The Institution of Engineering and Technology

SaRS SAFETY AND RELIABILITY SOCIETY

bcs The Chartered Institute for IT

Institution of MECHANICAL ENGINEERS

Position statement on **Security, Safety and ISA**

Change History

Version	Date	Status
1.0	October 2015	WEB

Please send suggestions for improvements, for consideration by the Working Group to:

isawg@theiet.org

Disclaimer

Cover Images (clockwise from top left)

- Nuclear power plant
- Euro fighter
- Oil and natural gas offshore platform
- London Underground

About the supporting organisations

- The IET is registered as a Charity in England & Wales (No. 211014) and Scotland (No. SC038698)
- The BCS is a registered charity (No. 292786)
- IMechE is a registered charity in England and Wales (No. 206882)
- SaRS is a registered charity in England and Wales (No. 801207)

Contents

Purpose

This position statement gives the opinion of the ISA Working Group on security and safety in so far as it affects independent safety assessment and ISAs. Its primary focus is on security and safety when these depend, at least in part, on electrical, electronic or programmable electronic systems. However, the general principles also apply to security and safety of systems that use other technologies.

Background

Independent safety assessment involves coming to a judgement about the safety of a system. The safety of potentially hazardous systems depends in part on provision of adequate security to protect against unauthorised or malicious interference with the system. This implies that independent safety assessment must address security-related aspects of safety. Security is therefore of both interest and importance for ISAs.

There is increasing public awareness of the risk posed by security threats, which has been emphasised by recent high profile incidents. Within the technical community, there is growing awareness that technical developments which bring benefits to businesses, individuals and society also raise issues in respect of security (see, for example, the IET Factfile 'Cloud Computing (part 3): The Security Challenge'). While public attention tends to be focused on non-safety consequences of security threats (e.g. loss of service; or breach of privacy; or financial loss), there is a perception among safety specialists that the chances of safety being compromised by a security attack are increasing.

Factors that support the perception of increasing security threat and consequential risk include:

- Increasingly highly distributed systems (possibly spanning continents).
- Use of cloud-based systems.
- Provision of ubiquitous access to system services.
- Interconnectedness between previously independent systems.
- Increasing complexity of systems.
- Use of wireless communications within a system.
- Increasingly complex control functions provided by computer systems.
- Autonomous control and decision-making by computer systems.
- Use of hardware and software of uncertain provenance.
- Complex supply chains and consequential difficulties in enforcing effective control of the supply chain.

These can make it difficult both to establish what security vulnerabilities may be present in a system and to detect whether they are actually present. In addition, attacks and security breaches may be difficult to detect and may also remain undetected for some time - perhaps until specific circumstances some time after a security breach trigger unsafe system behaviour. Hacking of electronic systems is also relatively cheap and easy (compared to physical attacks) and it is difficult to identify and catch the perpetrators of an attack. Cyber attack is now a potential weapon for hostile organisations, governments and organised crime as well as for the lone hacker.

Basis of Opinion

Safety and security is considered from the following three viewpoints:

- The relationship between safety and security.
- Implications of system security for technical aspects of safety assessment.
- Implications of system security for professional aspects of ISA.

Key observations from these viewpoints are given in Appendices A, B and C. These form the technical basis which underlies the ISA Working Group opinion on security and safety. The reader is encouraged to read the Appendices to ensure that both the reasons for and the implications of the opinion are fully understood. However, the opinion on security and safety is intended to be free-standing and not dependent on knowing and understanding the observations made in Appendices A, B and C.

ISA Working Group Opinion on Security and Safety

The ISA Working Group:

1. Recognises the importance of security in respect of ensuring the safety of a system.
2. Believes that consideration of security threats and mitigating measures can and must be included in system safety analysis, safety assessment, design, production, end use and disposal.
3. Encourages the use of security measures that are appropriate and proportionate to the risks to which they apply.
4. Recommends that safety and security programmes are coordinated if malicious access or acts may have an impact on safety.

The ISA Working Group notes that:

1. Hazards and accidents can arise from a number of different types of causes, of which security threats are one.
2. Safety analyses and assessments should therefore include consideration of security threats and mitigating measures as part of the overall consideration of causes and mitigations for hazards and accidents.
3. Security has wider scope and implications than just safety, thus it is appropriate for there to be distinct security and safety programmes. However, the security and safety programmes should be coordinated so as to ensure the timely and effective generation and exchange of information relevant to both security and safety.

