ETSI GR ZSM-017 V0.0.1 (2023-08)

**Group REPORT**

Zero-touch network and Service Management (ZSM) ;

Closed-Loop Automation;

Security aspects

<

***Disclaimer***

The present document has been produced and approved by the <long ISGname> (<short ISGname>) 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

<Workitem>

Keywords

<keywords>

***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:
<https://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](http://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>

If you find a security vulnerability in the present document, please report it through our

Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

***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.

***Copyright Notification***

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI yyyy.

All rights reserved.

Contents

Intellectual Property Rights 4

Foreword 4

Modal verbs terminology 4

Executive summary 5

Introduction 6

1 Scope 7

2 References 7

2.1 Normative references 7

2.2 Informative references 7

3 Definition of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 7

4 Security threats and risks analysis 8

4.1 Gap analysis with ZSM 010 8

4.1.1 Gap between ZSM010 and the present document 8

4.1.2 Relationship between ZSM010 and the present document 8

4.2 Threats and risk analysis on implementation of closed loop automation 8

4.2.1 Monitoring stage 8

4.2.2 Analysis stage 8

4.2.3 Decision stage 8

4.2.4 Execution stage 8

4.3 Threats and risk analysis on coordination of closed loop automation 9

4.3.1 Coordination between hierarchical Closed Loops 9

4.3.2 Coordination between peer Closed Loops 9

4.3.3 Interaction between Closed Loops and external entities 9

5 Potential security solutions 9

5.1 Closed-loop access control for coordination between closed loops 9

5.2 Closed-loop trust management for coordination between closed loops 9

5.3 Closed-loop security exposure for coordination between closed loops 10

6 Potential security requirements and capabilities 10

7 Recommendations 11

Annex A: Change history 12

History 13

# 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](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 “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](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx) (Verbal forms for the expression of provisions).

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

# Executive summary

# Introduction

# 1 Scope

The present document studies analysis of security risks related to closed-loop automation based on ETSI GS ZSM 009 series, ETSI GR ZSM 010, ETSI GS ZSM 014 and ETSI GS ZSM 016, as well as provides the gap analysis with ETSI GR ZSM 010. Based on the analysis conducted, the report will propose new security capabilities for the ZSM framework architecture to support the mitigation of relevant security risks, especially those applicable to the coordination across closed loops from different management domains under the ZSM framework. Recommendations for future work should be included in the present document.

# 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] <Standard Organization acronym> <document number><version number/date of publication>: "<Title>".

[i.2] etc.

# 3 Definition of terms, symbols and abbreviations

Editor’s note: This clause includes security related terminologies used in this study, e.g. access control, threat, risk analysis, trust evaluation, etc.

## 3.1 Terms

## 3.2 Symbols

## 3.3 Abbreviations

# 4 Security threats and risks analysis

Editor's note: This clause provides gap analysis with ZSM010, the previous ZSM security study and includes security threats and risks analysis of closed-loop automation (ZSM009 series, ZSM010 and ZSM014), as well as analyzes how the security risks can impact on service provider and consumer from technical view.This clause also identifies the security risks on implementation/coordination of closed loop both in single mangement domain and across management domains, etc.

## 4.1 Gap analysis with ZSM 010

Editor's note: This clause provides the gap analysis with ZSM 010 to show gap and relationship between ZSM010 and the present document.

### 4.1.1 Gap between ZSM010 and the present document

Editor's note: This clause provides the brief description about ZSM010 and closed loop automation to show new security challenges for ZSM framework which has not been covered by ZSM010 security study.

### 4.1.2 Relationship between ZSM010 and the present document

Editor's note: This clause provides the description about closed loop from assets protection view, and shows how to use the general methodologies for security and risks analysis of the closed loop automation, which also are adopted in ZSM010, such as CAPEC, ATT&CK projects of MITRE and etc.

## 4.2 Threats and risk analysis on implementation of closed loop automation

Editor's note: This clause includes the security risks analysis on Monitoring, Analysis, Decision and Execution 4 closed-loop stages from functional view in the clause 7.2 of ZSM009-1, e.g. flow data security risks in the four closed-loop stages, action plan security risks in the Decision stage, etc.

