

ICS 35.020

L09

GA

中华人民共和国公共安全行业标准

GA/T 709—2007

信息安全技术 信息系统安全等级保护基本模型

Information security technology—
Fundamental model of security classification protection for
information system

2007-08-13 发布

2007-10-01 实施

中华人民共和国公安部 发布

目 次

前 言	II
引 言	III
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 信息系统安全总体模型.....	1
5 信息系统安全等级保护基本模型.....	2
5.1 一级安全信息系统.....	2
5.2 二级安全信息系统.....	2
5.3 三级安全信息系统.....	3
5.4 四级安全信息系统.....	5
5.5 五级安全信息系统.....	7
参考文献.....	10

前 言

(略)

引 言

信息系统安全等级保护的基本模型是从系统角度对信息系统安全等级保护各个保护级别的安全模型的描述。

本标准首先给出了信息系统安全的总体模型，然后分别给出了信息系统安全等级保护 1 到 5 级的每一级的可供参考的基本模型。

对于一个复杂的大型信息系统，其不同的组成部份一般会有不同的安全保护要求。本标准以划分安全域的思想给出的信息系统安全等级保护的基本模型能够反映信息系统安全等级保护的需要。安全域是信息系统中实施相同安全保护策略的最小单元。安全域以信息系统所支撑的业务应用的安全需求为基本依据，以数据信息的保护需求为中心划分和确定。

信息安全技术

信息系统安全等级保护基本模型

1 范围

本标准规定了按照 GB 17859-1999 的五个安全保护等级的要求对信息系统实施安全等级保护，其中每一个安全保护等级的基本模型。

本标准适用于按照 GB 17859-1999 的五个安全保护等级的要求对信息系统实施安全等级保护所进行的设计。

2 规范性引用文件

下列文件中的有关条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859-1999 计算机信息系统安全保护等级划分准则

GA/T AAAA-XXXX 信息安全技术 信息系统安全等级保护体系框架

3 术语和定义

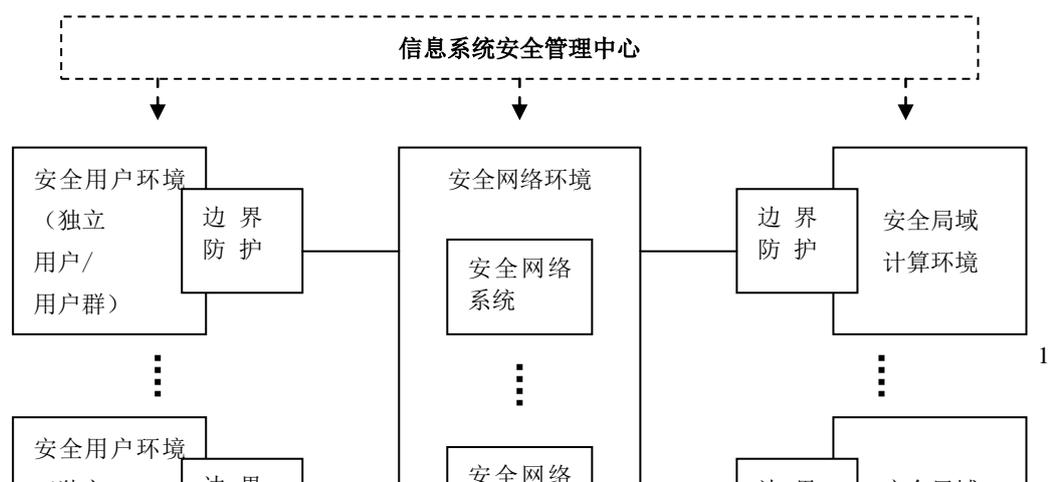
GA/T AAAA-XXXX 确立的术语和定义适用于本标准。

4 信息系统安全总体模型

一个信息系统主要是由实现计算任务的局域计算环境，实现数据传输的网络系统，以及用户/用户群组成。于是，一个安全的信息系统应由以下部分组成：

- 安全的局域计算环境；
- 局域计算环境的边界防护；
- 安全用户环境（独立用户/用户群及）其边界防护；
- 安全的网络系统；
- 信息系统安全管理中心。

图 1 给出由上述部分组成的信息系统安全的总体模型。



5 信息系统安全等级保护基本模型

5.1 一级安全信息系统

典型的一级安全信息系统由一个或多个具有一级安全的局域计算环境及其边界防护、一个或多个具有一级安全的独立用户/用户群及其边界防护以及具有一级安全的网络系统组成。具有一级安全的信息系统的组成与相互关系如图 2 所示。

