

Designing and Testing Security Capabilities according to IEC 62443-4-2

Peter Panholzer 10.10.2023, Wien



Who we are

- Vendor-independent cybersecurity consulting company founded in 2012
- Experts in the field of OT security and secure product development
- European, owner-managed company
- More than 30 highly qualified cybersecurity experts in three key locations
- Background from 160+ years of field experience through many challenging industrial security projects



What we help with

Areas of expertise



Secure operation of industrial facilities

We assist you with identifying technical and organizational weaknesses in your organization, aid you in setting up effective and efficient security organizations and implement appropriate countermeasures.

Secure development of products and solutions

We help you to identify defects in your products and solutions, assist with the setup of secure development practices and coach you to deal with vulnerabilities in the long run.

Training and certification of industrial staff

We enable you to build and integrate security capabilities into your organization through top-class security trainings and certification of your staff

IEC 62443 – Target groups & standard parts

General	IEC 62443-1-1 Concepts and Models	IEC/TR 62443-1-2 Master Glossary of Terms and Abbreviations	IEC 62443-1-3 System Security Compliance Metrics	IEC 62443-1-4 Security Life Cycle and Use Case
Operators	IEC 62443-2-1 Requirements for an IACS Security Management System	IEC 62443-2-2 Implementation Guidance for an IACS Security Management System	IEC/TR 62443-2-3 Patch Management in the IACS Environment	IEC 62443-2-4 Requirements for IACS Solution Provider
System integrators	IEC/TR 62443-3-1 Security Technologies for IACS	IEC 62443-3-2 Security Risk Assessment and System Design	IEC 62443-3-3 System Security Requirements and Security Levels	
Component vendors	IEC 62443-4-1 Product Development Requirements	IEC 62443-4-2 Technical Security Requirements for IACS components		

IEC 62443-4-1 Product Security Requirements Processes

IEC 62443 describes three processes in regard to security requirements.



SR-3: Product security requirements

Process to ensure that security requirements are documented



SR-4: Product security requirements content

Process to ensure that relevant content is included in the documented requirements



SR-5: Security requirements review

Process to ensure that reviews are conducted for all requirements and that they get updated (deleted, revised)

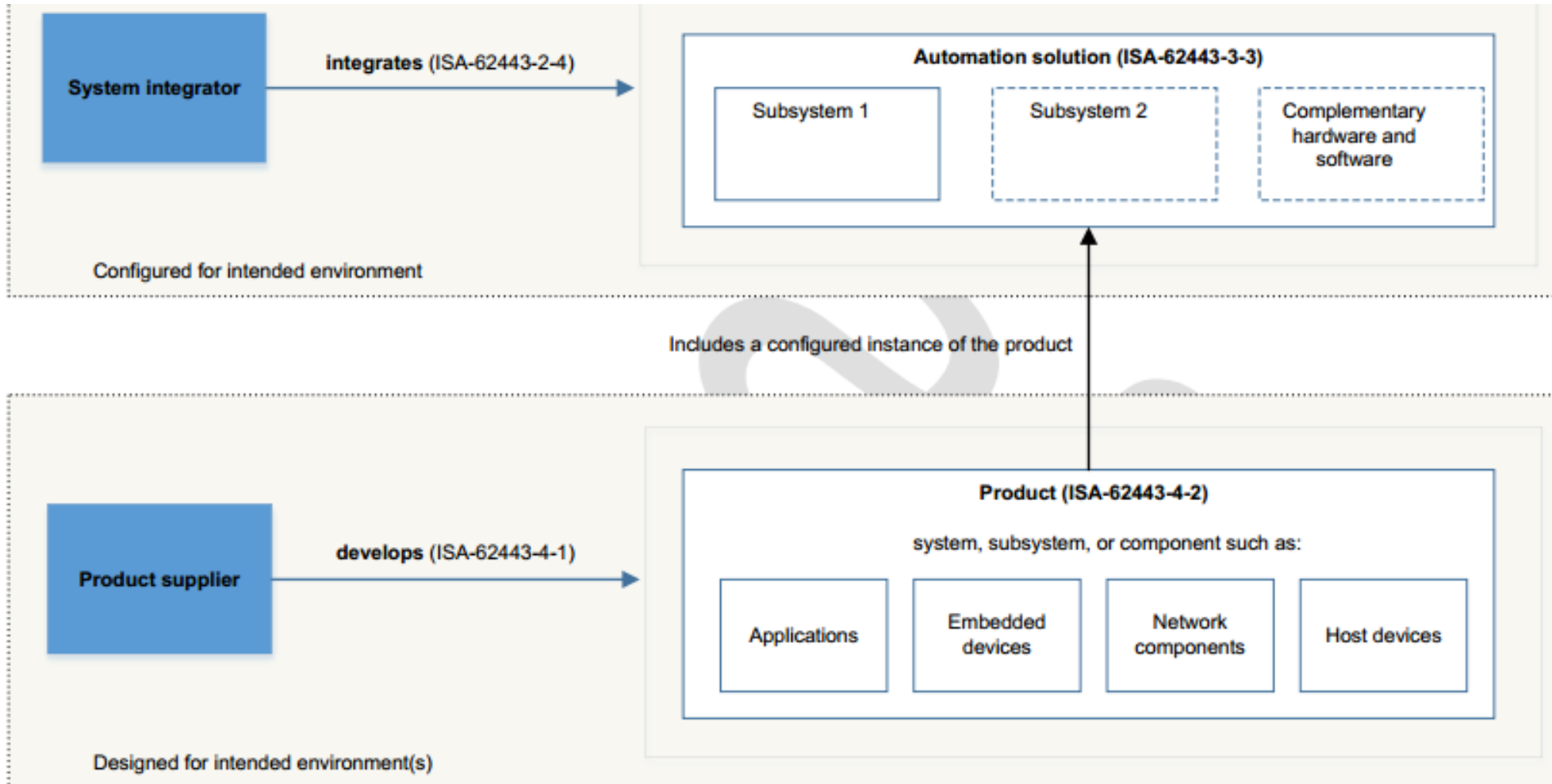
Development Of Security Requirements

To increase security during development it is needed to identify and define security requirements in the first place.



