国家信息安全测评

工业控制系统产品安全测评

文档编写指南

版本：1.0

二〇一四年八月

目　　录

1 文档清单

工业控制系统产品安全测评需提交文档清单如下：

序号	文档名称
1	（被测产品名称、型号、版本号）配置管理文档
2	（被测产品名称、型号、版本号）交付和运行文档
3	（被测产品名称、型号、版本号）开发类文档
4	（被测产品名称、型号、版本号）指导性文档
5	（被测产品名称、型号、版本号）测试文档
6	（被测产品名称、型号、版本号）生命周期支持文档

2 文档编写指南

以下针对每一个文档的具体要求进行阐述，内容应与提交的被测产品名称、型号、版本号相匹配。

2.1 配置管理文档

该文档用来确保配置项被唯一标识，并确保开发者用于控制和跟踪被测产品改变的程序是充分的，这包括应跟踪那些改变、潜在的改变如何体现等方面的详细信息。内容包括：配置管理能力和配置管理范围。

2.1.1 配置管理能力

配置管理能力是为了确定开发者是否清晰定义了被测产品和它的相关配置项，以及改变这些配置项的能力是否被适当的控制。要求包括如下内容：

1）被测产品的唯一标识，包括名称、版本号。该标识无论是从被测产品硬件、软件、包装还是文档上都应明确，且应统一及唯一。

2)包括一份配置清单,配置清单应包括与被测产品设计相关的所有文档(如：需求分析、概要设计、详细设计、源代码、测试文档），要唯一标识出每个配置项的版本信息（如名称、版本号等），还要作出详尽的解释。

3）包括一份配置管理计划，配置管理计划应包括如何使用配置管理系统保持被测产品配置项完整性的描述（包括人员授权、配置项的修改、并发处理等），如过程当中有相应记录产生，应同时提供。应包括配置管理系统记录及防止对配置项非授权访问的访问控制措施。

2.1.2 配置管理范围

配置管理范围至少应包括文档清单中的 6 类文档,从而确保它们的修改是在一个正确授权的可控方式下进行的。配置管理文档至少应能跟踪上述内容，并描述配置管理系统是如何跟踪这些配置项的。

2.2 交付和运行文档

该文档用来判断程序文档是否齐全，以确保以开发者期望的方式安装、生成与启动被测产品，以及被测产品在交付中不被修改。包括：交付文档、安装生成和启动程序。

2.2.1 交付

交付程序适用于整个被测产品，包括可用的软件、硬件、固件和文档；交付程序也适用于从生产环境到使用环境的整个交付过程的各个阶段，如：开发环境到测试环境、公司内部到最终用户。

在给用户方交付系统的各版本时，为维护安全所必需的所有程序。

开发者的向用户提供的产品版本和用户收到的版本之间的差异以及如何监测对产品的修改。

2.2.2 安装、生成和启动程序

被测产品所必需的所有安装、生成和启动步骤。

2.3 开发类文档

开发类文档包括功能规范、高层设计和对应性分析。

2.3.1 功能规范

本文档用来确认开发者对被测产品安全功能是否作了充分描述，被测产品提供的安全功能是否足以满足测评规范功能要求。

安全功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和出错信息的细节。

2.3.2 高层设计

高层设计应以非形式方法表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强产品安全功能的子系统和其它子系统分开。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提供安全功能子系统的作用、例外情况和出错信息的细节。高层设计还应标识系统安全要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件或软件所实现的保护机制。

2.3.3 对应性分析

本文档用以确认在实现表示中开发者是否正确、完整地实施了功能规范、高层设计的要求。如果对应性分析已经在功能规范、高层设计中进行了描述，则该部分可以省略，否则，应描述如下内容：

1）被测产品概要规范和功能规范之间的对应性分析

该对应性分析应该阐明被测产品概要规范中的安全功能和功能规范中的安全功能描述之间的对应关系，以确认功能规范是被测产品概要规范的完整的陈述。

2）功能规范和高层设计之间的对应性分析

该对应性分析应该阐明被测产品功能规范中的安全功能和高层设计中的子系统描述之间的对应关系，以确认高层设计是功能规范的完整的陈述。

2.4 指导性文档

该文档用以判断描述如何使用可操作的的文档是否详尽，这些文档针对两类用户，一类是可信的管理员用户，他们的不正确行为可以影响被测产品安全性，另一类是那些非管理员用户，他们的不正确行为可以影响其拥有的数据的安全性。如果文档在设计初期将两部分的描述合并在了一起，则此部分可提供一份文档，不用将一份文档刻意分为两份提交，但需在文档中以明确的标识加以注明。

2.4.1 管理员指南

应就管理员如何以安全方式管理被测产品进行详细而全面地说明。必要时，文档中应包括对受控功能和特权的警告。

2.4.2 用户指南

应详细说明被测产品安全功能和接口及有关被测产品安全使用方面的信息。必要时，文档中应包括对用户可访问的功能和特权的警告。

2.5 测试文档

本文档的目的是确定被测产品的行为是否与设计文档中的一样，并且与被测产品的安全功能要求说明一致。该文档包括测试文档本身、测试范围分析和测试深度分析。

1）功能测试

该文档应包括测试计划、测试方法、测试环境、测试工具、命令、测试步骤、预期测试结果和实际测试结果。

2）测试范围分析

阐明测试文档中列出的测试与功能规范是一致的。可采用表格或矩阵的形式来描述其对应关系。测试覆盖的分析结果应表明测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的，且该对应是完整的。

3）测试深度分析

阐明测试文档中列出的测试与高层设计是一致的。深度分析应证实测试文档中所标识的测试足以证实该产品的功能是依照其高层设计运行的。

2.6 生命周期支持文档

本文档用以确定开发者在被测产品开发和维护期间使用程序的能力。这一过程是为了保护被测产品及其相关的设计信息，以防他们受到干扰或暴露。开发过程中的干扰使故意引入脆弱性成为可能。而设计信息的暴露可能导致脆弱性更容易被人利用。

2.6.1 开发安全

开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其它方面的安全措施，并应提供在产品的开发和维护过程中执行安全措施的证据。

2.6.2 脆弱性分析

该文档用于确定被测产品在特定环境下的漏洞或脆弱性的存在及可利用性。应从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析。对被确定的脆弱性，开发者应明确记录采取的措施。对每一条脆弱性，应有证据显示在使用产品的环境中，该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的产品可以抵御明显的穿透性攻击。