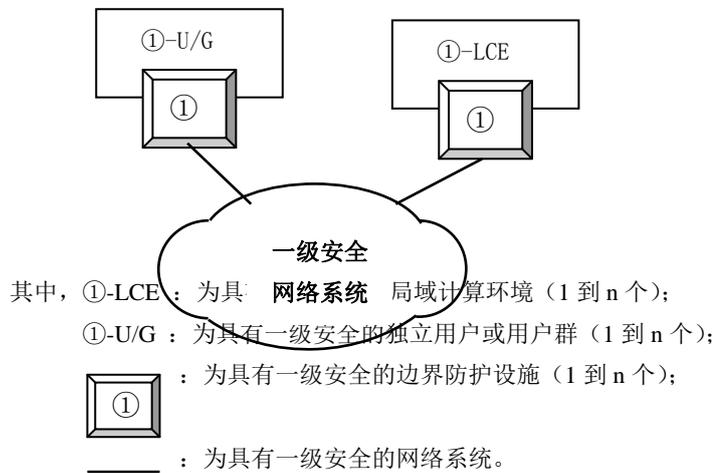


图 2 一级安全信息系统的组成与相互关系

如图 2 所示，一级安全信息系统主要由以下部分组成：

- 1 到 n 个具有一级安全的局域计算环境及其边界防护设施；
- 1 到 n 个具有一级安全的独立用户或用户群及其边界防护设施；
- 具有一级安全的网络系统。

如果信息系统仅由一个局域计算环境组成，则不涉及网络系统的安全问题。

5.2 二级安全信息系统

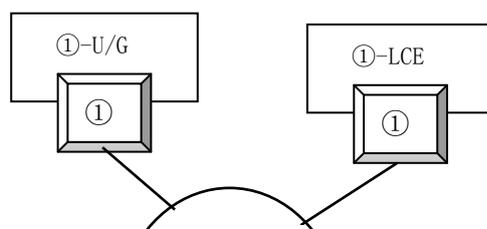
典型的二级安全信息系统可以包含具有一级安全的安全域和具有二级安全的安全域，但至少应具有一个具有二级安全的安全域。

具有一级安全的安全域由一个或多个具有一级安全的局域计算环境及其边界防护、一个或多个具有一级安全的独立用户/用户群及其边界防护以及具有一级安全的网络系统组成。

具有二级安全的安全域由一个或多个具有二级安全的局域计算环境及其边界防护、一个或多个具有二级安全的独立用户/用户群及其边界防护以及具有二级安全的网络系统组成。

根据实际需要，具有二级安全的信息系统可以由只有二级安全的各个安全域组成。

在具有二级安全的信息系统中的数据，应有需要进行二级安全保护的数据，也可以有需要进行一级安全保护的数据，图 3 给出了这种情况的安全信息系统的组成与相互关系。当没有需要进行一级保护的数据时，就只需要考虑进行二级保护的情况。



- 其中，①-LCE：为具有一级安全的局域计算环境（0 到 n 个）；
 ②-LCE：为具有二级安全的局域计算环境（1 到 n 个）；
 ①-U/G：为具有一级安全的独立用户或用户群（0 到 n 个）；
 ②-U/G：为具有二级安全的独立用户或用户群（1 到 n 个）；
：为具有一级安全的边界防护设施（0 到 n 个）；
：为具有二级安全的边界防护设施（1 到 n 个）；
：为具有一级安全的网络系统；
：为具有二级安全的网络系统。

图 3 二级安全信息系统的组成与相互关系

如图 3 所示，二级安全信息系统主要由以下部分组成：

- 0 到 n 个具有一级安全的局域计算环境及其边界防护设施；
- 1 到 n 个具有二级安全的局域计算环境及其边界防护设施；
- 0 到 n 个具有一级安全的独立用户或用户群及其边界防护设施；
- 1 到 n 个具有二级安全的独立用户或用户群及其边界防护设施；
- 具有一级安全的网络系统；
- 具有二级安全的网络系统。

5.3 三级安全信息系统

典型的三级安全信息系统，可以包含具有一级安全的安全域和/或具有二级安全的安全域和具有三级安全的安全域，但至少应具有一个具有三级安全的安全域。

具有一级安全的安全域由一个或多个具有一级安全的局域计算环境及其边界防护、一个或多个具有一级安全的独立用户/用户群及其边界防护以及具有一级安全的网络系统组成。

具有二级安全的安全域由一个或多个具有二级安全的局域计算环境及其边界防护、一个或多个具有二级安全的独立用户/用户群及其边界防护以及具有二级安全的网络系统组成。

具有三级安全的安全域由一个或多个具有三级安全的局域计算环境及其边界防护、一个或多个具有三级安全的独立用户/用户群及其边界防护以及具有三级安全的网络系统组成。

根据实际需要，具有三级安全的信息系统可以由只有三级安全的各部分组成或由具有三级安全的各部分与具有二级安全的各部分或由具有三级安全的各部分与具有一级安全的各部分组成。

对于具有三级安全的典型信息系统，根据其所保护的数据信息的要求及数据分布情况，可以按照全系统同一安全等级保护、分系统不同安全等级保护或虚拟系统不同安全等级保护的方法实施安全等级保护。

在具有三级安全的信息系统中的数据，应有需要进行三级安全保护的数据，也可以有需要进行一级安全保护和/或二级安全保护的数据。图4给出了这种情况的安全信息系统的组成与相互关系。当没有需要进行一级和/或二级保护的数据时，就只需要考虑仅有三级保护的情况，或者仅有一级和三级保护的情况，或者仅有二级和三级保护的情况。

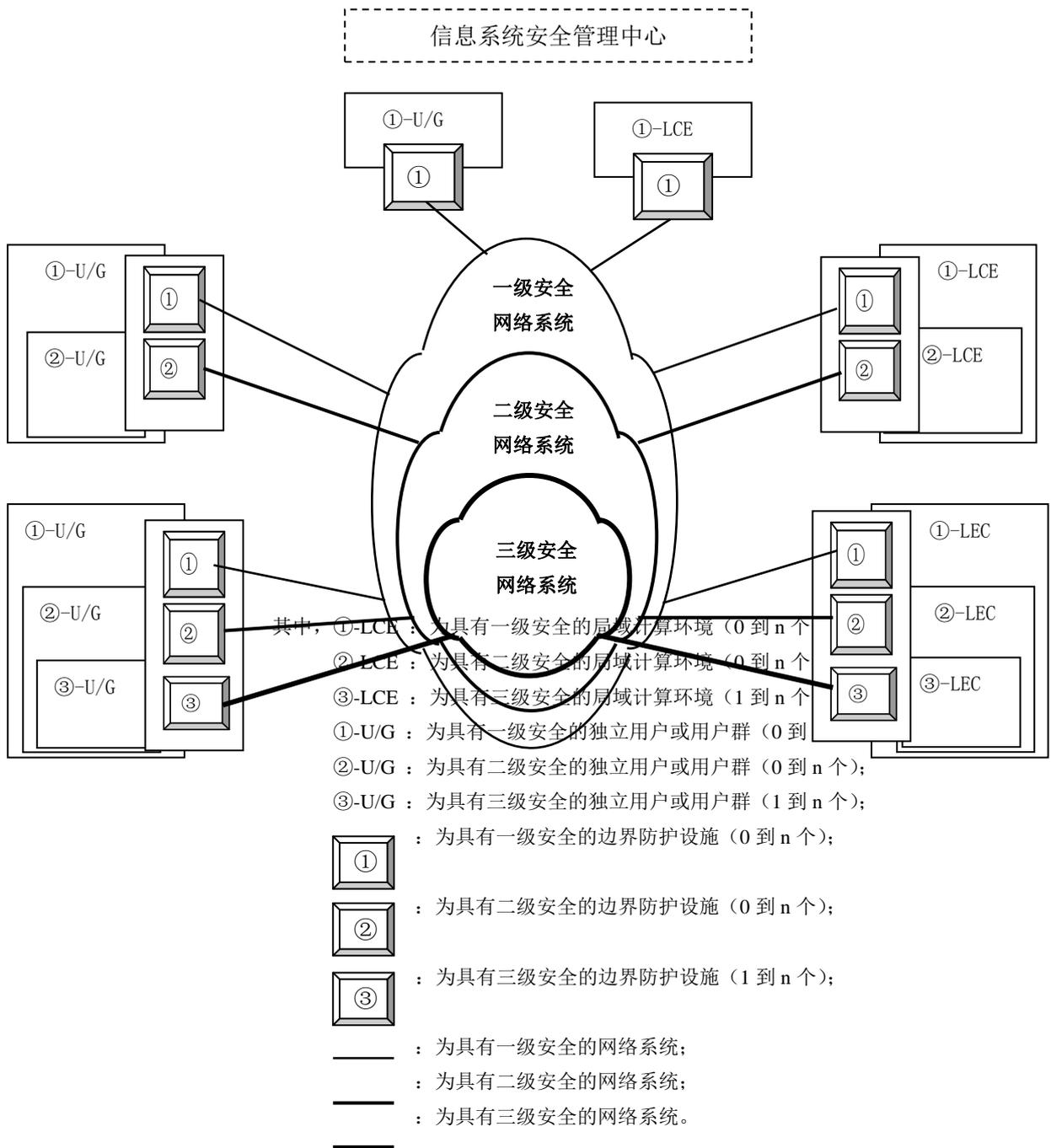


图4 三级安全信息系统的组成与相互关系

如图4所示，三级安全信息系统主要由以下部分组成：

——0到n个具有一级安全的局域计算环境及其边界防护设施；

- 0 到 n 个具有二级安全的局域计算环境及其边界防护设施；
- 1 到 n 个具有三级安全的局域计算环境及其边界防护设施；
- 0 到 n 个具有一级安全的独立用户或用户群及其边界防护设施；
- 0 到 n 个具有二级安全的独立用户或用户群及其边界防护设施；
- 1 到 n 个具有三级安全的独立用户或用户群及其边界防护设施；
- 具有一级安全的网络系统；
- 具有二级安全的网络系统；
- 具有三级安全的网络系统；
- 具有三级安全的信息系统安全管理中心。

5.4 四级安全信息系统

典型的四级安全信息系统，可以包含具有一级安全的安全域和/或具有二级安全的安全域和/或具有三级安全的安全域和具有四级安全的安全域，但至少应包含一个具有四级安全的安全域。

具有一级安全的安全域由一个或多个具有一级安全的局域计算环境及其边界防护、一个或多个具有一级安全的独立用户/用户群及其边界防护以及具有一级安全的网络系统组成。

具有二级安全的安全域由一个或多个具有二级安全的局域计算环境及其边界防护、一个或多个具有二级安全的独立用户/用户群及其边界防护以及具有二级安全的网络系统组成。

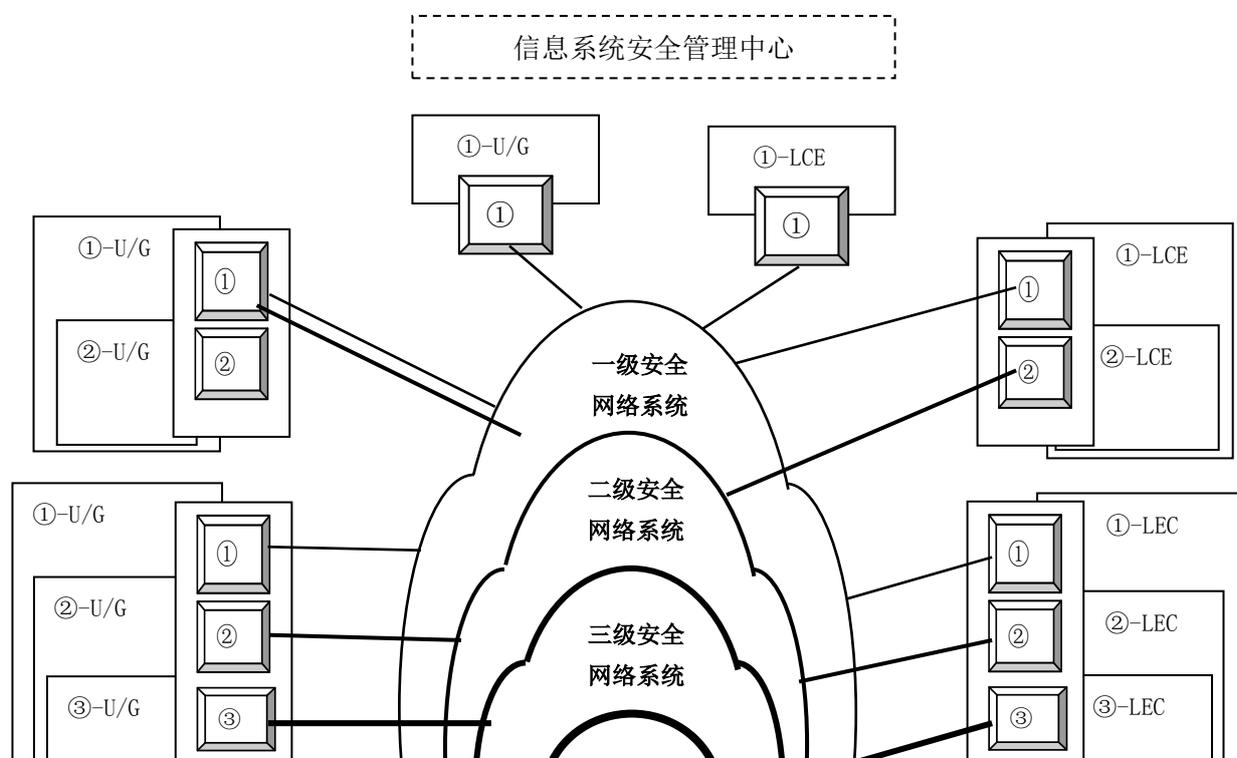
具有三级安全的安全域由一个或多个具有三级安全的局域计算环境及其边界防护、一个或多个具有三级安全的独立用户/用户群及其边界防护以及具有三级安全的网络系统组成。

具有四级安全的安全域由一个或多个具有四级安全的局域计算环境及其边界防护、一个或多个具有四级安全的独立用户/用户群及其边界防护以及具有四级安全的网络系统组成。

根据实际需要，具有四级安全的信息系统可以由只有四级安全的各部分组成或由具有四级安全的安全域与具有一级安全域和/或二级安全域和/或三级安全域的全部或部分组成。

对于具有四级安全的典型信息系统，根据其所保护的数据信息的要求及数据分布情况，可以按照全系统同一安全等级保护、分系统不同安全等级保护或虚拟系统不同安全等级保护的方法实施安全等级保护。

在具有四级安全的信息系统中的数据，应有需要进行四级安全保护的数据，也可以有需要进行一级安全保护和/或二级安全保护和/或三级安全保护的数据。图 5 给出了这种情况的安全信息系统的组成与相互关系。当没有需要进行一级和/或二级和/或三级保护的数据时，就只需要考虑仅有四级保护的情况，或四级保护和需要对相应数据保护的级别保护的情况。



- 其中，①-LCE：为具有一级安全的局域计算环境（0到n个）；
 ②-LCE：为具有二级安全的局域计算环境（0到n个）；
 ③-LCE：为具有三级安全的局域计算环境（0到n个）；
 ④-LCE：为具有四级安全的局域计算环境（1到n个）；
 ①-U/G：为具有一级安全的独立用户或用户群（0到n个）；
 ②-U/G：为具有二级安全的独立用户或用户群（0到n个）；
 ③-U/G：为具有三级安全的独立用户或用户群（0到n个）；
 ④-U/G：为具有四级安全的独立用户或用户群（1到n个）；
：为具有一级安全的边界防护设施（0到n个）；
：为具有二级安全的边界防护设施（0到n个）；
：为具有三级安全的边界防护设施（0到n个）；
：为具有四级安全的边界防护设施（1到n个）；
：为具有一级安全的网络系统；
：为具有二级安全的网络系统；
：为具有三级安全的网络系统；
：为具有四级安全的网络系统。

图5 四级安全信息系统的组成与相互关系

如图5所示，四级安全信息系统主要由以下部分组成：

- 0到n个具有一级安全的局域计算环境及其边界防护设施；
- 0到n个具有二级安全的局域计算环境及其边界防护设施；
- 0到n个具有三级安全的局域计算环境及其边界防护设施；
- 1到n个具有四级安全的局域计算环境及其边界防护设施；
- 0到n个具有一级安全的独立用户或用户群及其边界防护设施；
- 0到n个具有二级安全的独立用户或用户群及其边界防护设施；
- 0到n个具有三级安全的独立用户或用户群及其边界防护设施；
- 1到n个具有四级安全的独立用户或用户群及其边界防护设施；
- 具有一级安全的网络系统；
- 具有二级安全的网络系统；
- 具有三级安全的网络系统；

- 具有四级安全的网络系统；
- 具有四级安全的信息系统安全管理中心。

5.5 五级安全信息系统

典型的五级安全信息系统，可以包含具有一级安全的安全域和/或具有二级安全的安全域和/或具有三级安全的安全域和/或具有四级安全的安全域和具有五级安全的安全域，但至少应包含一个具有五级安全的安全域。

具有一级安全的安全域由一个或多个具有一级安全的局域计算环境及其边界防护、一个或多个具有一级安全的独立用户/用户群及其边界防护以及具有一级安全的网络系统组成。

具有二级安全的安全域由一个或多个具有二级安全的局域计算环境及其边界防护、一个或多个具有二级安全的独立用户/用户群及其边界防护以及具有二级安全的网络系统组成。

具有三级安全的安全域由一个或多个具有三级安全的局域计算环境及其边界防护、一个或多个具有三级安全的独立用户/用户群及其边界防护以及具有三级安全的网络系统组成。

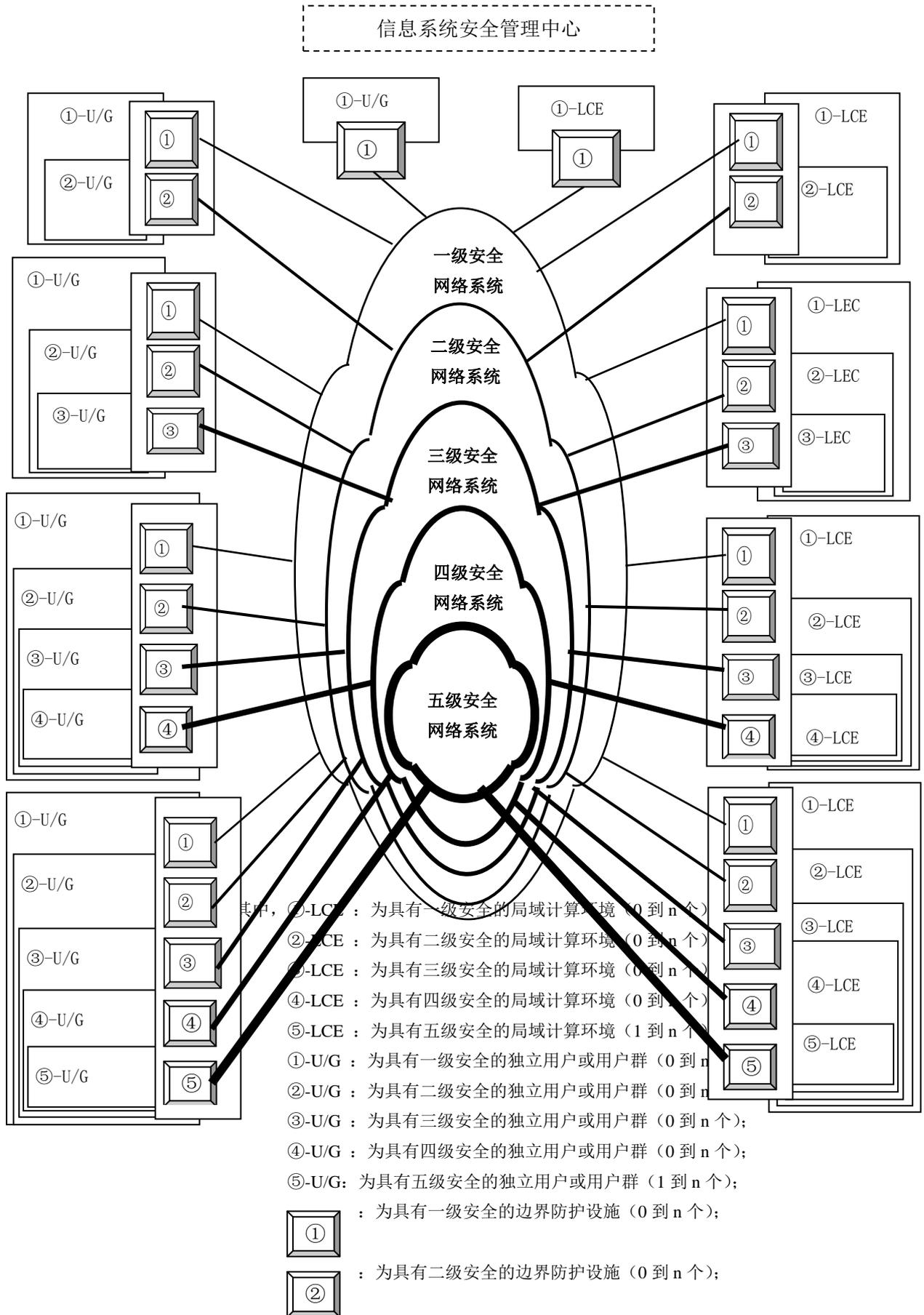
具有四级安全的安全域由一个或多个具有四级安全的局域计算环境及其边界防护、一个或多个具有四级安全的独立用户/用户群及其边界防护以及具有四级安全的网络系统组成。