IEC 62443 Scope

Addressed to all participants of the ICS and SCADA system life cycle



Component Requirements (CRs)

The component requirements (CRs) are derived from the system requirements (SRs) in IEC 62443-3-3 and are designated to the following types of components:

- Software application
- Embedded device
- Host device
- Network device

Foundational Requirements

The component requirements (CRs) are derived from the system requirements (SRs) in IEC 62443-3-3

- The requirements are grouped in 7 **foundational requirements**
 - FR 1 – Identification and authentication control
 - FR 2 – Use control
 - FR 3 – System integrity
 - FR 4 – Data confidentiality
 - FR 5 – Restricted data flow
 - FR 6 – Timely response to events
 - FR 7 – Resource availability

Common Component Security Constraints

Must be applied during the implementation of the described requirements

- Support of essential functions
- Compensating countermeasures
- Least privilege
- Software development process

Meet the KNX BCU Key



- The BCU Key allows to set a device password to protect against modification
- Once the BCU key is set, the following actions are no longer possible:
 - Change the parameters / memory
 - Change the programming
 - Reset the device -> Bricked
- Hardly documented
- Helpful for ransomware for your building automation
- **Violates the support of essential functions**

Use Of Security Levels

The IEC 62443-1-1 defines security levels based on the expected threat actors

Level	Description
SL 0	No security requirements or protection
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentionl violation using simple means with low resources, generic skills and low motivation
SL 3	Protection against intentionl violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Security Requirements are statically mapped to security levels

The classification of BR & RE into security levels leads to a "compliance approach"

Table B.1 – Mapping of SRs and REs to FR SL levels 1-4 (1 of 4)

SRs and REs		SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)					
SR 1.1 – Human user identification and authentication	5.3	✓	✓	✓	✓
SR 1.1 RE 1 – Unique identification and authentication	5.3.3.1		✓	✓	✓
SR 1.1 RE 2 – Multifactor authentication for untrusted networks	5.3.3.2			✓	✓
SR 1.1 RE 3 – Multifactor authentication for all networks	5.3.3.3				✓
SR 1.2 – Software process and device identification and authentication	5.4		✓	✓	✓
SR 1.2 RE 1 – Unique identification and authentication	5.4.3.1			✓	✓
SR 1.3 – Account management	5.5	✓	✓	✓	✓
SR 1.3 RE 1 – Unified account management	5.5.3.1			✓	✓
SR 1.4 – Identifier management	5.6	✓	✓	✓	✓
SR 1.5 – Authenticator management	5.7	✓	✓	✓	✓
SR 1.5 RE 1 – Hardware security for software process identity credentials	5.7.3.1			✓	✓

Profiles (IEC 62443-1-5)

An IEC 62443 cyber security profile is a defined set of IEC 62443 requirements.

- These selected requirements can for example be mapped to:
 - a specific application domain (e.g. discrete manufacturing, process industry);
 - an area of activity (e.g. integration, patch management);
 - the intended operational environment and the security context of a product (component, system) or automation solution; or
 - particular type(s) of product(s).
- The cyber security profile shall be based on a security risk evaluation that is appropriate to the specific application domain, area of activity and the intended operational environment.
- The cyber security profile shall refer to a single or multiple IEC 62443 standard(s) (TS/IS) and select a set of requirements from those IEC 62443 standard(s).
- The profile shall not introduce new requirements
- The cyber security profile may select a minimum security level

A story of missing component capabilities

Hacking

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people



Cyber-flaw affects 745,000 pacemakers

30 August 2017

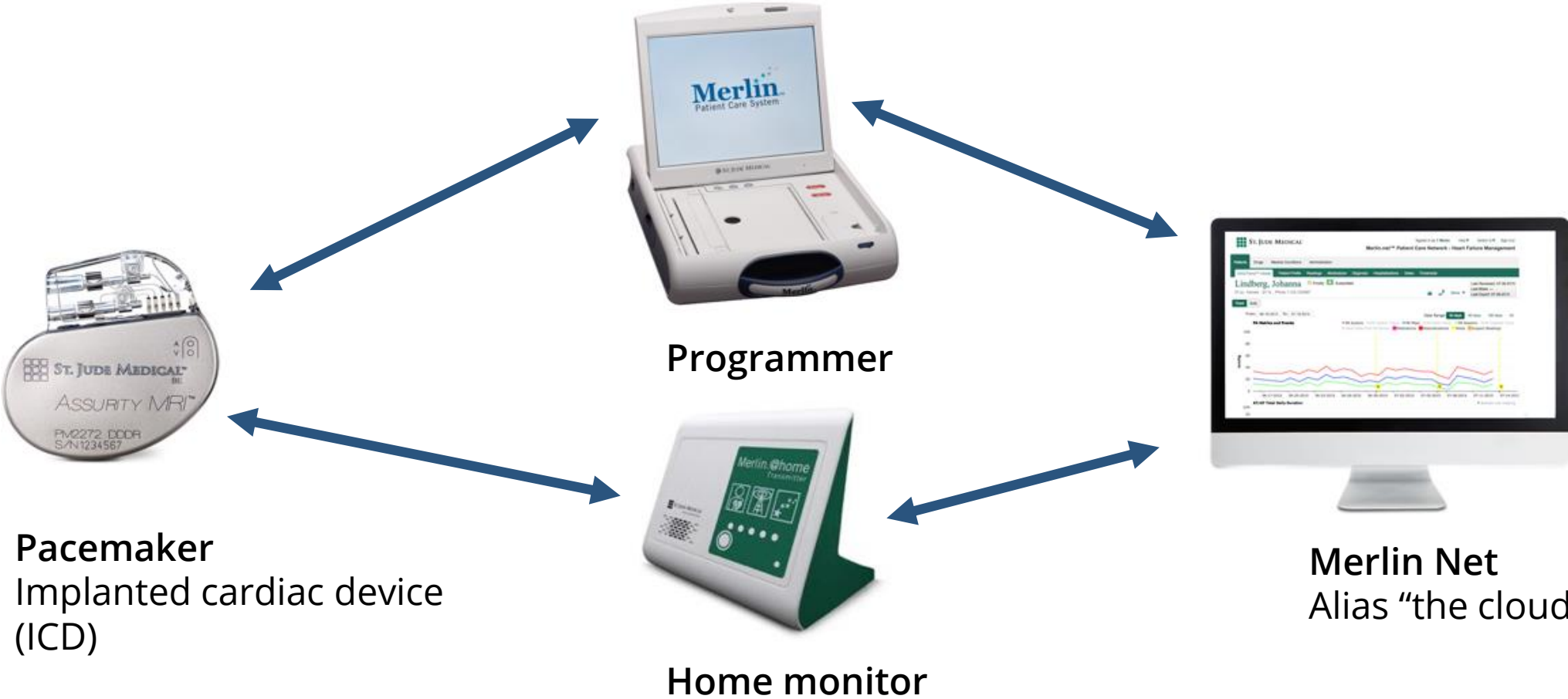
[f](#) [m](#) [t](#) [e](#) [Share](#)



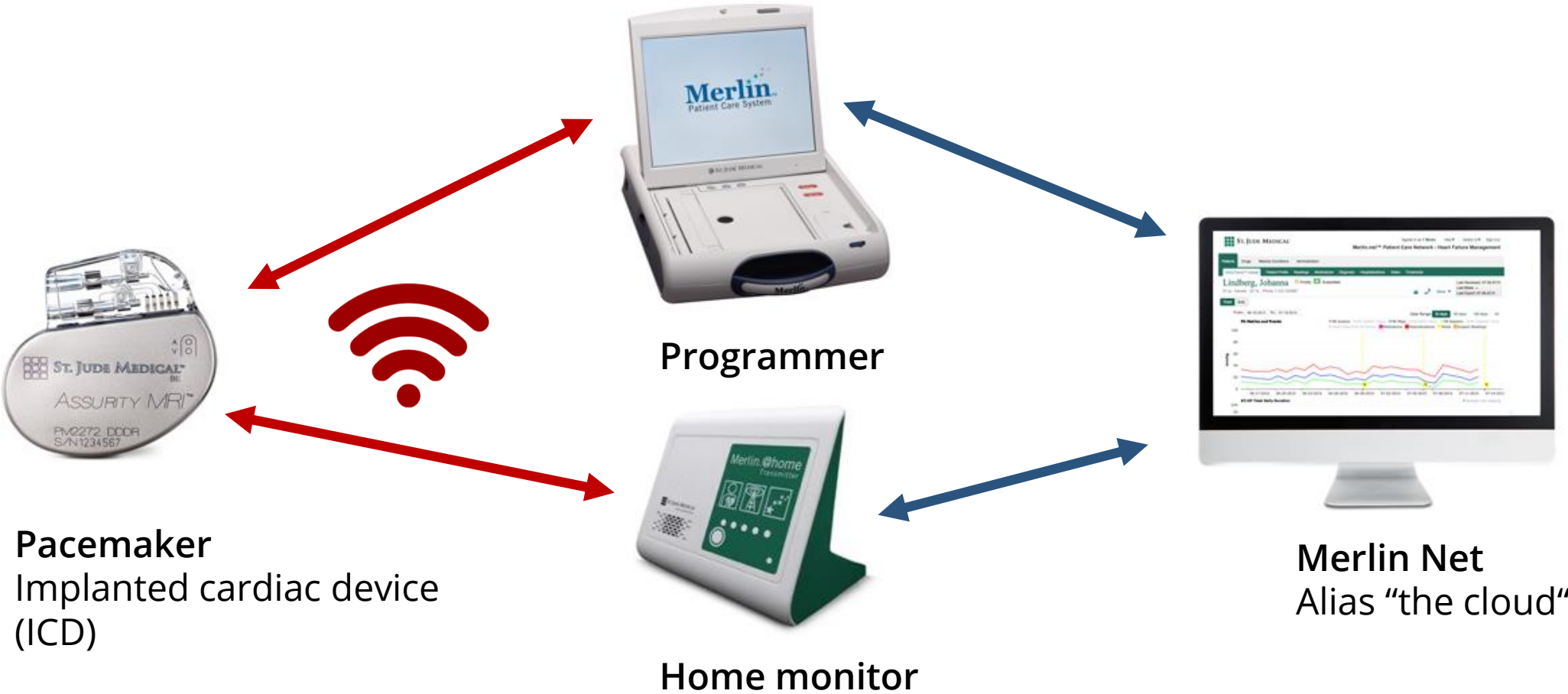
A total of 745,000 pacemakers have been confirmed as having cyber-security issues that could let them be hacked.

The Food and Drug Administration **revealed that 465,000 pacemakers** in the US were affected, in an advisory note about a fix to the problem.

The ecosystem



The ecosystem



First attack vector

- New generation is able to communicate wireless
- Medical Implant Communication System (MICS)
 - low-power, short-range (2 m)
 - high-data-rate
 - 401–406 MHz (the core band is 402–405 MHz)
 - accepted worldwide for transmitting data to support the diagnostic or therapeutic functions associated with medical implant devices.
- Software Defined Radio / GNURadio



First vulnerabilities identified

- Energy depletion attack
- Crash attack



This violates e.g.

11.3 CR 7.1 – Denial of service protection

11.3.1 Requirement

Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event.

11.3.2 Rationale and supplemental guidance

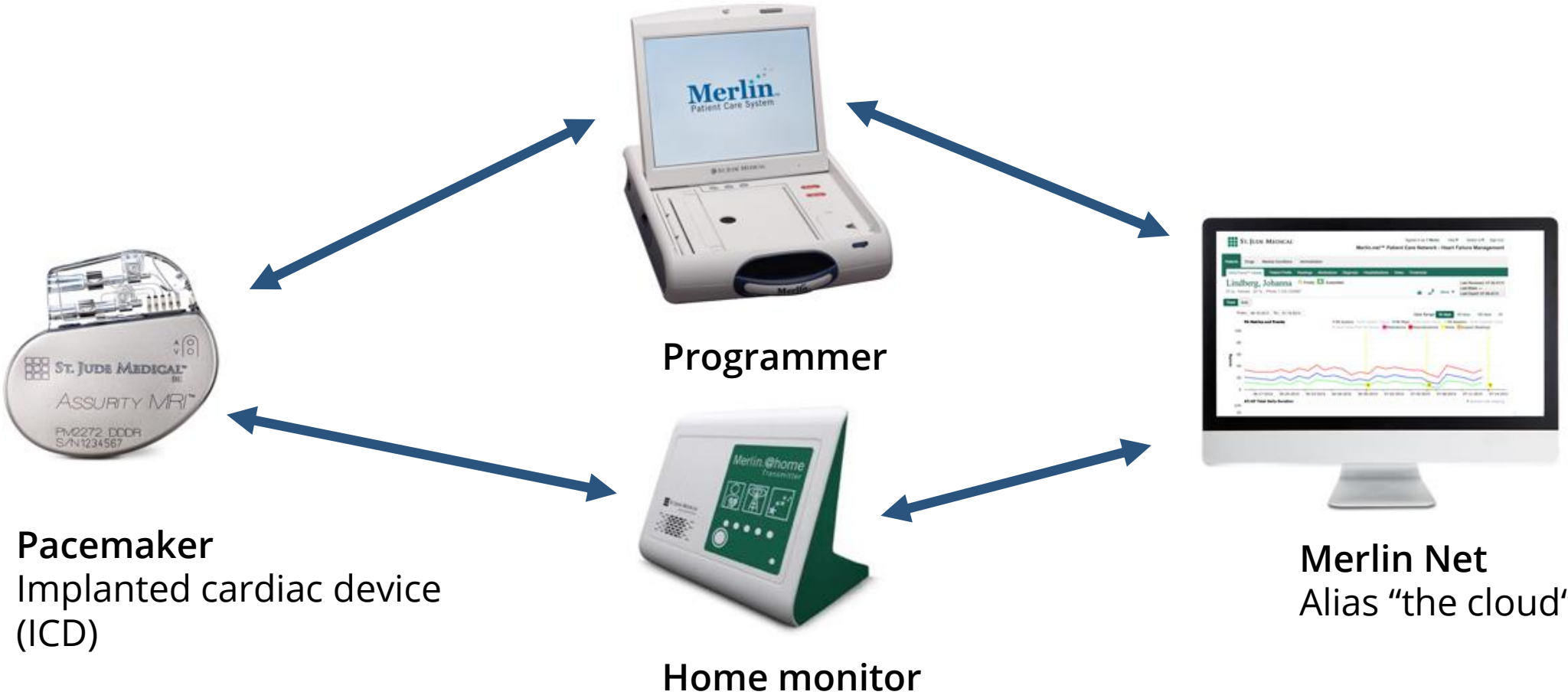
Components may be subjected to different forms of DoS situations. When these occur, the component should be designed in such a manner that it maintains essential functions necessary for continued safe operations while in a degraded mode.

11.3.3 Requirement enhancements

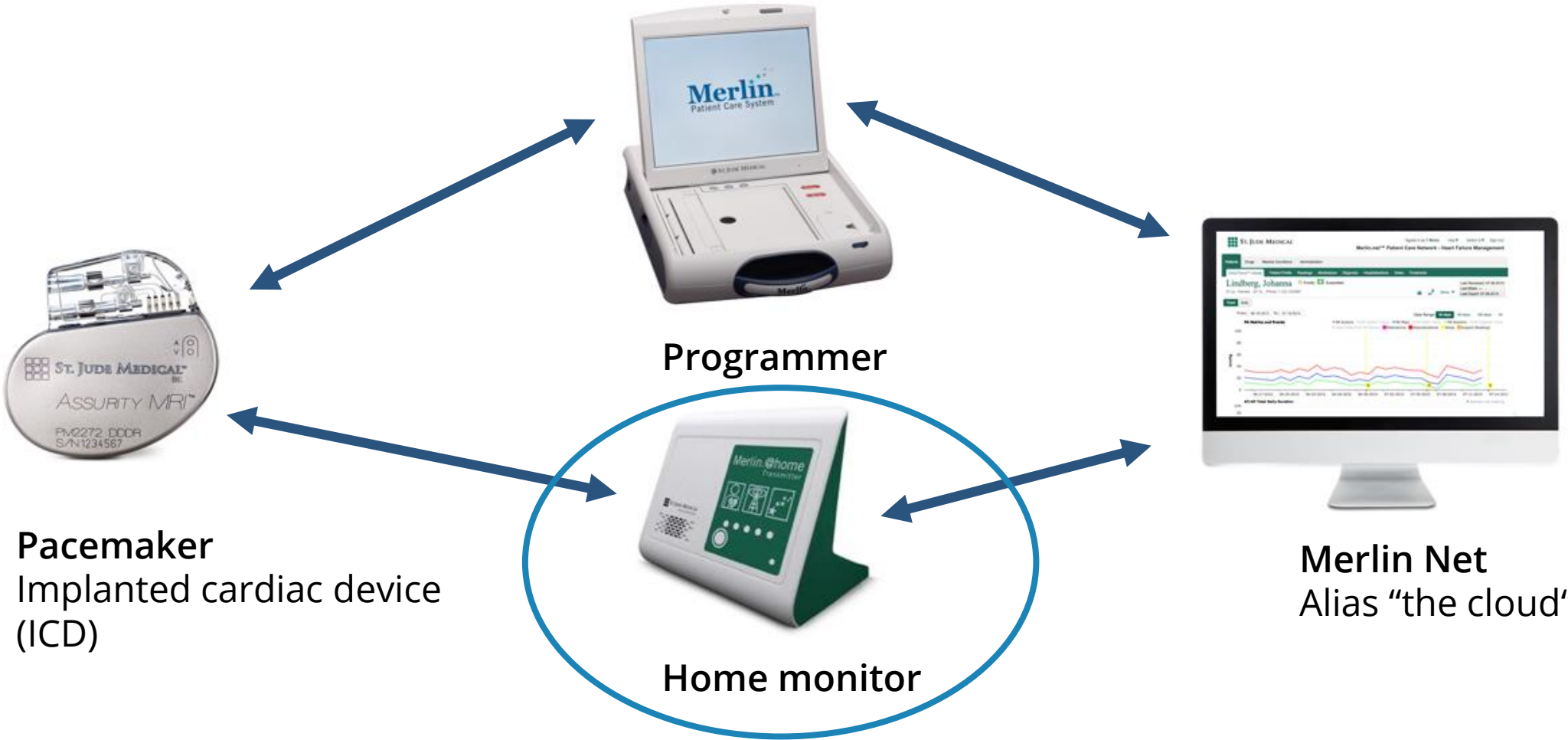
(1) Manage communication load from component

Components shall provide the capability to mitigate the effects of information and/or message flooding types of DoS events.

What else to attack?

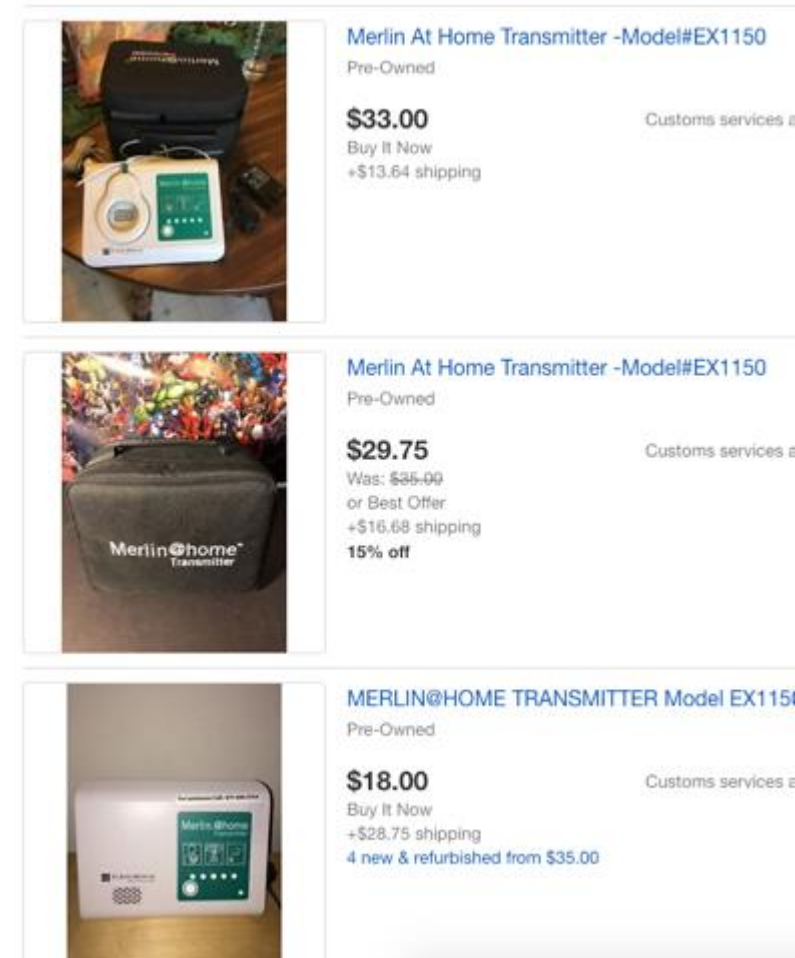


What else to attack?



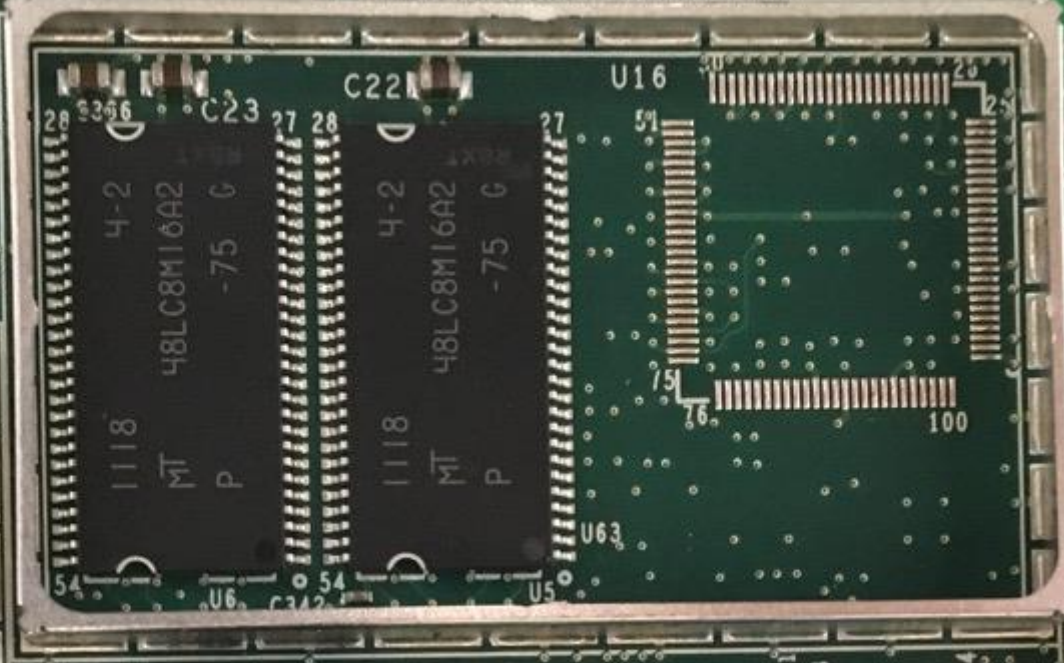
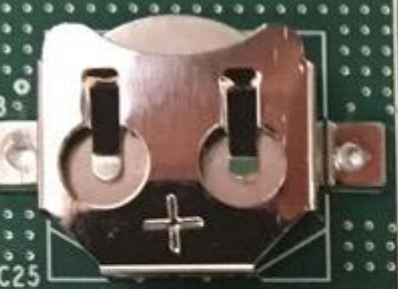
Merlin@Home

- Home monitor for patients
- Transmits health data to doctor
- Huge comfort benefits for patient
- Available interfaces
 - RJ11 jack
 - USB interface



Listing Title	Price	Shipping	Other Info
Merlin At Home Transmitter -Model#EX1150 Pre-Owned	\$33.00	+\$13.64 shipping	Buy It Now
Merlin At Home Transmitter -Model#EX1150 Pre-Owned	\$29.75	+\$16.68 shipping	Was: \$36.00 or Best Offer 15% off
MERLIN@HOME TRANSMITTER Model EX1150 Pre-Owned	\$18.00	+\$28.75 shipping	4 new & refurbished from \$35.00

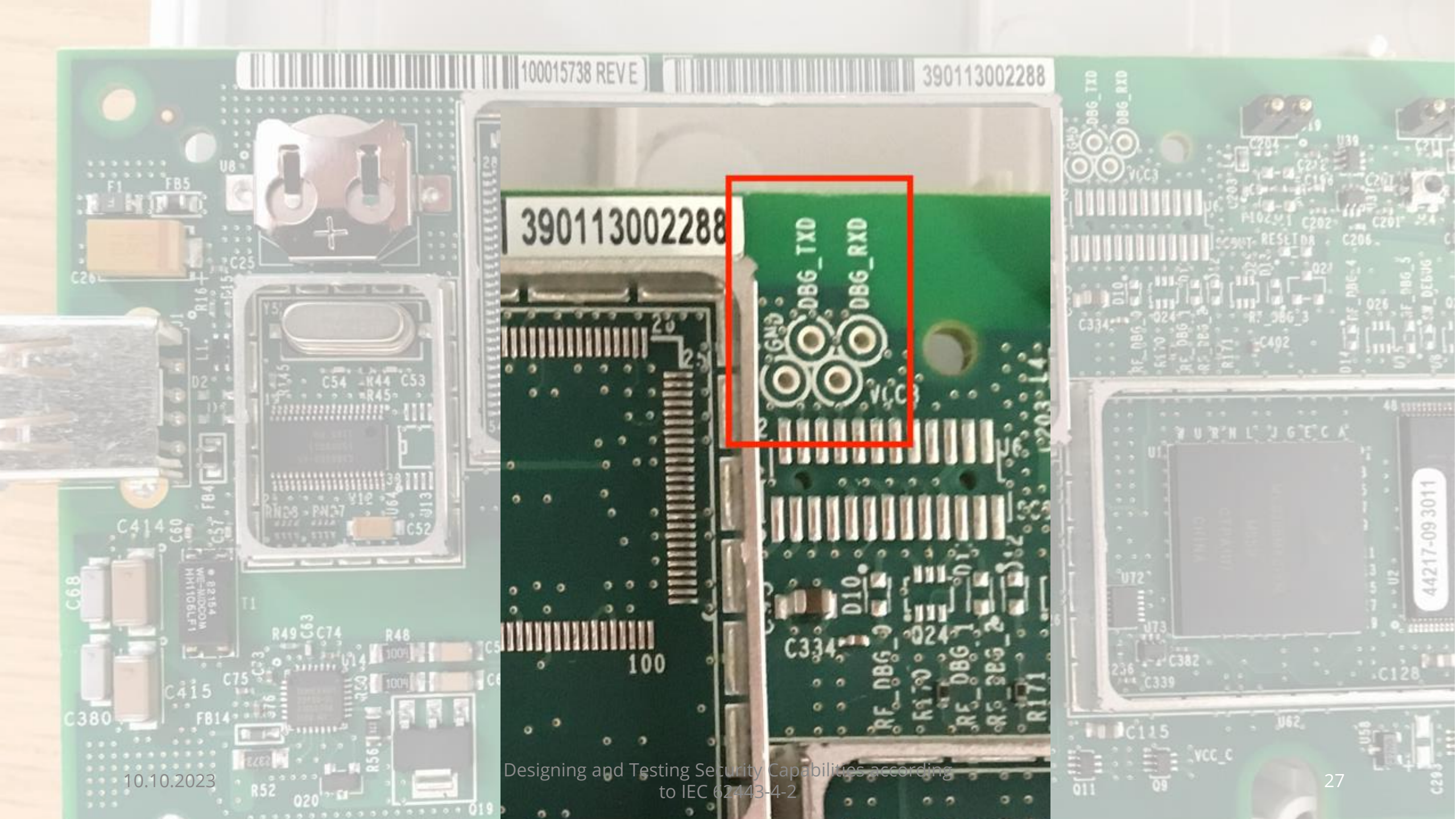
100015738 REV E 390113002288



10.10.2023

Designing and Testing Security Capabilities according to IEC 62443-4-2

26

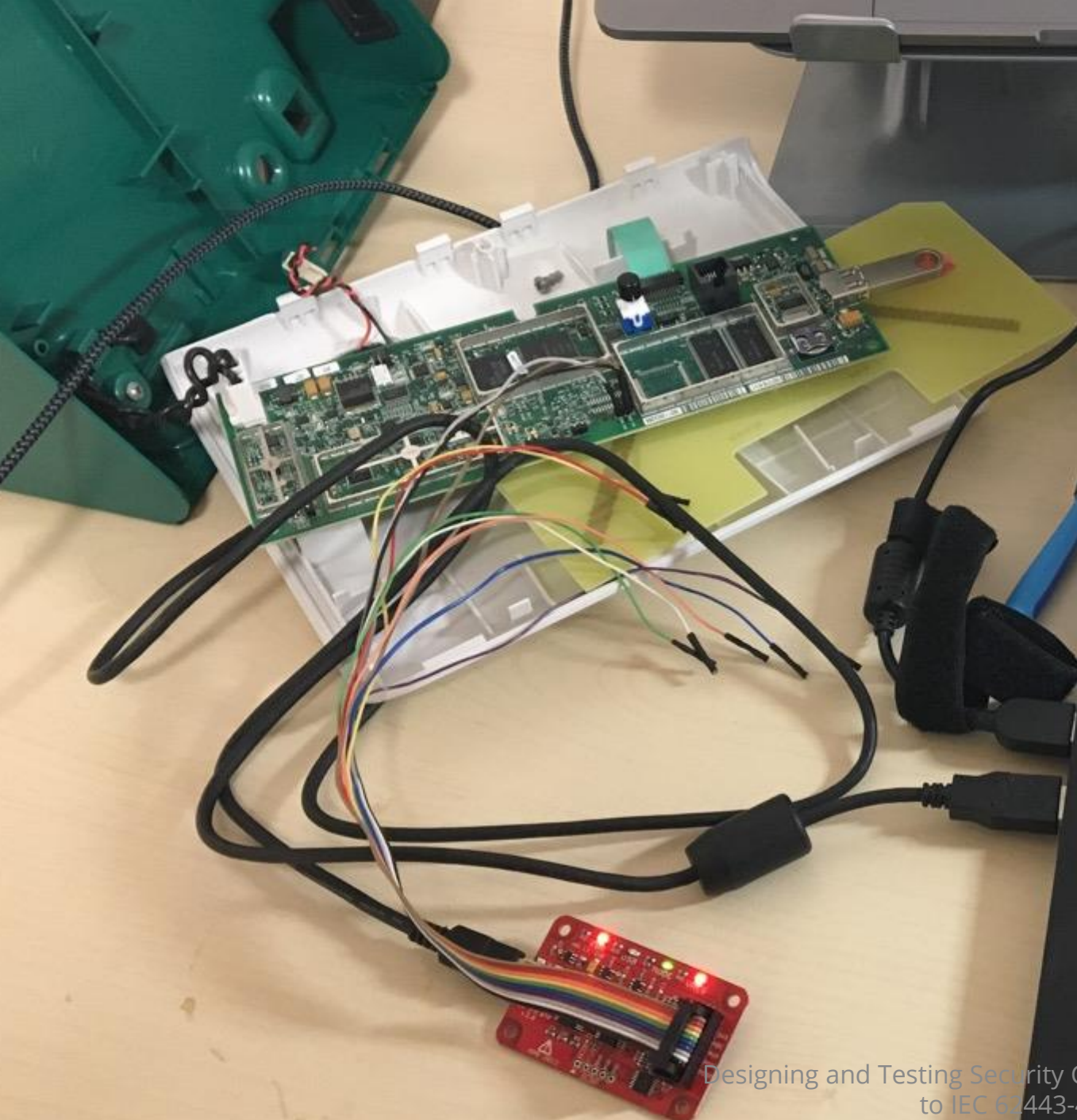


100015738 REVE

390113002288

390113002288

GND
DBG_TXD
DBG_RXD
VCC3



```
root@vml:/vml/vml
operator@(none):~$
operator@(none):~$
operator@(none):~$
operator@(none):~$
operator@(none):~$ id
uid=12(operator) gid=0(root)
operator@(none):~$ ls
devel_install.sh setdev.sh
operator@(none):~$ cd
operator@(none):~$ ls
devel_install.sh setdev.sh
operator@(none):~$ ls -la
drwxr-xr-x  3 root  root
drwxr-xr-x 20 root  root
-rw-r--r--  1 root  root
-rw-r--r--  1 root  root
drwx----- 2 root  root
-r-xr-xr-x  1 root  root
-r-xr-xr-x  1 root  root
-r-xr-xr-x  1 root  root
operator@(none):~$ cd /
operator@(none):/$ ls
apps boot dev home mnt  proc sbin usr  vpd
bin  data  etc  lib  opt  root  tmp  var
operator@(none):/$ id
uid=12(operator) gid=0(root)
operator@(none):/$
```

```
setlog.sh
setlog.sh
0 Oct 11 2011 .
0 Jan 1 00:00 ..
0 Apr 21 2008 .bash_history
52 Apr 24 2008 .bash_profile
0 Oct 11 2011 .ssh
2584 Jul 13 2011 devel_install.sh
443 Jul 13 2011 setdev.sh
267 Jul 13 2011 setlog.sh
```

Designing and Testing Security Capabilities according to IEC 62443-4-2

The hacker's perspective

```
# Version 0.1 - Ashok Iyer (aiyer at sjm dot com)

# Setup the PATH. Don't assume we get a sane one
export PATH=/usr/local/bin:/usr/bin:/bin:/usr/sbin:/sbin

# IP address of the server from which we download the devel package using scp.
SERVER="10.16.155.27"

function download_package()
{
    # Download the devel package and the md5sum.txt file
    echo -e "\n==> Downloading $1 package using wget.\n"

    wget ftp://tantopr:mah1200@10.16.155.27/$2/$1

    if [ "$?" != 0 ]; then
        echo "scp failed..."
        exit 1
    fi
}
```

This violates e.g.

13.3 EDR 2.13 – Use of physical diagnostic and test interfaces

13.3.1 Requirement

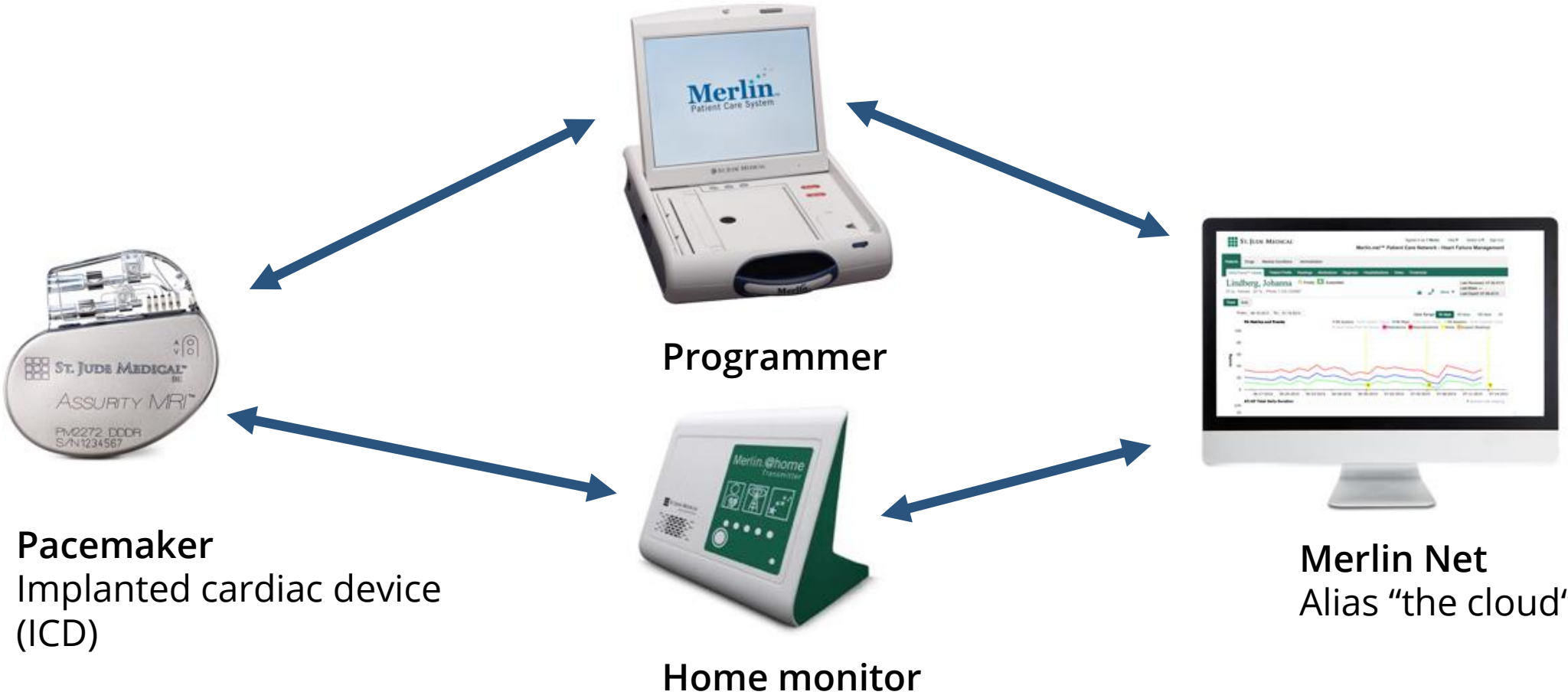
Embedded devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).

