ICS 65.020.01
B 65

LY

中华人民共和国林业行业标准

LY/T 2413.3—2015

林业物联网　第3部分:信息安全通用技术要求

Forestry internet of things—Part 3:General technical requirement of information security

2015-01-27 发布　　2015-05-01 实施

国家林业局　发布

前　言

LY/T 2413《林业物联网》分为以下几部分：

——第 1 部分：体系结构；

——第 2 部分：术语；

——第 3 部分：信息安全通用技术要求；

——第 401 部分：标识对象分类规范；

——第 402 部分：标识解析规范。

本部分为 LY/T 2413 的第 3 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由国家林业局提出。

本部分由全国林业信息数据标准化技术委员会(SAC/TC 386)归口。

本部分起草单位：国家林业局信息中心、中国电子技术标准化研究院、同方股份有限公司、深圳市海思半导体有限公司。

本部分主要起草人：李世东、温战强、卓兰、徐全平、陈强、王琦、刘培、白莹。

林业物联网　第3部分:信息安全通用技术要求

1　范围

LY/T 2413的本部分规定了林业物联网的信息安全资产、信息安全威胁、信息安全目标、信息安全策略与机制以及信息安全保护级别划分。

本部分适用于林业物联网的设计、开发、建设、运行、维护和安全评估。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 5271.8　信息技术　词汇　第8部分:安全

3　术语和定义

GB/T 5271.8界定的以及下列术语和定义适用于本文件。

3.1

可用性　availability

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[GB/T 25069—2010,定义2.1.20]

3.2

保密性　confidentiality

使信息不泄露给未授权的个人、实体、进程,或不被其利用的特性。

[GB/T 25069—2010,定义2.1.1]

3.3

数据完整性　data integrity

数据没有遭受以未授权方式所作的更改或破坏的特性。

[GB/T 25069—2010,定义2.1.36]

3.4

新鲜性　freshness

保证接收到数据的时效性,确保没有重放过时的数据。

3.5

客体　object

信息的载体。

[GB 17859—1999,定义3.3]

3.6

安全策略　security policy

指明林业物联网中如何管理、保护和分配资产(包括结点、网络、数据、应用系统等)的一组安全规

则、指导、惯例和实践。

3.7

安全机制　security mechanism

实现安全功能，提供安全服务的一组有机组合的基本方法。

[GB/T 25069—2010，定义 2.2.1.5]

3.8

主体　subject

引起信息在客体之间流动的人、进程或设备等。

[GB 17859—1999，定义 3.4]

4　信息安全资产

林业物联网的信息安全资产如表 1 所示。信息安全模型参见附录 A。

表 1　林业物联网的信息安全资产

类目	信息安全资产
感知层	各种软件和硬件资产，包括网关、路由器、传感器网络结点、传感器等
传输层	通信基础设施，包括有线网络、移动通信网络、卫星通信网络等
应用层	各种软件和硬件资产，包括数据库、应用系统及相关硬件设施等

5　信息安全威胁

5.1　感知层

5.1.1　感知层安全假设

感知层安全假设如下：

a）　传感器网络结点部署合理；

b）　传感器网络设备符合产品设计以及林业特定环境的要求。

5.1.2　感知层安全威胁

感知层安全威胁如下：

a）　攻击者通过假冒身份、占用信道、重发信息、篡改信息等方式导致合法信息被截取、传输异常或信息破坏；

b）　不法厂商或攻击者通过设置或利用后门，导致感知对象和传感器网络设备的信息被窃取、篡改以及传感器网络设备无法正常工作；

c）　有外接传感器或外设接口的传感器网络结点，所采集的数据被未授权拷贝；

d）　由于操作过失导致传感器网络设备无法正常工作或采集的数据丢失。

5.2　传输层

5.2.1　传输层安全假设

传输层安全假设为有线网络、移动通信网络和卫星通信网络等的信息传输是安全的。

5.2.2 传输层安全威胁

传输层安全威胁如下：

a) 攻击者通过实施拦截、篡改、伪造、欺骗、窃听等恶意行为，造成数据传输中断、延时、错误以及数据被窃取或丢失等；

b) 攻击者通过控制网关等网络关键设备，导致通信密钥、广播密钥、配对密钥等泄漏，从而对网络通信安全造成威胁；

c) 攻击者通过破坏网络传输设备或利用软件漏洞等，导致网络无法正常运行；

d) 由于操作过失导致网络传输设备无法正常工作或传输的数据丢失、失真等。

5.3 应用层

5.3.1 应用层安全假设

应用层安全假设如下：

a) 部分应用可以直接访问感知层和传输层；

b) 数据资源中非林业物联网采集的数据是安全的；

c) 数据中心的物理环境是安全的。

5.3.2 应用层安全威胁

应用层安全威胁如下：

a) 攻击者通过入侵应用系统，获得访问目标系统的权限，从而造成用户信息和相关数据被泄漏、篡改等；

b) 攻击者通过在短期内发送大规模的认证请求消息，造成应用服务器过载、瘫痪等；

c) 非法用户使用未授权的业务功能或者合法用户使用未定制的业务功能，造成应用系统紊乱、瘫痪等。

6 信息安全目标

6.1 数据完整性

通过采用国家相关标准规定的完整性机制以及自主完整性策略、强制完整性策略，检测所有数据和敏感标记，确保两者在传输和存储过程中不被有意改动和破坏，并具备更正被改动数据的能力。