具有五级安全的安全域由一个或多个具有五级安全的局域计算环境及其边界防护、一个或多个具有五级安全的独立用户/用户群及其边界防护以及具有五级安全的网络系统组成。

根据实际需要，具有五级安全的信息系统可以由只有四五级安全的各部分组成或由具有五级安全的安全域与一级安全域和/或二级安全域和/或三级安全域和/或四级安全域的全部或部分组成。

对于具有五级安全的典型信息系统，根据其所保护的数据信息的要求及数据分布情况，可以按照全系统同一安全等级保护、分系统不同安全等级保护或虚拟系统不同安全等级保护的方法实施安全等级保护。

在具有五级安全的信息系统中的数据，应有需要进行五级安全保护的数据，也可以有需要进行一级安全保护和/或二级安全保护和/或三级安全保护和/或四级安全保护的数据。图 6 给出了这种情况的安全信息系统的组成与相互关系。当没有需要进行一级和/或二级和/或三级和/或四级保护的数据时，就只需要考虑仅有五级保护的情况，或者五级和需要对相应数据保护的级别保护的情况。



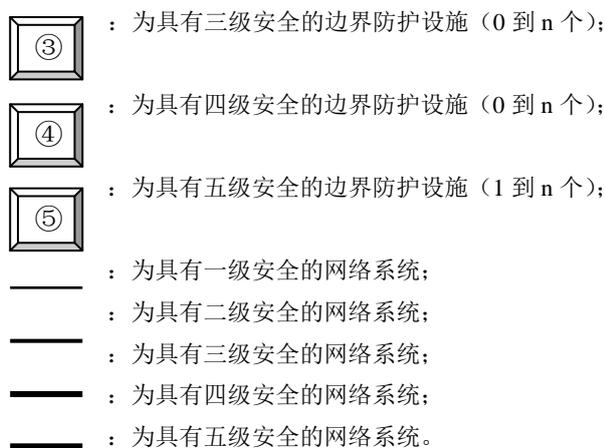


图 6 五级安全信息系统的组成与相互关系

如图 6 所示, 五级安全信息系统主要由以下部分组成:

- 0 到 n 个具有一级安全的局域计算环境及其边界防护设施;
- 0 到 n 个具有二级安全的局域计算环境及其边界防护设施;
- 0 到 n 个具有三级安全的局域计算环境及其边界防护设施;
- 0 到 n 个具有四级安全的局域计算环境及其边界防护设施;
- 1 到 n 个具有五级安全的局域计算环境及其边界防护设施;
- 0 到 n 个具有一级安全的独立用户或用户群及其边界防护设施;
- 0 到 n 个具有二级安全的独立用户或用户群及其边界防护设施;
- 0 到 n 个具有三级安全的独立用户或用户群及其边界防护设施;
- 0 到 n 个具有四级安全的独立用户或用户群及其边界防护设施;
- 1 到 n 个具有五级安全的独立用户或用户群及其边界防护设施;
- 具有一级安全的网络系统;
- 具有二级安全的网络系统;
- 具有三级安全的网络系统;
- 具有四级安全的网络系统;
- 具有五级安全的网络系统;
- 具有五级安全的信息系统安全管理中心。

参考文献

- [1] 信息保障技术框架 (3.0 版), 美国国家安全局发布, 国家 973 信息与网络安全体系研究课题组组织翻译, 北京中软电子出版社, 2004 年 4 月第一版
 - [2] NIST SP800 , National Institute of Standards and Technology, Technology and Ministriation, U.S. Department of Commerce
-