilient, adaptable and timely, i.e., robust. • It is necessary to take safety into consideration, including but not limited to system security of the AN, data security, privacy and compliance.
<i>Reference</i>	[b-ITU-T Y Suppl. 71] – Clause 7.22

Bibliography

- [b-ITU-T Y Suppl. 71] Supplement 71 to ITU-T Y-series Recommendations (2022), *Use cases for autonomous networks*.
- [b-ITU-T TR Trust] ITU-T Technical Report (2017), *Trust in ICT*.
- [b-ITU-R M.1645] Recommendation ITU-R M.1645 (2003), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000*.
- [b-3GPP TS 28.100] Technical Specification 3GPP TS 28.100 (2021), *Levels of autonomous network*, 3GPP, V17.0.0.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems