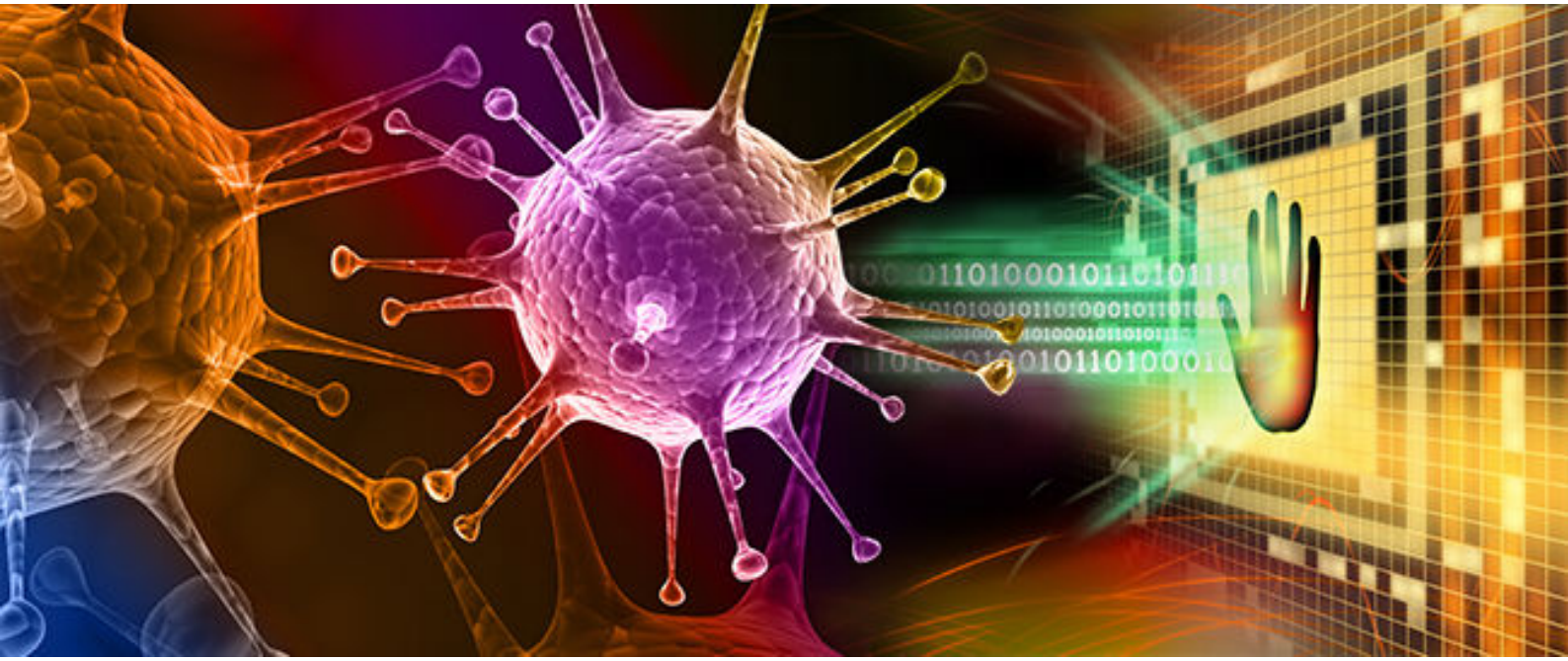

Security Concept Audit Report

Secomea

June 27th 2023

TG alpha GmbH

Ulrichsberger Str. 17
94469 Deggendorf
Germany

Phone: +49.991.402.271-00
Fax: +49.991.402.271-99
Email: info@tgalpha.de
Web: https://www.tgalpha.de

Contents

Executive Summary

TG alpha GmbH was contracted by Secomea to conduct a security audit of the components for remote access to industrial equipment. The product security audit was carried out with the following goals:

- Identification of potential vulnerabilities within the implementation
- Determination of the potential risk based on the discovered vulnerabilities
- Reevalution of the concept using the BSI Grundschutz Compendium as well as the IEC 62443-3-3 and IEC 62443-4-2

All tests and actions were conducted under controlled conditions. Also the web front end for the hardware components as well as the software implementations have been tested for known vulnerabilities and flaws in regard to the OWASP Top 10 list. A targeted penetration test with state of the art penetration testing tools has been conducted in order to evaluate the potential risk of potential vulnerabilities in the implementation of the components.

Tested Components

- GateManager with version 11.0.623222013
- GateManager API
- SiteManager Embedded with version 11.0.623222013
- SiteManager with version 11.0.623222013
- LinkManager Mobile with version 11.0.623222013
- LinkManager with version 11.0.623222013

Out-Of-Scope Components

- Data Collection Module (DCM)

Results:
The audit was successfully passed. The hardware and software components were tested for vulnerabilities. Therefore a vulnerability assessment, exploitation with standard tools, fuzzing on Ethernet interface and analysis of communication principles were done. Also the TLS connections have been tested. The result of the component audit is that all components are robust against the most common attacks. No critical vulnerabilities or issues exist.

Thr result of the concept audit is: The concept is almost conform to the BSI Grundschutz Compendium standard level and mostly SL-2 for the IEC 62443-3-3. The remaining issues for the IEC 62443-3-3 can be compensated by the customer by introducing firewalls, intrusion detection systems, network devices such as switches throttling the bandwidth towards the Secomea devices as well as uninterruptible power supplies (UPS). With best practices documentation including suggestions as how to handle these four remaining issues, the customer can make sure to deploy the Secomea concept achieving SL-2 for remote maintenance today.

The security audit is successfully passed.

Changelog

2022

IEC 62443-4-2

Change of CR 1.12 - System use notification to "Not Relevant, no local user authentication" because only remote authenication is in use.

OWASP TOP10

Removed Chapter of OWASP Top 10. Chapter was removed, because it was more or less a self declaration. It is coverd already by tests in the component audit.Web Technology Analysis and OWASP ZAP. Future Reports will contain the OWASP Top10 topics in a seperated chapter in the component audit report.

2023

No changes

1 Concept Audit

1.1 Generic Risk Analysis

On the basis of the *BSI-Grundschutz* potential threats for the system under review are determined. A generic risk analysis was done for the provided architecture. For this purpose, the functions of the GateManager, the SiteManager Embedded and the LinkManager Mobile described in the documentation have been taken into account. The risk for the success of one of the attack vectors were divided into the three classes *low*, *middle* and *high*. *High* is the risk of an attack vector without countermeasures. Countermeasures have been taken for the risk class *middle*, which, however, cannot completely prevent but at least hinder the attack vector. For the risk class *low* implemented measures are assumed which, according to the current state of the art, make an attack vector impossible or only possible with high effort. The attack vectors reflect the most popular threats. However, due to different evaluation and view, they are not exhaustive. With the further development of existing and new features it could happen that new attack vectors have to be added. In addition, the potential hazards and the risk assessment can also be changed.

Espionage

Espionage refers to attacks that aim to collect, analyze and process information about companies, people, products or other target objects. The processed information can then be used, for example, to give another company certain competitive advantages to be able to recreate a product.

Attack vector	Risk	Explanation
Customer data	low	There are only encrypted data transmissions and data is stored in protected areas
Company data (e.g. software used)	low	There are only encrypted data transmissions and data is stored in protected areas
Machine configurations	low	There are only encrypted data transmissions and data is stored in protected areas
Access data	low	There are only encrypted data transmissions.

Eavesdropping

Eavesdropping refers to targeted attacks on communication links of all kinds. This begins with unnoticed, secretive eavesdropping an insecure information channel and extends to highly sophisticated complex attacks to encrypted messages. IT systems can be used to gather information or decrypt messages.

Attack vector	Risk	Explanation
Communication Admin User - GateManager	low	HTTPS-Connection used
Communication Humen User - GateManager	low	HTTPS-Connection used
Communication GateManager - SiteManager Embedded	low	HTTPS-Connection used
Communication Admin User - SiteManager Embedded	low	HTTPS-Connection used
Communication Humen User - SiteManager Embedded	low	HTTPS-Connection used
Communication GateManager - LinkManager Mobile	low	HTTPS-Connection used
Communication Humen User - LinkManager Mobile	low	HTTPS-Connection used

Disclosure of Sensitive Information

Confidential data and information may only be accessible to authorized persons. For confidential information such as passwords, personal data, company secrets or development data, there is a risk that these will be disclosed by technical failure, inattention or by intentional acts.

Attack vector	Risk	Explanation
Programming error	low	All code changes are reviewed before being integrated. Static code analysis is used to identify issues.

Manipulation of Software

Manipulation is any form of targeted but secretive intrusion to alter targets of all kinds unnoticed. Tampering of software can cause a high impact to availability. The focus can

may be on all kind of devices like data carriers, applications or databases.

Attack vector	Risk	Explanation
Manipulation of GateManager updates	low	GateManager validates updates. Updates are transferred via secure channel.
Manipulation of SiteManager Embedded updates	low	SiteManager Embedded validates updates. Updates are transferred via secure channel.
Manipulation of LinkManager Mobile updates	low	Updates are transferred via secure channel.
Manipulation of software on GateManager	low	All code changes are reviewed before being integrated.
Manipulation of software on the SiteManager Embedded	low	All code changes are reviewed before being integrated.
Manipulation of software on the LinkManager Mobile	low	All code changes are reviewed before being integrated.

Manipulation of Information

Information can be manipulated in a variety of ways, e.g. incorrect data entry or changes to the content of database fields. An intruder can only manipulate the information he has access to. The more access rights a person has to files and directories of IT systems or the more accessibility to information they have, the more manipulations they can accomplish. If the manipulations are not detected early enough, the smooth running of business processes and specialized tasks can be severely disturbed.

Attack vector	Risk	Explanation
Change of GateManager settings	low	Changes are logged. Assuming that the logs are checked regularly. Logs can only be deleted by the Admin.
Change of SiteManager Embedded settings	low	Changes are logged. Assuming that the logs are checked regularly. Logs can only be deleted by the Admin.

Lack of Resources

Resource shortages can occur in IT operations and communication links. If the resource availability in an area is insufficient, bottlenecks in the supply of these resources,

overloads and outages can occur. Depending on the nature of the resources involved, a small event whose occurrence was predictable may ultimately affect a variety of business processes.

Attack vector	Risk	Explanation
DoS on GateManager	low	System is in the intranet and depends on the operator infrastructure or hosted by Secomea(Assuming Secomea-hosted instances are secured by common practice standards)
DoS on SiteManager Embedded	low	System is in the intranet and depends on the operator infrastructure
Overuse of services	low	Assuming the host resources of the GateManager fits to the application

Software Vulnerabilities

For any software, the more complex it is, the more often errors occur. Even with intensive tests, not all vulnerabilities are usually discovered before delivery to the customers. If software vulnerabilities are not detected in time, the crashes or errors that occur during the application can lead to far-reaching consequences.

Attack vector	Risk	Explanation
Exploitation of vulnerabilities GateManager	low	All code changes are reviewed. Regular security audits are done.
Exploitation of vulnerabilities SiteManager Embedded	low	All code changes are reviewed. Regular security audits are done.
Exploitation of vulnerabilities LinkManager Mobile	low	All code changes are reviewed. Regular security audits are done.

Unauthorized Use or Administration of Devices and Systems

Without appropriate mechanisms for access control unauthorized use of devices and systems cannot be prevented or detected. In IT systems, the basic mechanism is the identification and authentication of users. But even with IT systems with a strong identification and authentication function, unauthorized use is conceivable if the corresponding security features, like passwords or tokens, fall into the wrong hands. A lot of mistakes can also be done when assigning and maintaining authorizations, for

example, if authorizations are granted too far-reaching or if they are not updated in a timely manner.

Attack vector	Risk	Explanation
Administration of GateManager	low	Is executed by customer admin or Secomeaitself, all interfaces are secured
Administration of SiteManager Embedded	low	Is carried out by the user himself, all interfaces are secured
Using the GateManager	low	Is carried out by the user himself, all interfaces are secured
Using the SiteManager Embedded	low	Is carried out by the user himself, all interfaces are secured
Using the LinkManager Mobile	low	Is carried out by the user himself, all interfaces are secured

Abuse of Permissions

Depending on their roles and tasks, users will be given access privileges. In this way, on the one hand, the access to information should be controlled and on the other hand, it should enable a user to do certain tasks. For example, users or groups need specific permissions to run applications or edit information. Abuse of privileges occurs when intentionally acquired opportunities outside the intended scope are used.

Attack vector	Risk	Explanation
Using the GateManager	low	Is carried out by the user himself, all interfaces are secured. Rights can be customized individually per user
Using the SiteManager Embedded	low	Is carried out by the user himself, all interfaces are secured. Rights can be customized individually per user
Privilege Escalation	low	Use of standardized authentication methods

Repudiation

Individuals may deny having committed certain actions for a variety of reasons, such as violating security requirements. In the field of information security, therefore, the liability is often highlighted to ensure that actions taken cannot be denied (Non-Repudiation).

Attack vector	Risk	Explanation

User executes an action and denies it.	low	All actions are logged including admin actions

Malware

A malicious program is software designed to perform unwanted and often detrimental functions. The typical types of malicious programs include viruses, worms and trojans. Malicious programs are usually secretly active without the knowledge and consent of the user. Malicious programs today offer an attacker extensive communication and control options and have a variety of functions. Among other things, malicious programs can specifically search passwords, remotely control systems, deactivate protection software and spy on data.

Attack vector	Risk	Explanation
Execution of third-party software on GateManager	low	It is not possible to run third-party software on GateManager.
Execution of third-party software on the SiteManager Embedded	low	It is not possible to run third-party software on GateManager API

Import or Replay Information

Attackers use this form of attack to send special prepared messages to systems or individuals for the purpose of gaining access or affecting the victim. For example, to construct the messages properly, the attackers use interface descriptions, protocol specifications, or communication history records.

Attack vector	Risk	Explanation
Communication Admin User - GateManager	low	HTTPS-Connection used
Communication Humen User - GateManager	low	HTTPS-Connection used
Communication GateManager - SiteManager Embedded	low	HTTPS-Connection used
Communication Admin User - SiteManager Embedded	low	HTTPS-Connection used
Communication Humen User - SiteManager Embedded	low	HTTPS-Connection used

Communication GateManager - LinkManager Mobile	low	HTTPS-Connection used
Communication Humen User - LinkManager Mobile	low	HTTPS-Connection used

Loss of Data

A data loss is an event that causes a database to become unusable as required (loss of availability). A common form of data loss is that data is deleted unintentionally or unauthorized, as a result of incorrect operation, malfunctions, power failures, contamination or malware.

Attack vector	Risk	Explanation
Data on the GateManager is deleted	low	GateManager has a backup system
Data on the GateManager API is deleted	low	SiteManager Embedded has a backup system. Configuration and backups can be push by GateManager

Conclusion

The risk for the most threat is low. The concept of the GateManager, SiteManager Embedded and the LinkManager Mobile address most of the possible attack vectors. However, there is one *middle* risk for specific attack vectors.

1.2 Evaluation against BSI Grundschutz Catalog

To evaluate Secomea's concept of the GateManager and SiteManager the relevant parts of the Federal Office for Information Security (German: Bundesamt für Informations Sicherheit, BSI) Grundschutz Compendium[1] were considered for assessment.

For this purpose the following parts were considered:

- APP.3.1 Web applications for GateManager and SiteManager
- APP.3.2 Web server for GateManager and SiteManager
- IND.2.1 General ICS component for SiteManager
- SYS.4.3 Embedded System for SiteManager

Other seemingly relevant parts were not considered as they may primarily focus on the requirements for processes of the end users using the Secomea concept.

APP.3.1 Web Application		
Basic Requirements		
Requirement	fulfilled	Comment
A1 Authentication of users	x	
A4 Controlled insertion of data and contents for web applications	x	
A7 Protection against unauthorized automated usage of web application	x	
A14 Protection of confidential data	x	
Standard Requirements		
Requirement	fulfilled	Comment

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2022.pdf

A8 System Architecture	x	We assume that security is already considered while designing/updating the architecture. This is evident by previous threat analysis, etc.
A9 Ordering, developing and extending web applications		End Customer Task Documentation is provided, web applications are created with security in mind and tested
A11 Secure connection to background systems/services	x	
A12 Secure configuration of web applications	x	
A21 Secure HTTP-configuration	x	
A22 Periodically security tests for web applications	x	
Increased protection requirement		
Requirement	fulfilled	Comment
A20 Employing Web application firewalls		End Customer Task Documentation is provided

APP.3.2 Webserver		
Basic Requirements		
Requirement	fulfilled	Comment
A1 Secure configuration	x	
A2 Protection of web server files	x	
A3 Securing file uploads and downloads	x	
A4 Logging events	x	
A5 Authentication	x	
A7 General/legal conditions for web services		Out of Scope
A11 Encryption over TLS	x	
Standard Requirements		
Requirement	fulfilled	Comment
A8 Planning the use of a web server		End Customer Task Documentation is provided
A9 Defining a security policy for the web server		End Customer Task Documentation is provided
A10 Selection of a suitable web-hoster		End Customer Task
A12 Appropriate handling of errors and error messages	x	
A13 Access control for web crawlers		Secomea: Will be fixed in the future
A14 Integrity checks and malware protection	x	

A16 Penetration test and revision	x	
A20 Appointment of contact persons	x	
Increased protection requirement		
Requirement	fulfilled	Comment
A15 Redundancy		Out of Scope May be relevant when GateManager is provided per cloud
A18 Protection against denial-of-service attacks		End Customer Task SiteManager and GateManager are robust against denial-of-service

IND.2.1 General ICS component		
Basic Requirements		
Requirement	fulfilled	Comment
A1 Restrict access to configuration and maintenance interfaces	x	
A2 Use of secure protocols for configuration and maintenance	x	
A4 Deactivation of unused services, functions and interfaces	x	
A6 Network segmentation		End Customer Task Feature is provided
Standard Requirements		
Requirement	fulfilled	Comment
A7 Backups		End Customer Task Feature is provided
A8 Protection against malware	x	Device is hardened
A11 Maintenance of ICS components		End Customer Task
A13 Suitable commissioning of ICS components		End Customer Task
A16 Protection of external interfaces	x	USB can be disabled. Serial port can only be used to interface a PLC or HMI
A17 Use of secure protocols for the transmission of information	x	
Increased protection requirement		
Requirement	fulfilled	Comment

A18 Communication in case of failure		Out of Scope
A19 Security-Tests	x	Partially End Customer Task
A20 Trusted Code	x	

SYS.4.3 Embedded Systems		
Basic Requirements		
Requirement	fulfilled	Comment
A1 Organisation for the deployment of embedded systems		End Customer Task Documentation is provided
A2 Deactivation of unused services, functions and interfaces	x	
A3 Logging security relevant events	x	
Standard Requirements		
Requirement	fulfilled	Comment
A4 Criteria for ordering embedded devices		End Customer Task Documentation is provided
A5 Protection against environmental influences	x	Datasheet for SiteManager mentions enhanced temperature range (between -25℃ and +60℃). Considering the device case a sufficient IP value (IEC 60529) can be assumed (not documented in datasheet). It is assumed that the device is unlikely to be deployed in harsh weather conditions without additional protection.
A6 Prevention of debugging possibilities	x	
A7 Designing hardware and software with security in mind	x	We assume that Secomea does security-by-design. This happens evidently
A8 Secure operating system for embedded devices	x	May be enhanced by introducing a Trusted Platform Module (TPM)

A9 Usage of (co-) cryptoprocessors		Out of scope. No dedicated cryptoprocessor exists for which the connection to the main controller has to be secured.
A10 Restoration of embedded devices	x	
A11 Secure decommissioning of embedded devices		End Customer Task Documentation should be provided if it does not exist yet
Increased protection requirement		
Requirement	fulfilled	Comment
A12 Selecting trustworthy vendors		Out of Scope
A13 Employing a certified operating system		The operating system on the SiteManager should be evaluated with an appropriate standard. (The BSI compendium does not state any explicit standard)
A14 Secure and authenticated boot process		
A15 Protection of memory		Currently Out of scope. Due to the used architecture the entire memory is considered a trusted domain. As such no memory spaces isolated from the trusted domain exist.
A16 Tamper protection		
A17 Automatic health checks for components	x	
A18 Resistance against side-channel attacks		

Conclusion

The assessment of Secomea's concept according compliance to the BSI IT-Grundschutz Compendium revealed that almost all requirements are fulfilled. The standard security level is nearly achieved with only APP.3.2 A13 remaining as a minor issue.

1.3 Evaluation against IEC 62443

The System-under-Consideration (SuC) has been defined, as proposed in the *IEC 62443 part 3-2*, including the boundary and all access points.

Since the focus of the audit are GateManager, SiteManager SiteManager Embedded, LinkManager Mobile and LinkManager, only Secomea components were considered. Other components are not included in this evaluation. If some requirement is not met by a Secomea device, this does not necessarily mean that the evaluation has not been passed. These can optionally be compensated by other measures. Only critical deviations would jeopardize a positive assessment. For a detailed risk assessment each individual use case must be considered separately. This individual consideration is then up to the integrators and users of the components/concept.

1.3.1 IEC 62443-3-3 Analysis

Subsequently the requirements of *IEC 62443 part 3-3*[2] are compared with the shown system configuration. The gray boxes in the tables below are not relevant for the row of a given security level. The reason could be that the part is out of scope for the Secomea components or they are irrelevant for the security level. It is proposed to reach SL 2 first and consider SL 3 in the future.

SR: System requirement
SL-C: Capable security level

IEC 62443-3-3 Evaluation					
	SL-C				
Requirement	1	2	3	4	Comment
FR 1: Identification and authentication control					
SR 1.1 - Human user identification and authentication	x	x	x	x	Requirement fulfilled with enhancement (1), (2) and (3)
SR 1.2 - Software process and device identification and authentication		x	x	x	Requirement fulfilled with enhancement (1)
SR 1.3 - Account management	x	x	x	x	Requirement fulfilled with enhancement (1)

[2] IEC 62443 Part 3-3: System security requirements and security levels, Edition 1.0, August 2013

SR 1.4 - Identifier management	x	x	x	x	Requirement fulfilled
SR 1.5 - Authenticator management	x	x			Requirement fulfilled
SR 1.6 - Wireless access management					Out of scope
SR 1.7 - Strength of password-based authentication	x	x	x	x	Requirement partly fulfilled enhancement (1) and (2), not configurable
SR 1.8 - Public key infrastructure certificates		x	x	x	Requirement fulfilled
SR 1.9 - Strength of public key authentication		x			Requirement fulfilled
SR 1.10 - Authenticator feedback	x	x	x	x	Requirement fulfilled
SR 1.11 - Unsuccessful login attempts	x	x	x	x	Requirement fulfilled
SR 1.12 - System use notification					Requirement not fulfilled; Compensation with additional measures
SR 1.13 - Access via untrusted networks	x	x	x	x	Requirement fulfilled with enhancement (1)
FR 2 - Use control					
SR 2.1 - Authorization enforcement	x	x	x		Requirement fulfilled with enhancement (1), (2) and (3)
SR 2.2 - Wireless use control					Out of Scope
SR 2.3 - Use control for portable and mobile devices	x	x			Requirement fulfilled

SR 2.4 - Mobile code					Not relevant, because only an admin can upload and execute code
SR 2.5 - Session lock	x	x	x	x	Requirement fulfilled
SR 2.6 - Remote session termination		x	x	x	Requirement fulfilled
SR 2.7 - Concurrent session control					
SR 2.8 - Auditable events	x	x	x	x	Requirement fulfilled
SR 2.9 - Audit storage capacity	x	x			Requirement fulfilled
SR 2.10 - Response to audit processing failures	x	x	x	x	Requirement fulfilled
SR 2.11 - Timestamps		x	x		Requirement fulfilled with enhancement (1)
SR 2.12 - Non-repudiation			x	x	Requirement fulfilled with enhancement (1)
FR 3 - System integrity					
SR 3.1 - Communication integrity	x	x	x	x	Requirement fulfilled with enhancement (1)
SR 3.2 - Malicious code protection					Not relevant, because only an admin can upload and execute code
SR 3.3 - Security functionality verification	x	x			Requirement fulfilled
SR 3.4 - Software and information integrity		x			Requirement fulfilled
SR 3.5 - Input validation	x	x	x	x	Requirement fulfilled
SR 3.6 - Deterministic output	x	x	x	x	Requirement fulfilled

SR 3.7 - Error handling		x	x	x	Requirement fulfilled
SR 3.8 - Session integrity		x	x	x	Requirement fulfilled with enhancement (1)
SR 3.9 - Protection of audit information		x	x		Requirement fulfilled
FR 4 - Data confidentiality					
SR 4.1 - Information confidentiality	x	x	x	x	Requirement fulfilled with enhancement (1) and (2)
SR 4.2 - Information persistence		x			Requirement fulfilled
SR 4.3 - Use of cryptography	x	x	x	x	Requirement fulfilled
FR 5 - Restricted data flow					
SR 5.1 - Network segmentation	x	x	x	x	Requirement fulfilled with enhancement (1), (2) and (3)
SR 5.2 - Zone boundary protection	x	x			Requirement fulfilled with enhancement (1) and (2)
SR 5.3 - General purpose person-to-person communication restrictions	x	x	x	x	Requirement fulfilled with enhancement (1)
SR 5.4 - Application partitioning	x	x	x	x	Requirement fulfilled
FR 6 - Timely response to events					
SR 6.1 - Audit log accessibility	x	x	x	x	Requirement fulfilled with enhancement (1)
SR 6.2 - Continuous monitoring					Requirement not fulfilled; Compensation with additional measures
FR 7 - Resource availability					

SR 7.1 - Denial of service protection					Requirement not fulfilled; Compensation with additional measures
SR 7.2 - Resource management	x	x	x	x	Requirement fulfilled
SR 7.3 - Control system backup	x	x	x	x	Requirement fulfilled with enhancement (1) and (2)
SR 7.4 - Control system recovery and reconstitution	x	x	x	x	Requirement fulfilled
SR 7.5 - Emergency power					equirement not fulfilled; Compensation with additional measures
SR 7.6 - Network and security configuration settings	x	x	x	x	Requirement fulfilled with enhancement (1)
SR 7.7 - Least functionality	x	x	x	x	Requirement fulfilled
SR 7.8 - Control system component inventory		x	x	x	Requirement fulfilled

Conclusion

The verification of the requirements against the IEC 62443-3-3 shows that the Secomea concept already provides a good basis for an implementation of an application which corresponds to SuC. However, it should be noted that the Secomea solution does not cover all parts itself. In the GAP analysis the necessary compensation measures for the different security levels are listed.

As a result it can be stated that the Secomea solution is not fully compliant with the IEC 62443-3-3. For full compliance the recommendations in the GAP analysis has to be taken into account.

1.3.2 IEC 62443 3-3 Gap Analysis

The following part contains a IEC 62443-3-3 GAP analysis based on the IEC 62443-3-3 compliance analysis before. Only the Secomea components are considered for GAP analysis. It is divided in four parts according to the four possible security levels. Each security level is based on the previous lower security level and needs also their necessary improvements.

Security Level - SL 1

SR 1.12 System use notification
"The control system shall provide the capability to display a system use notification message before authenticating." The notification message should be configurable by authorized personnel. To meet this requirement on the login screen it should be printed that access to the system is monitored.

SR 7.1 Denial of service protection
The “system shall provide the capability to operate in a degraded mode during a DoS event”. When using the Secomea components appropriate protection must be ensured to be compliant with the IEC 62443-3-3. For example, it can be done using a bandwidth control at network level to block the packet flood and thereby prevent a DoS attack.

SR 7.5 Emergency power
Another statement in the IEC 62443-3-3 is, that the “system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode”. This part should be ensured by an external emergency power supply and appropriate measures to meet the requirements of the IEC 62443-3-3.

Security Level - SL 2

SR 6.2 Continuous monitoring
The “system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner” regarding IEC 62443-3-3. The Secomea components need to be supported by additional measures at this point to be compliant with the IEC 62443-3-3 SL 2. This can be accomplished by various tools, e.g. IDS, IPS.

Security Level - SL 3

SR 1.5 Authenticator management
To achieve IEC 62443-3-3 SL 3 the enhancement (1) of SR 1.5 “Hardware security for software process identity credentials” is needed. This means that the authentication needs to be secured by a hardware security device like a TPM. Therefore the GateManager needs the ability to bind authentication credentials to hardware security devices.

SR 1.9 Strength of public key authentication
For SL3 SR1.9 also needs the enhancement (1) “Hardware security for public key authentication” All relevant private keys have to be secured via “hardware mechanisms according to commonly accepted security industry practices and recommendations”. As in SR1.5(1) this can be achieved by TPMs or other hardware security devices.

SR 2.3 Use control for portable and mobile devices
The SR 2.3 enhancement (1) “Enforcement of security status of portable and mobile devices” needs additional hardware or software to verify that portable or mobile devices which want to connect to a zone comply with the security requirements of that zone.

SR 2.7 Concurrent session control
This requirement expects the components to be able to limit the concurrent sessions per interface for any given user to a configure number of sessions. This means that one user may only login as many parallel sessions at a given time as the number configured.

SR 2.9 Audit storage capacity
For the SL 3 the SR 2.9 enhancement (1) “Warn when audit record storage capacity threshold reached” is needed. Therefore a warning has to be generated “when the allocated audit record storage volume reaches a configurable percentage of maximum audit record storage capacity”. This can be done by a program in the underlying system of the GateManager.

SR 3.3 Security functionality verification
The enhancement (1) “Automated mechanisms for security functionality verification” of SR 3.3 has to be implemented for SL 3. The system needs “automated mechanisms to support management of security verification” during factory acceptance testing, site acceptance testing and scheduled maintenance. This can be done by functions similar to unittest functions which have to be initiated by the system in regular intervals. These functions have to be implemented by Secomea or by additional tools.

SR 3.4 Software and information integrity
For SL3 SR3.4 also needs the enhancement (1) “Automated notification about integrity violations” it is necessary to implement an automated tool that can inform the administrators when wrong integrity measures arise. For that purpose a SIEM could be useful.

SR 4.2 Information persistence
The SR 2.3 enhancement (1) “Purging of shared memory resources” needs “to prevent unauthorized and unintended information transfer via volatile shared memory resources”. Data has to be released secure from volatile memory before the memory can be used by an other user. This has to be ensured by additional software on the host of the SiteManagers.

SR 5.2 Zone boundary protection
For SL 3 the enhancements (2) “Island mode” and (3) “Fail close” are necessary. Therefore additional hardware should be used which provides “the capability to prevent any communication through the control system boundary” and “to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms“. This can be achieved by firewalls which are already recommended by Secomea.

Security Level - SL 4

SR 2.1 Authorization enforcement
For SL 4 of the IEC 62443-3-3 the enhancement (4) “Dual approval” is needed. Therefore the system “shall support dual approval where an action can result in serious impact on the industrial process”. Because of dual approval should be only used for actions which require a very high level of confidence, it is not necessary to implement this in the GateManager, but additional hardware would be necessary to achieve this functionality on the necessary network parts.

SR 2.11 Timestamps
The enhancement (2) is needed for SR 2.11 “protection of time source integrity”. The time source which is used by the system components has to be protected from unauthorized alteration. For this purpose a special hardened NTP-time-server can be used.

SR 3.3 Security functionality verification
For the SR 3.3 enforcement (2) “Security functionality verification during normal operation” the system has to verify the intended operation of security functions during normal operations. This can be done by functions similar to unittest functions which have to be initiated by the system in regular intervals. These functions have to be implemented by Secomea or by additional tools.

SR 3.9 Protection of audit information
The last point to achieve the SL4 is the enhancement (1) “Audit records on write-once media” of SR 3.9. Therefore the audit logs have to be stored on a hardware-enforced write-once media. To achieve this goal a special external log server which provides this functionality can be used.

1.3.3 IEC 62443-4-2 Analysis

A component analyze on basis of the *IEC 62443-4-2* [3] was be done . To reach a SL in IEC 62443 Part 4-2 it is necessary to accomplish IEC 62443 Part 4-1. IEC 62443 Part 4-1 is not part of the audit, the components just have been tested wich parts of the IEC 62443 Part 4-2 are considered.

This analysis gives an overview which requirements are taken into account by the individual parts of the Secomea system. Depending on the device the requirements may be also part of the Network Device Requirements (NDR) or the Software Application Requirments (SAR). The gray boxes are not relevant for the row of a given security level. The reason could be that the part out of scope for the Secomea components or they are irrelevant for the security level. It is proposed to reach SL 2 first and consider SL 3 in the future.

CR: Component requirement
EDR: Embedded device requirement
HDR: Host device requirement
NDR: Network device requiprement
SAR: Software application requirement
SL-C: Capable security level

GateManager

IEC 62443-4-2 Evaluation					
	SL-C				
Requirement	1	2	3	4	Comment
FR 1: Identification and authentication control					
CR 1.1 - Human user identification and authentication	x	x	x	x	Requirement fulfilled with enhancement (1) and (2)
CR 1.2 - Software process and device identification and authentication		x	x	x	Requirement fulfilled with enhancement (1)
CR 1.3 - Account management	x	x	x	x	Requirement fulfilled

[3] IEC 62443 Part 4-2: Technical security requirements for IACS components, Edition 1.0, February 2019

CR 1.4 - Identifier management	x	x	x	x	Requirement fulfilled
CR 1.5 - Authenticator management	x	x			Requirement fulfilled
CR 1.6 - Wireless access management					Not relevant for SAR
CR 1.7 - Strength of password-based authentication	x	x	x	x	Requirement partly fulfilled, not configurable
CR 1.8 - Public key infrastructure certificates		x	x	x	Requirement fulfilled
CR 1.9 - Strength of public key authentication		x			Requirement fulfilled
CR 1.10 - Authenticator feedback	x	x	x	x	Requirement fulfilled
CR 1.11 - Unsuccessful login attempts	x	x	x	x	Requirement fulfilled
CR 1.12 - System use notification					Not Relevant, no local user authentication
CR 1.13 - Access via untrusted networks					Not relevant for SAR
CR 1.14 – Strength of symmetric key authentication		x			Requirement fulfilled
FR 2 - Use control					
CR 2.1 - Authorization enforcement	x	x	x		Requirement fulfilled with enhancement (1), (2) and (3)
CR 2.2 - Wireless use control					Out of scope

CR 2.3 - Use control for portable and mobile devices					Not required in IEC 62443-4-2
SAR 2.4 - Mobil code					Not relevant, because only an admin can upload and execute code
CR 2.5 - Session lock	x	x	x	x	Requirement fulfilled
CR 2.6 - Remote session termination		x	x	x	Requirement fulfilled
CR 2.7 - Concurrent session control					
CR 2.8 - Auditable events	x	x	x	x	Requirement fulfilled
CR 2.9 - Audit storage capacity	x	x			Requirement fulfilled
CR 2.10 - Response to audit processing failures	x	x	x	x	Requirement fulfilled
CR 2.11 - Timestamps	x	x	x		Requirement fulfilled with enhancement (1)
CR 2.12 - Non-repudiation	x	x	x	x	Requirement fulfilled with enhancement (1)
CR 2.13 - Use of physical diagnostic and test interfaces					Not relevant for SAR
FR 3 - System integrity					
CR 3.1 - Communication integrity	x	x	x	x	Requirement fulfilled with enhancement (1)
SAR 3.2 - Protection from malicious code	x	x	x	x	Requirement fulfilled
CR 3.3 - Security functionality verification	x	x	x		Requirement fulfilled

CR 3.4 - Software and information integrity	x	x	x	x	Requirement fulfilled with enhancement (1) and (2)
CR 3.5 - Input validation	x	x	x	x	Requirement fulfilled
CR 3.6 - Deterministic output					Out of Scope
CR 3.7 - Error handling	x	x	x	x	Requirement fulfilled
CR 3.8 - Session integrity		x	x	x	Requirement fulfilled
CR 3.9 - Protection of audit information		x	x		Requirement fulfilled
CR 3.10 - Support for updates					Not relevant for SAR
CR 3.11 - Physical tamper resistance and detection					Not relevant for SAR
CR 3.12 - Provisioning product supplier roots of trust					Not relevant for SAR
CR 3.13 - Provisioning asset owner roots of trust					Not relevant for SAR
CR 3.14 - Integrity of the boot process					Not relevant for SAR
FR 4 - Data confidentiality					
CR 4.1 - Information confidentiality	x	x	x	x	Requirement fulfilled
CR 4.2 - Information persistence		x			Requirement fulfilled
CR 4.3 - Use of cryptography	x	x	x	x	Requirement fulfilled
FR 5 - Restricted data flow					

CR 5.1 - Network segmentation	x	x	x	x	Requirement fulfilled
CR 5.2 - Zone boundary protection					Not relevant for SAR
CR 5.3 - General purpose, person-to-person communication restrictions					Not relevant for SAR
CR 5.4 - Application partitioning					Not required in IEC 62443-4-2
FR 6 - Timely response to events					
CR 6.1 - Audit log accessibility	x	x	x	x	Requirement fulfilled with enhancement (1)
CR 6.2 - Continuous monitoring		x	x	x	Requirement not fulfilled; Compensation with additional measures such as IDS/IPS.
FR 7 - Resource availability					
CR 7.1 - Denial of service protection	x				Requirement fulfilled
CR 7.2 - Resource management	x	x	x	x	Requirement fulfilled
CR 7.3 - Control system backup	x	x	x	x	Requirement fulfilled with enhancement (1)
CR 7.4 - Control system recovery and reconstitution	x	x	x	x	Requirement fulfilled
CR 7.5 - Emergency power					Not required in IEC 62443-4-2
CR 7.6 - Network and security configuration settings	x	x	x	x	Requirement fulfilled with enhancement (1)
CR 7.7 - Least functionality	x	x	x	x	Requirement fulfilled

CR 7.8 - Control system component inventory		x	x	x	Requirement fulfilled

SiteManager

.

IEC 62443-4-2 Evaluation					
	SL-C				
Requirement	1	2	3	4	Comment
FR 1: Identification and authentication control					
CR 1.1 - Human user identification and authentication	x	x	x	x	Requirement fulfilled with enhancement (1) and (2)
CR 1.2 - Software process and device identification and authentication		x	x	x	Requirement fulfilled with enhancement (1)
CR 1.3 - Account management	x	x	x	x	Requirement fulfilled
CR 1.4 - Identifier management	x	x	x	x	Requirement fulfilled
CR 1.5 - Authenticator management	x	x			Requirement fulfilled
NDR 1.6 - Wireless access management					Out of Scope
CR 1.7 - Strength of password-based authentication	x	x			
CR 1.8 - Public key infrastructure certificates					Out of scope. Covered by Gatemanager
CR 1.9 - Strength of public key authentication					Out of scope. Covered by Gatemanager
CR 1.10 - Authenticator feedback	x	x	x	x	Requirement fulfilled

CR 1.11 - Unsuccessful login attempts	x	x	x	x	Requirement fulfilled
CR 1.12 - System use notification					Not Relevant, no local user authentication
NDR 1.13 - Access via untrusted networks	x	x	x	x	Requirement fulfilled with enhancement (1)
CR 1.14 – Strength of symmetric key authentication		x			Requirement fulfilled
FR 2 - Use control					
CR 2.1 - Authorization enforcement	x	x			Requirement fulfilled with enhancement (1) and (2)
CR 2.2 - Wireless use control					Out of scope
CR 2.3 - Use control for portable and mobile devices					Not required in IEC 62443-4-2
NDR 2.4 - Mobil code					Not relevant, because no mobil code execution possible
CR 2.5 - Session lock					Requirement not fulfilled; Compensation with additional measures
CR 2.6 - Remote session termination		x	x	x	Requirement fulfilled
CR 2.7 - Concurrent session control					
CR 2.8 - Auditable events	x	x	x	x	Requirement fulfilled
CR 2.9 - Audit storage capacity	x	x	x	x	Requirement fulfilled with enhancement (1)
CR 2.10 - Response to audit processing failures	x	x	x	x	Requirement fulfilled

CR 2.11 - Timestamps	x	x	x		Requirement fulfilled with enhancement (1)
CR 2.12 - Non-repudiation	x	x	x		Requirement fulfilled
NDR 2.13 - Use of physical diagnostic and test interfaces		x			Requirement fulfilled
FR 3 - System integrity					
CR 3.1 - Communication integrity	x	x	x	x	Requirement fulfilled with enhancement (1)
NDR 3.2 - Protection from malicious code	x	x	x	x	Requirement fulfilled
CR 3.3 - Security functionality verification	x	x	x		Requirement fulfilled
CR 3.4 - Software and information integrity	x	x	x	x	Requirement fulfilled with enhancement (1) and (2)
CR 3.5 - Input validation	x	x	x	x	Requirement fulfilled
CR 3.6 - Deterministic output	x	x	x	x	Requirement fulfilled
CR 3.7 - Error handling	x	x	x	x	Requirement fulfilled
CR 3.8 - Session integrity		x	x	x	Requirement fulfilled
CR 3.9 - Protection of audit information		x	x		Requirement fulfilled
NDR 3.10 - Support for updates	x	x	x	x	Requirement fulfilled with enhancement (1)

NDR 3.11 - Physical tamper resistance and detection					Requirement not fulfilled. Tamper resistance may be provided by the end customer. This can be done by locking the SiteManager appropriately away. A door switch to detect the door/lock being opened may be used to send an automatic message to the administrators or similar personnel.
NDR 3.12 - Provisioning product supplier roots of trust		x	x	x	Requirement fulfilled
NDR 3.13 - Provisioning asset owner roots of trust					This requirement is relevant if the end customer can deploy mobile code, user programs and similar. Since the SiteManager is not intended for the end customer to add software on it, this requirement is not relevant.
NDR 3.14 - Integrity of the boot process	x				Requirement fulfilled
FR 4 - Data confidentiality					
CR 4.1 - Information confidentiality	x	x	x	x	Requirement fulfilled
CR 4.2 - Information persistence		x			Requirement fulfilled
CR 4.3 - Use of cryptography	x	x	x	x	Requirement fulfilled
FR 5 - Restricted data flow					
CR 5.1 - Network segmentation	x	x	x	x	Requirement fulfilled
NDR 5.2 - Zone boundary protection	x	x			Requirement fulfilled with enhancement (1)

NDR 5.3 - General purpose, person-to-person communication restrictions	x	x	x	x	Requirement fulfilled
CR 5.4 - Application partitioning					Not required in IEC 62443-4-2
FR 6 - Timely response to events					
CR 6.1 - Audit log accessibility	x	x	x	x	Requirement fulfilled with enhancement (1)
CR 6.2 - Continuous monitoring					Requirement not fulfilled; Compensation with additional measures such as IDS/IPS.
FR 7 - Resource availability					
CR 7.1 - Denial of service protection					Requirement not fulfilled; Compensation with additional measures
CR 7.2 - Resource management	x	x	x	x	Requirement fulfilled
CR 7.3 - Control system backup	x	x	x	x	Requirement fulfilled with enhancement (1)
CR 7.4 - Control system recovery and reconstitution	x	x	x	x	Requirement fulfilled
CR 7.5 - Emergency power					Not required in IEC 62443-4-2
CR 7.6 - Network and security configuration settings	x	x	x	x	Requirement fulfilled with enhancement (1)
CR 7.7 - Least functionality	x	x	x	x	Requirement fulfilled
CR 7.8 - Control system component inventory		x	x	x	Requirement fulfilled

SiteManager Embedded

IEC 62443-4-2 Evaluation					
	SL-C				
Requirement	1	2	3	4	Comment
FR 1: Identification and authentication control					
CR 1.1 - Human user identification and authentication	x	x			Requirement fulfilled with enhancement (1) and (2)
CR 1.2 - Software process and device identification and authentication		x			Requirement fulfilled
CR 1.3 - Account management	x	x	x	x	Requirement fulfilled
CR 1.4 - Identifier management	x	x	x	x	Requirement fulfilled
CR 1.5 - Authenticator management	x	x			Requirement fulfilled
CR 1.6 - Wireless access management					Not relevant for SAR
CR 1.7 - Strength of password-based authentication	x	x	x	x	Requirement partly fulfilled through Gatemanager integration, not configurable
CR 1.8 - Public key infrastructure certificates		x	x	x	Requirement fulfilled through Gatemanager integration
CR 1.9 - Strength of public key authentication		x			Requirement fulfilled through Gatemanager integration
CR 1.10 - Authenticator feedback	x	x	x	x	Requirement fulfilled

CR 1.11 - Unsuccessful login attempts	x	x	x	x	Requirement fulfilled through Gatemanager integration
CR 1.12 - System use notification					Not Relevant, no local user authentication
CR 1.13 - Access via untrusted networks					Not relevant for SAR
CR 1.14 – Strength of symmetric key authentication		x			Requirement fulfilled
FR 2 - Use control					
CR 2.1 - Authorization enforcement	x	x	x		Requirement fulfilled with enhancement (1), (2) and (3)
CR 2.2 - Wireless use control					Out of scope
CR 2.3 - Use control for portable and mobile devices					Not required in IEC 62443-4-2
SAR 2.4 - Mobil code					Out of scope
CR 2.5 - Session lock	x	x	x	x	Requirement fulfilled
CR 2.6 - Remote session termination		x	x	x	Requirement fulfilled through Gatemanager integration
CR 2.7 - Concurrent session control					
CR 2.8 - Auditable events	x	x	x	x	Requirement fulfilled
CR 2.9 - Audit storage capacity	x	x			Requirement fulfilled through Gatemanager integration
CR 2.10 - Response to audit processing failures	x	x	x	x	Requirement fulfilled
CR 2.11 - Timestamps	x	x	x		Requirement fulfilled with enhancement (1)

CR 2.12 - Non-repudiation	x	x	x	x	Requirement fulfilled with enhancement (1)
CR 2.13 - Use of physical diagnostic and test interfaces					Not relevant for SAR
FR 3 - System integrity					
CR 3.1 - Communication integrity	x	x	x	x	Requirement fulfilled with enhancement (1)
SAR 3.2 - Protection from malicious code	x	x	x	x	Requirement fulfilled
CR 3.3 - Security functionality verification	x	x	x		Requirement fulfilled
CR 3.4 - Software and information integrity	x	x	x	x	Requirement fulfilled with enhancement (1) and (2)
CR 3.5 - Input validation	x	x	x	x	Requirement fulfilled
CR 3.6 - Deterministic output					Out of Scope
CR 3.7 - Error handling	x	x	x	x	Requirement fulfilled
CR 3.8 - Session integrity		x	x	x	Requirement fulfilled
CR 3.9 - Protection of audit information		x	x		Requirement fulfilled
CR 3.10 - Support for updates					Not relevant for SAR
CR 3.11 - Physical tamper resistance and detection					Not relevant for SAR
CR 3.12 - Provisioning product supplier roots of trust					Not relevant for SAR

CR 3.13 - Provisioning asset owner roots of trust					Not relevant for SAR
CR 3.14 - Integrity of the boot process					Not relevant for SAR
FR 4 - Data confidentiality					
CR 4.1 - Information confidentiality	x	x	x	x	Requirement fulfilled
CR 4.2 - Information persistence		x			Requirement fulfilled
CR 4.3 - Use of cryptography	x	x	x	x	Requirement fulfilled
FR 5 - Restricted data flow					
CR 5.1 - Network segmentation	x	x	x	x	Requirement fulfilled
CR 5.2 - Zone boundary protection					Not relevant for SAR
CR 5.3 - General purpose, person-to-person communication restrictions					Not relevant for SAR
CR 5.4 - Application partitioning					Not required in IEC 62443-4-2
FR 6 - Timely response to events					
CR 6.1 - Audit log accessibility	x	x	x	x	Requirement fulfilled with enhancement (1) through Gatemanager integration
CR 6.2 - Continuous monitoring		x	x	x	Requirement not fulfilled; Compensation with additional measures such as IDS/IPS.
FR 7 - Resource availability					

CR 7.1 - Denial of service protection	x				Requirement fulfilled
CR 7.2 - Resource management	x	x	x	x	Requirement fulfilled
CR 7.3 - Control system backup	x	x	x	x	Requirement fulfilled with enhancement (1) through Gatemanager integration
CR 7.4 - Control system recovery and reconstitution	x	x	x	x	Requirement fulfilled through Gatemanager integration
CR 7.5 - Emergency power					Not required in IEC 62443-4-2
CR 7.6 - Network and security configuration settings	x	x	x	x	Requirement fulfilled with enhancement (1)
CR 7.7 - Least functionality	x	x	x	x	Requirement fulfilled through Gatemanager integration
CR 7.8 - Control system component inventory		x	x	x	Requirement fulfilled through Gatemanager integration

LinkManager Mobile

IEC 62443-4-2 Evaluation					
	SL-C				
Requirement	1	2	3	4	Comment
FR 1: Identification and authentication control					
CR 1.1 - Human user identification and authentication	x	x			Requirement fulfilled with enhancement (1) and (2)
CR 1.2 - Software process and device identification and authentication		x			Requirement fulfilled
CR 1.3 - Account management	x	x	x	x	Requirement fulfilled
CR 1.4 - Identifier management	x	x	x	x	Requirement fulfilled
CR 1.5 - Authenticator management	x	x			Requirement fulfilled
CR 1.6 - Wireless access management					Not relevant for SAR
CR 1.7 - Strength of password-based authentication	x	x	x	x	Requirement partly fulfilled through Gatemanager integration, not configurable
CR 1.8 - Public key infrastructure certificates		x	x	x	Requirement fulfilled through Gatemanager integration
CR 1.9 - Strength of public key authentication		x			Requirement fulfilled through Gatemanager integration
CR 1.10 - Authenticator feedback	x	x	x	x	Requirement fulfilled

CR 1.11 - Unsuccessful login attempts	x	x	x	x	Requirement fulfilled through Gatemanager integration
CR 1.12 - System use notification					Not Relevant, no local user authentication
CR 1.13 - Access via untrusted networks					Not relevant for SAR
CR 1.14 – Strength of symmetric key authentication		x			Requirement fulfilled
FR 2 - Use control					
CR 2.1 - Authorization enforcement	x	x	x		Requirement fulfilled with enhancement (1), (2) and (3)
CR 2.2 - Wireless use control					Out of scope
CR 2.3 - Use control for portable and mobile devices					Not required in IEC 62443-4-2
SAR 2.4 - Mobil code					Out of scope
CR 2.5 - Session lock	x	x	x	x	Requirement fulfilled
CR 2.6 - Remote session termination		x	x	x	Requirement fulfilled through Gatemanager integration
CR 2.7 - Concurrent session control					
CR 2.8 - Auditable events	x	x	x	x	Requirement fulfilled
CR 2.9 - Audit storage capacity	x	x			Requirement fulfilled through Gatemanager integration
CR 2.10 - Response to audit processing failures	x	x	x	x	Requirement fulfilled
CR 2.11 - Timestamps	x	x	x		Requirement fulfilled with enhancement (1)

CR 2.12 - Non-repudiation	x	x	x	x	Requirement fulfilled with enhancement (1)
CR 2.13 - Use of physical diagnostic and test interfaces					Not relevant for SAR
FR 3 - System integrity					
CR 3.1 - Communication integrity	x	x	x	x	Requirement fulfilled with enhancement (1)
SAR 3.2 - Protection from malicious code	x	x	x	x	Requirement fulfilled
CR 3.3 - Security functionality verification	x	x	x		Requirement fulfilled
CR 3.4 - Software and information integrity	x	x	x	x	Requirement fulfilled with enhancement (1) and (2)
CR 3.5 - Input validation	x	x	x	x	Requirement fulfilled
CR 3.6 - Deterministic output					Out of Scope
CR 3.7 - Error handling	x	x	x	x	Requirement fulfilled
CR 3.8 - Session integrity		x	x	x	Requirement fulfilled
CR 3.9 - Protection of audit information		x	x		Requirement fulfilled
CR 3.10 - Support for updates					Not relevant for SAR
CR 3.11 - Physical tamper resistance and detection					Not relevant for SAR
CR 3.12 - Provisioning product supplier roots of trust					Not relevant for SAR

CR 3.13 - Provisioning asset owner roots of trust					Not relevant for SAR
CR 3.14 - Integrity of the boot process					Not relevant for SAR
FR 4 - Data confidentiality					
CR 4.1 - Information confidentiality	x	x	x	x	Requirement fulfilled
CR 4.2 - Information persistence		x			Requirement fulfilled
CR 4.3 - Use of cryptography	x	x	x	x	Requirement fulfilled
FR 5 - Restricted data flow					
CR 5.1 - Network segmentation	x	x	x	x	Requirement fulfilled
CR 5.2 - Zone boundary protection					Not relevant for SAR
CR 5.3 - General purpose, person-to-person communication restrictions					Not relevant for SAR
CR 5.4 - Application partitioning					Not required in IEC 62443-4-2
FR 6 - Timely response to events					
CR 6.1 - Audit log accessibility	x	x	x	x	Requirement fulfilled with enhancement (1) through Gatemanager integration
CR 6.2 - Continuous monitoring		x	x	x	Requirement not fulfilled; Compensation with additional measures such as IDS/IPS.
FR 7 - Resource availability					

CR 7.1 - Denial of service protection	x				Requirement fulfilled
CR 7.2 - Resource management	x	x	x	x	Requirement fulfilled
CR 7.3 - Control system backup	x	x	x	x	Requirement fulfilled with enhancement (1) through Gatemanager integration
CR 7.4 - Control system recovery and reconstitution	x	x	x	x	Requirement fulfilled through Gatemanager integration
CR 7.5 - Emergency power					Not required in IEC 62443-4-2
CR 7.6 - Network and security configuration settings	x	x	x	x	Requirement fulfilled with enhancement (1)
CR 7.7 - Least functionality	x	x	x	x	Requirement fulfilled through Gatemanager integration
CR 7.8 - Control system component inventory		x	x	x	Requirement fulfilled through Gatemanager integration

1.4 System Audit Conclusion

BSI Compendium Conclusion

The concept audit shows that most requirements for the standard level as described in the BSI Compendium are fulfilled. The only remaining issue is APP.3.2 - A13 which should be handled in short-term. All other issues are related to the increased protection level which can be considered a long-term goal.

APP.3.2 - A13 Access control for web crawlers

By introducing a robots.txt for well-meaning web crawlers of web search engines such as Google and limiting access to content for malicious web crawlers this requirement will be fulfilled. For the malicious web crawlers there is already sufficient access control in place requiring a login to reach the user interface of the GateManager. As such only the robots.txt remains to be implemented.

SYS.4.3 - A14 Secure and authenticated boot process

For ensuring tamper detection in regards of the firmware, a secure boot process should be implemented. The boot process shall create a hash or similar cryptographic value and compare this value with a previously created and stored of the current firmware. If the newly measured/created value is the same as the previous one, the firmware is authenticated and the boot process may continue. For the protection objective of availability the boot process may continue regardless, but the issues of incorrect values have to be passed to a central platform such as the GateManager.

SYS.4.3 - A15 Protection of memory

Once more memory domains than the trusted domain are to be implemented, appropriate security mechanism such as ARM Trustzone and similar should be considered and implemented.

SYS.4.3 - A16 Tamper protection

To protect a device tampering it should be detected by either a tamper evident tape or a circuit which can be checked by the firmware. Also to prevent tamper attacks, a best practice guide may be issued to the customers, so they can lock the SiteManager et all securely against physical attacks. Also a plan with countermeasures should be established in case of a successful tampering attack. This plan may also be communicated to the customer via a best practice guide.

SYS.4.3 - A18 Resistance against side-channel attacks

To prevent side-channel attacks such as timing attacks, security critical operations should be implemented in such a way that by measure the power signals on I/Os cannot be used to determine the values transmitted or that currently a critical operation is running. A typical way is to make all kinds of operations look the same in terms of time required and sequency.

IEC 62443 Conclusion

In conclusion for the IEC 62443 we can state that the Secomea concept mostly achieves security level (SL) 2 with good progress towards SL 3. The remaining system requirements (SR) and component requirements (CR) to achieve an overall security level of 3 can be compensated by additional means in the field where the Secomea concept is deployed. With sufficient documentation for the end user as well as enough effort by the end user the overall security level of 2 can be achieved for remote maintenance today.

Following compensation measures may be necessary to be deployed by the end user:

SR 5.2 - Zone boundary protection

Deploying a proper configured firewall for SR 5.2 segmentating control system networks from non-control system networks and other control system networks. Additionally the firewall should be configured to deny all traffic by default to the control system network and only allow other traffic by exception as necessary. As the Secomea concept only uses outgoing connections, a standard configured firewall will be sufficient.

SR 6.2 - Continuous monitoring

For continuously monitoring the Secomea devices an intrusion detection system (IDS) or similar may be deployed near the places the SiteManager and GateManager are used. The IDS should analyze the network traffic related to the SiteManagers and the GateManager in terms of meta data (source IP/port, destination IP/port, protocol flags such as TCP SYN to determine who initiated the connection, etc.) and possibly in terms of deep packet inspection (DPI) to verify the contents of the packets if possible.

SR 7.1 - Denial of service protection

To further protect the SiteManager and GateManager from DoS attacks, the relevant network components including switches, gateways and other parts of a network/web infrastructure should be configured to throttle bandwidth if possible once a high load is detected from one or more possible DoS sources.

SR 7.5 - Emergency power

To fulfill this requirement the SiteManager and GateManager components should be connected to uninterruptible power supply (UPS) as necessary.