The ISA Working Group recommends that ISAs:

1. Ensure that they know and understand the security aspects of system safety that are relevant and appropriate to the sector and technical domain in which they provide ISA services.
2. Develop and maintain competence to understand potential security threats, assess which security threats may have an adverse effect on safety, understand potential mitigations for the threats and assess their effectiveness.
3. Use independent security assessment expertise to supplement personal competence where appropriate, this to be included in ISA planning.
4. Consider relevant security threats and mitigations in independent safety assessments. Justification should be provided if they are excluded.
5. Include relevant security-related activities in safety process audits and assessments, coordinating with any independent security assessments in order to avoid duplication.
6. Ensure that appropriate security measures are used to protect client information, in particular information that could contribute to or facilitate a security threat by a 3rd party.

Appendix A

Relationship Between Safety and Security

Security is the means by which a system (including associated data and other information) is protected against unauthorised or malicious access or acts. Protection can involve preventing such access and/or limiting the scope and impact of acts if such access were to occur. Unauthorised or malicious access or acts are not limited to when the system is in service, they may also take place during design and development.

Safety is concerned with harm to people, its causes and its prevention. Ensuring adequate safety involves identifying and addressing all credible means by which people may be harmed. Safety measures can involve preventing potentially harmful events and/or limiting the impact if such events were to occur.

Unauthorised or malicious access provides an opportunity to use or change a system (including associated data and other information) so as to compromise safety. Safety might be compromised by increasing the probability of a harmful event occurring (perhaps by making it certain to occur), increasing the consequences of a harmful event or by reducing protection against a harmful event. (Of course, there may also be other, non-safety, consequences of unauthorised or malicious access, for example harm to the environment or financial damage.)

Use of a system (including associated data and other information) that has been subjected to unauthorised or malicious access cannot result in new ways by which people are harmed by the system. However, the unauthorised or malicious access may:

- Increase the frequency or probability of already credible ways by which people may be harmed by the system.
  - **Example:** By disabling a safety protection system.
- Make credible one or more ways by which people may be harmed by the system that would otherwise be deemed incredible.
  - **Example:** By the system giving maliciously incorrect information or messages to operators or users (such messages being otherwise impossible to create or issue).
- Make it possible for malicious persons to cause harm in ways that are outside the scope of the system itself.
  - **Example:** By introducing an explosive device after breaching a security boundary.

Changes to a system resulting from unauthorised or malicious access may affect the sequence or timing of events leading up to harm. For example, a harmful event might be triggered only at a particular time, or when a particular set of circumstances arises. This may affect the amount of harm (for example, if a harmful event were to be timed so that the maximum number of people would be affected).

Changes to a system resulting from unauthorised or malicious access may result in the linking of two or more failures that would otherwise only occur independently of each other. For example, a malicious change to a system might cause the system to behave in an unsafe way and at the same time cause the protection provided against such behaviour to fail. Such linking of failures may make a sequence of failures credible that would otherwise be regarded as incredible. Unauthorised or malicious access is therefore a potential source of dependent failures (i.e. multiple failures that occur due to a single cause).

If follows that security measures taken to prevent unauthorised or malicious access or acts that may result in harm to persons are hazard prevention measures. Similarly, security measures taken to limit the safety impact if such access or acts were to occur are hazard mitigation measures. As with all hazard prevention and mitigation measures, it is important that security measures do not interfere with the correct functioning of safety-related functions of the system, including other hazard prevention and mitigation measures.

Appendix B

Implications of System Security for Technical Aspects of Safety Assessment

Safety assessment needs to address security in so far as it can affect safety. This includes assessment of security threats, system vulnerabilities and measures taken to mitigate them. This assessment should be comprehensive in scope. However, it should also be proportionate to the safety risks relating to security. In particular, the depth and rigour of assessment should be that which would be used for comparable non-security related safety risks. Depending on the system and its operational context, this might be less than or greater than what would be appropriate for security-related risks that do not affect safety.

Assessment (whether independent or not) should consider whether security in respect of safety is adequately addressed in all phases of the safety life cycle, specifically:

- Safety requirements
- Design
- Development
- Verification and validation
- Commissioning
- Operation
- Maintenance
- Decommissioning
- Disposal

Assessment should be evidence-based. The strongest evidence is direct evidence of system properties in respect of security. Direct evidence may need to go beyond that usually associated with safety. For example, testing might need to include tests to provide evidence of the effectiveness of protection against security threats (e.g. penetration testing). This might need to address protection against security threats both in the system as initially developed and in the event that faults are subsequently introduced by authorised activities carried out incorrectly (e.g. Computer Software Configuration Item (CSCI) upgrades, configuration file changes or data file changes). Such testing might be best carried out as part of a security assessment. Safety and security assessments should therefore be coordinated to ensure that generation of direct evidence that is relevant to both safety and security is carried out cost effectively and satisfies the needs of both.

Direct evidence should be supported by indirect evidence of system properties and process evidence. Assessment of process evidence should include whether the safety process:

- Adequately facilitates the identification and addressing of security-related safety risks.
- Is coordinated, and has effective links, with relevant security work, particularly in respect of:
  - Timescales
  - Exchange of information

In addition, assessment should consider whether there is mutual understanding among relevant safety and security personnel of the implications of security for safety and vice versa.

The frequency of an unauthorised or malicious access or act cannot usually be quantified. Thus the risk of harm (which is a combination of frequency and consequential harm) cannot usually be quantified. A safety assessment should therefore not attempt to quantify, or assess a quantification of, the risk of harm relating to security. However, if a measure is in place to detect a security attack, the probability of failing to detect such an attack if it were to take place may be assessed.

Appendix C

Implications of System Security for Professional Aspects of ISA

The 'Code of Practice for Independent Safety Assessors (ISAs)' produced by the ISA Working Group places a number of obligations on ISAs in respect of the conduct of their work. Implications for ISAs in respect of security and safety as follows:

Clause	Item	Implication for ISA and Security
1. General Professional Conduct	"ISAs should practice continuous improvement, for example by professional development and maintaining awareness of relevant developments in science, technology and legislation."	Continuous improvement should include developing competence and awareness of relevant aspects of security.
3. Competence	a) "The ISA shall be demonstrably competent to undertake the assessment activities" b) "It is unlikely that one individual has sufficient competency to adequately undertake the complete assessment for a complex system. Therefore where a team of assessors is used the team should collectively have adequate competency."	a) The ISA shall be demonstrably competent in respect of any assessment activities they carry out that involve security-related aspect of safety. b) Competency in respect of safety-related aspects of safety may be achieved by including security expertise in an ISA team.
4. Communication	"Findings should be reported in a timely manner so that remedial action may be taken without unduly compromising the development programme."	The timing of reports of findings that may have implications for security should take into account the timescales of the project security programme.
5. Proportionality	a) "The ISA's assessment rigour shall be in proportion to the safety risk addressed." b) "The ISA should balance effort on safety issues according to their safety criticality."	a) Proportionality in rigour of assessment shall extend to security-related aspects of safety. b) Safety criticality should determine how much effort the ISA puts into security-related aspects of safety. The ISA should not be influenced by the criticality of non-safety consequences of security hazards.
8. Priority of Safety	"The ISA shall seek to ensure that safety is given due priority."	The ISA shall seek to ensure that safety-related aspects of security are given due priority by persons with responsibilities for security-related work as well as by those with safety or overall project responsibilities.
10. Management and Planning	a) "The ISA shall ensure that the ISA work programme is planned and managed so that it delivers the required outputs when needed and minimises disruption or delay to the client project or programme." b) "The ISA work programme should be planned and agreed with the client."	a) The ISA work programme shall take into account the timescales and needs of those parts of the client project or programme that address security-related aspects of the system. b) The ISA should ensure that planning takes into account client plans for work that addresses security-related aspects of the system.

Furthermore, during the course of an assessment, an ISA is likely to acquire information about the system and its use that may compromise safety if it were to be known by a person with malicious intent. ISAs must therefore apply an appropriate level of security to such information in order to ensure that it cannot be accessed by unauthorised persons. This applies to information retained after completion of an assessment as well as during an assessment.