### 4.2.1 Monitoring stage

### 4.2.2 Analysis stage

### 4.2.3 Decision stage

### 4.2.4 Execution stage

## 4.3 Threats and risk analysis on coordination/governance of closed loop automation

Editor's note: This clause includes the security risks analysis on coordination/governance between different Closed Loops (hierarchical CLs, peer CLs), e.g. sensitive data disclosed on coordination between CLs, malicious tampering for CL goals between CLs, etc.This clause may also provide security risks analysis according to interaction between two or more CLs, e.g. unauthorized interaction between CLs, inappropriate external visibility for management services through CLs, leakage and tampering of interaction information between CLs, etc.

### 4.3.1 Coordination between hierarchical Closed Loops

Editor's note: This clause includes the security risks analysis on coordination between hierarchical Closed Loops. Closed Loop should take into consideration accuracy and timeliness of information received from another CL. This is especially important in the hierarchical closed loop when controlling subordinate CLs across management domain. Some important and sensitive data (e.g. interaction information, CL instance attribute details, closed-loop action plan, etc.) may be disclosed and information may be tampered to make closed loop unable to achieve the accurate goal.

### 4.3.2 Coordination between peer Closed Loops

Editor's note: This clause includes the security risks analysis on coordination between peer Closed Loops, e.g. some important information exchanged between peer Closed Loops may be tampered and make peer Closed Loops unable to cooperate in achieving a common objective.

### 4.3.3 Interaction between Closed Loops and external entities

Editor's note: This clause includes the security risks analysis on internal/external governance between CLs and external entities based on closed loop automation (ZSM009 series) and intent-driven closed loops (ZSM016), e.g. sensitive information (e.g. status, performance, etc.) may be provided to external unauthorized entities when the CLs in a management domain are governed by management services internal to the management domain.

# 5 Potential security solutions

Editor’s note: This clause includes issue descriptions and potential security solutions to mitigate security risks of closed loop automation mentioned in clause 4, especially those applicable to the coordination across closed loops from different management domains under the ZSM framework, e.g. closed-loop access control, closed-loop security data collection, closed-loop security analytics/decision, closed-loop trust management, closed-loop security exposure, etc.

## 5.1 Closed-loop access control for coordination between closed loops

Editor’s note: This clause includes issue description and potential security solutions about closed-loop access control to mitigate the security risk for unauthorized interaction between CLs, which may be based on access control services defined in ZSM014.

### 5.1.1 Issue description

### 5.1.2 Potential proposed solutions

## 5.2 Closed-loop trust management for coordination between closed loops

Editor’s note: This clause includes issue description and potential security solutions about closed-loop trust management to collect different metrics from CLs related to trust, make trust evaluation for the CLA and provide level of trust for specific CLs within a given management domain or across management domains, which may be based on trust management service defined in ZSM014.

### 5.2.1 Issue description

### 5.2.2 Potential proposed solutions

## 5.3 Closed-loop security exposure for coordination between closed loops

Editor’s note: This clause includes issue description and potential security solutions about closed-loop security exposure to mitigate security risks of unexpected exposure of CLs and management services between CLs.

### 5.3.1 Issue description

### 5.3.2 Protential proposed solutions

# 6 Potential security requirements and capabilities

Editor’s note: This clause includes potential security requirements and capabilities according to security risks of closed loop automation in clause 4 and potential security solutions in clause 5, e.g. ZSM Closed Loop Automation framework shall support dynamic authentication policy management for coordination between closed loops, etc.

# 7 Recommendations

Editor’s note: This clause includes the list of recommendations for further standardization activities for ZSM Closed Loop Automation framework according to the threat risks analyzed in clause 4 and the potential security solutions in clause 5 and security capabilities of CLA in clause 6.

Annex A:
Change history

| Date | Version | Information about changes |
| --- | --- | --- |
| November 2023 | 0.0.1 | Skeleton |
|  |  |  |
|  |  |  |
|  |  |  |

# History

|  |
| --- |
| **Document history** |
| <Version> | <Date> | <Milestone> |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

*Latest changes made on 2022-03-14*