6.2 数据保密性

确保具有保密性要求的数据在传输过程中不被泄露给未授权的个人、实体、进程，或不被其利用。需要时，确保数据在存储过程中不被泄露给未授权的个人、实体、进程，或不被其利用。

6.3 数据新鲜性

确保各类设备采用安全机制对接收数据的新鲜性进行验证，并丢弃不满足新鲜性要求的数据，以抵抗对特定数据的重放攻击。

6.4 可用性

确保已授权实体一旦需要，就可访问和使用数据及资源。

6.5 可控性

在保障数据保密性、完整性、可用性的前提下，提供相应的安全控制部件，形成控制、检测和评估环节，构成完整的安全控制回路，实现林业物联网的安全可控。

6.6 抗干扰性

通过采用适当机制防止对数据发送、接收和转发过程的干扰，避免对信息传输造成严重影响。

6.7 可鉴别性

在进行数据或身份鉴别时，通过提供有限的主体反馈信息，确保非法主体不能通过反馈数据获得利益。

7 信息安全策略与机制

7.1 感知层的信息安全策略与机制

7.1.1 感知层的信息安全策略

采用数据备份、加密存储、设置访问权限、身份鉴别、局部隔离等策略，提高数据的安全防范水平。

7.1.2 感知层的信息安全机制

安全机制包括密钥管理机制、安全数据融合机制、加密机制、路由安全机制等。

7.2 传输层的信息安全策略与机制

7.2.1 传输层的信息安全策略

传输层的信息安全策略如下：

a) 通过防范和抵御网络资源可能受到的攻击，保证网络资源不被非法使用和访问，从而保障网内流转数据的安全；

b) 通过防止数据被偶然或故意地非法泄露、更改、破坏或者被非法识别和控制，确保数据的完整、保密、可用。

7.2.2 传输层的信息安全机制

安全机制包括加密机制、路由安全机制、密钥管理机制、访问控制机制等。

7.3 应用层的信息安全策略与机制

7.3.1 应用层的信息安全策略

应用层的信息安全策略如下：

a) 防止信息系统由于存在系统缺陷或安全漏洞，而导致系统被非法控制或使系统性能下降、拒绝服务、宕机；

b) 加强信息系统运行管理，并制定冗灾备份计划。

7.3.2 应用层的信息安全机制

安全机制包括加密机制、认证机制、访问控制机制等。

8 信息安全保护级别划分

8.1 信息安全保护级别

林业物联网的信息安全保护级别分为以下三级：

第一级，林业物联网的信息安全资产受到破坏后，会对林业部门的正常工作造成一般影响，但不会损害公民、法人和其他组织的合法权益，也不会对社会秩序和公共利益造成损害。

第二级，林业物联网的信息安全资产受到破坏后，会对林业部门的正常工作造成较大影响，并对公民、法人和其他组织的合法权益造成一般损害，但不会对社会秩序和公共利益造成损害。

第三级，林业物联网的信息安全资产受到破坏后，会对林业部门的正常工作造成严重影响，对公民、法人和其他组织的合法权益造成较大损害，同时对社会秩序和公共利益构成一般威胁。

8.2 信息安全保护级别划分要素

8.2.1 概述

林业物联网信息安全保护级别划分由两个要素决定：信息安全资产受到破坏时所侵害的客体和对客体造成侵害的程度。

8.2.2 受侵害的客体

林业物联网信息安全资产受到破坏时所侵害的客体包括以下三个方面：

a） 林业部门的正常工作；

b） 公民、法人和其他组织的合法权益；

c） 社会秩序和公共利益。

8.2.3 对客体的侵害程度

对客体的侵害程度由客观方面的不同外在表现综合决定。侵害程度分为以下三种：

a） 造成一般影响、一般损害、一般威胁；

b） 造成较大影响、较大损害；

c） 造成严重影响。

8.3 级别划分要素与级别的关系

林业物联网信息安全保护级别划分要素与级别的关系如表 2 所示。

表 2 保护级别划分要素与级别的关系

受侵害的客体	对客体的侵害程度					
	一般影响	较大影响	严重影响	一般损害	较大损害	一般威胁
林业部门的正常工作	第一级	第二级	第三级			
公民、法人和其他组织的合法权益				第二级	第三级	
社会秩序和公共利益						第三级

附 录 A
（资料性附录）
信息安全模型

通过分析林业物联网面临的安全威胁，从而确定林业物联网需要达到的安全目标，并以此目标为依据，确定安全策略和与之相应的安全机制。

林业物联网信息安全模型参考 ISO/IEC 29180:2012 建立。信息安全模型如图 A.1 所示。

图 A.1 林业物联网信息安全模型

参 考 文 献

[1] GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

[2] LY/T 2170—2013 林业信息系统安全评估准则

[3] 物联网安全威胁与措施.清华大学学报:自然科学版,2011,51(10)

中华人民共和国林业
行业标准
林业物联网　第3部分：信息安全通用技术要求
LY/T 2413.3—2015
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址：www.gb168.cn
服务热线：400-168-0010
010-68522006
2015年4月第一版
*
书号：155066·2-28534

LY/T 2413.3-2015