GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 20261-2020

Replacing GB/T 20261-2006

Information security technology - System security engineering - Capability maturity model

信息安全技术 系统安全工程 能力成熟度模型

(ISO/IEC 21827:2008, Information technology - Security techniques - Systems security engineering - Capability maturity model, MOD)

Issued on: November 19, 2020 **Implemented on: June 01, 2021**

Issued by: State Administration for Market Regulation;
Standardization Administration of the People's Republic of China.

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This Standard replaces GB/T 20261-2006, *Information technology - Systems security engineering - Capability maturity model*. Compared with GB/T 20261-2006, the main technical changes are as follows (see Annex G for the comparison of main changes):

– Modify some normative references (see Clause 2; Clause 2 of the 2006 edition);

– Add terms and definitions, namely “base practices; BP”, “capability”, “information security event”, “information security incident”, “process area; PA”, “risk management”;

– Modify the definitions of “assurance”, “engineering group”, “work product” in Terms and definitions; and modify “residual risk” to “residual risk” (see Clause 3; Clause 3 the 2006 edition).

– Remove the term “practices” (see 3.24 of the 2006 edition);

– Modify some clause and sub-clause titles, merge, adjust and delete some contents that are related or not suitable as national standards (see 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1);

– Delete the original Clause 5, and adjust the original Clause 6 and Clause 7 to Clause 5 and Clause 6 (Clause 5, Clause 6 and Clause 7 of the 2006 edition);

– Add BP.06.03 Define Security Measures in Clause 6, and the additions and revisions of ISO/IEC 21827:2008 relative to ISO/IEC 21827:2002 (see Clause 6);

– Add Annex A and Annex B (see Annex A, Annex B);

– Modify the definition of the five levels of capability level in Annex C to be consistent with the description of the current standard GB/T 30271 and other standards;

– Modify the error message that the serial process area number does not match the process area description in Annex D (see D.6.1.1, D.7.7.3, D.9.3.3, D.11.1.1, D.11.4, D.11.4.1, D.12.3.1);

– Add Annex F to facilitate the mapping relationship between the standard model and the current security services (see Annex F);

– Add a comparison table of major changes compared with GB/T 20261-2006 (see Annex G).

Information security technology - System security engineering - Capability maturity model

1 Scope

This Standard specifies the Systems Security Engineering – Capability Maturity Model (SSE-CMM®). The SSE-CMM® is a process reference model focused upon the requirements for implementing security in a system or series of related systems that are the information technology security (ITS) domain. Within the ITS domain, the SSE-CMM® is focused on the processes used to achieve ITS, most specifically on the maturity of those processes. There is no intent within the SSE-CMM® to dictate a specific process to be used by an organization, let alone a specific methodology. Rather the intent is that the organization making use of the SSE-CMM® should use its existing processes, be those processes based upon any other ITS guidance document.

While the SSE-CMM® is a distinct model to improve and assess security engineering capability, this does not imply that security engineering should be practised in isolation from other engineering disciplines. On the contrary, the SSE-CMM® promotes integration, taking the view that security is pervasive across all engineering disciplines (e.g., systems, software and hardware) and defining components of the model to address such concerns. The Common Feature “Coordinate Practices” recognizes the need to integrate security with all disciplines and groups involved on a project or within an organization. Similarly, the Process Area “Coordinate Security” defines the objectives and mechanisms to be used in coordinating the security engineering activities.

The scope encompasses:

- the system security engineering activities for a secure product or a trusted system addressing the complete life cycle of concept definition, requirements analysis, design, development, integration, installation, operation, maintenance and de-commissioning;
- requirements for product developers, secure systems developers and integrators, organizations that provide computer security services and computer security engineering;
- all types and sizes of security engineering organization, from commercial to government and the academe; and
- demanders, providers and evaluators of system security engineering.

- human factors engineering;
- communications engineering;
- hardware engineering; and
- enterprise engineering.

Note 1: With respect to systems engineering, further information can be found in ISO/IEC 15288 which views security from a systems perspective.

Note 2: With respect to software engineering, further information can be found in GB/T 8566-2007 which views security from a software perspective.

Security engineering activities must be coordinated with many external entities because assurance and the acceptability of residual operational impacts are established in conjunction with the developer, integrator, acquirer, user, independent evaluator, and other groups. It is these interfaces and the requisite interaction across a broad set of organizations that make security engineering particularly complex and different from other engineering disciplines.

4.6 Security Engineering Specialties

While Security Engineering and Information Technology Security are very often the driving disciplines in the current security and business environment, other more traditional security disciplines, such as Physical Security and Personnel Security should not be overlooked. Security Engineering will need to draw upon these and many other specialist sub-disciplines if they are to achieve the most efficient and effective results in the performance of their work. The list below gives a few examples of specialty security sub-disciplines likely to be required, along with a short description of each, including:

- operations security -- targets the security of the operating environment, and the maintenance of a secure operating posture;
- information security -- pertains to information and the maintenance of security of the information during its manipulation and processing;
- network security -- involves the protection of network hardware, software, and protocols, including information communicated over networks;
- physical security -- focuses on the protection buildings and physical locations;
- personnel security -- is related to people, their trustworthiness and their awareness of security concerns;
- administrative security -- is related to the administrative aspects of security and security in administrative systems; and

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------