5.4 CR 1.2 – Software process and device identification and authentication

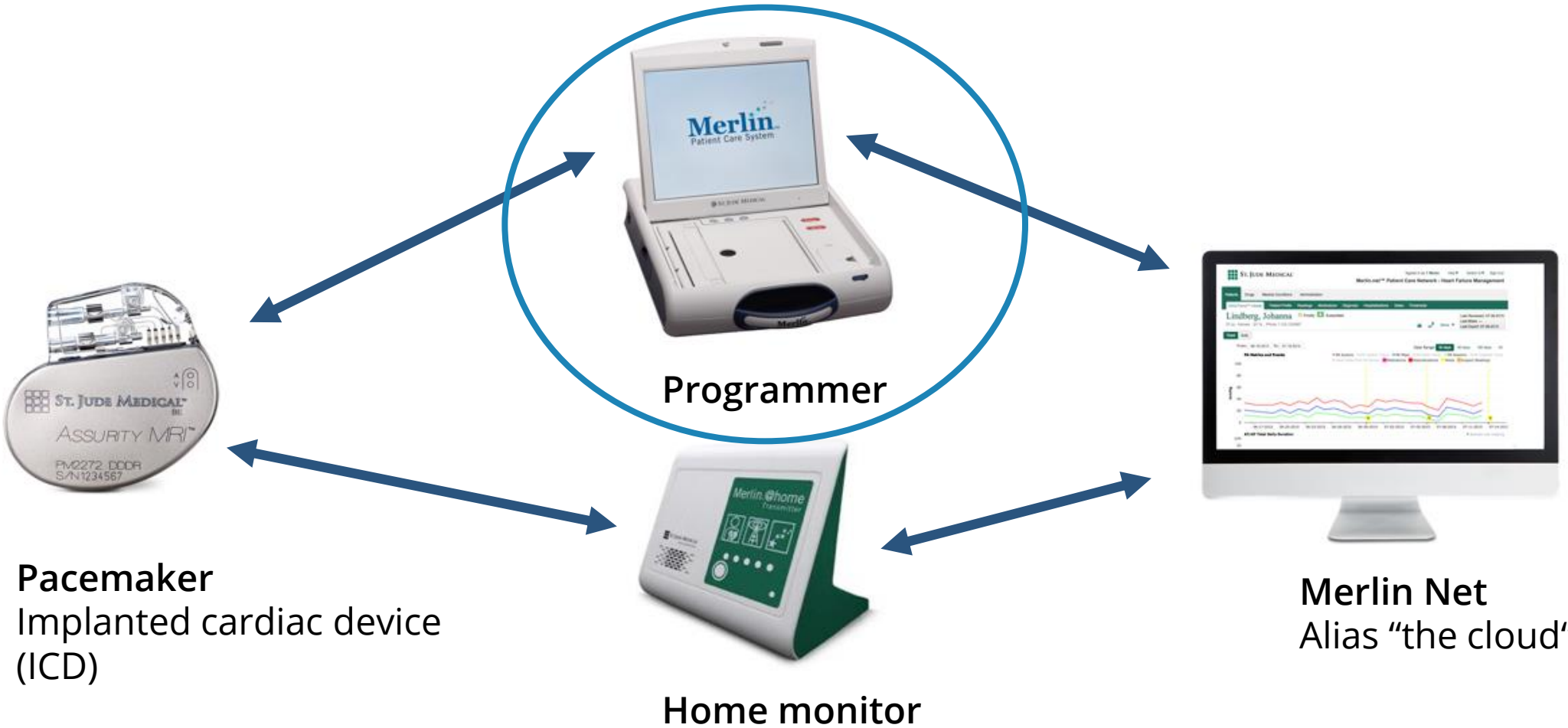
5.4.1 Requirement

Components shall provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to IEC 62443-3-3 SR1.2.




What else to attack?



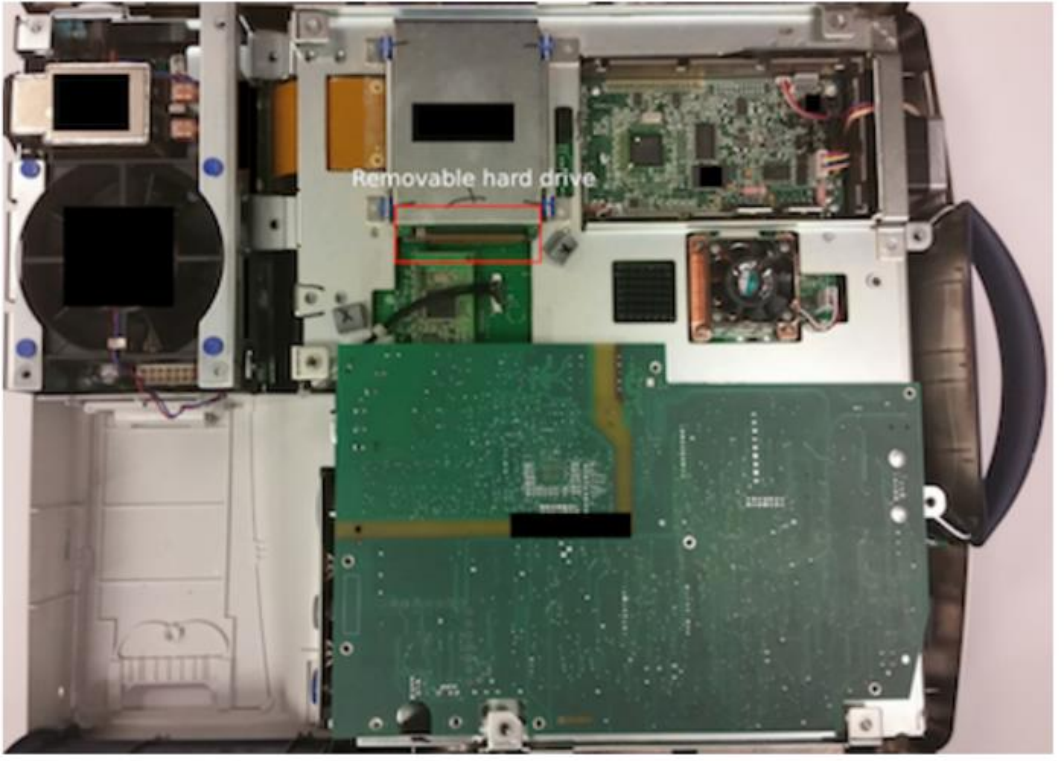
What else to attack?



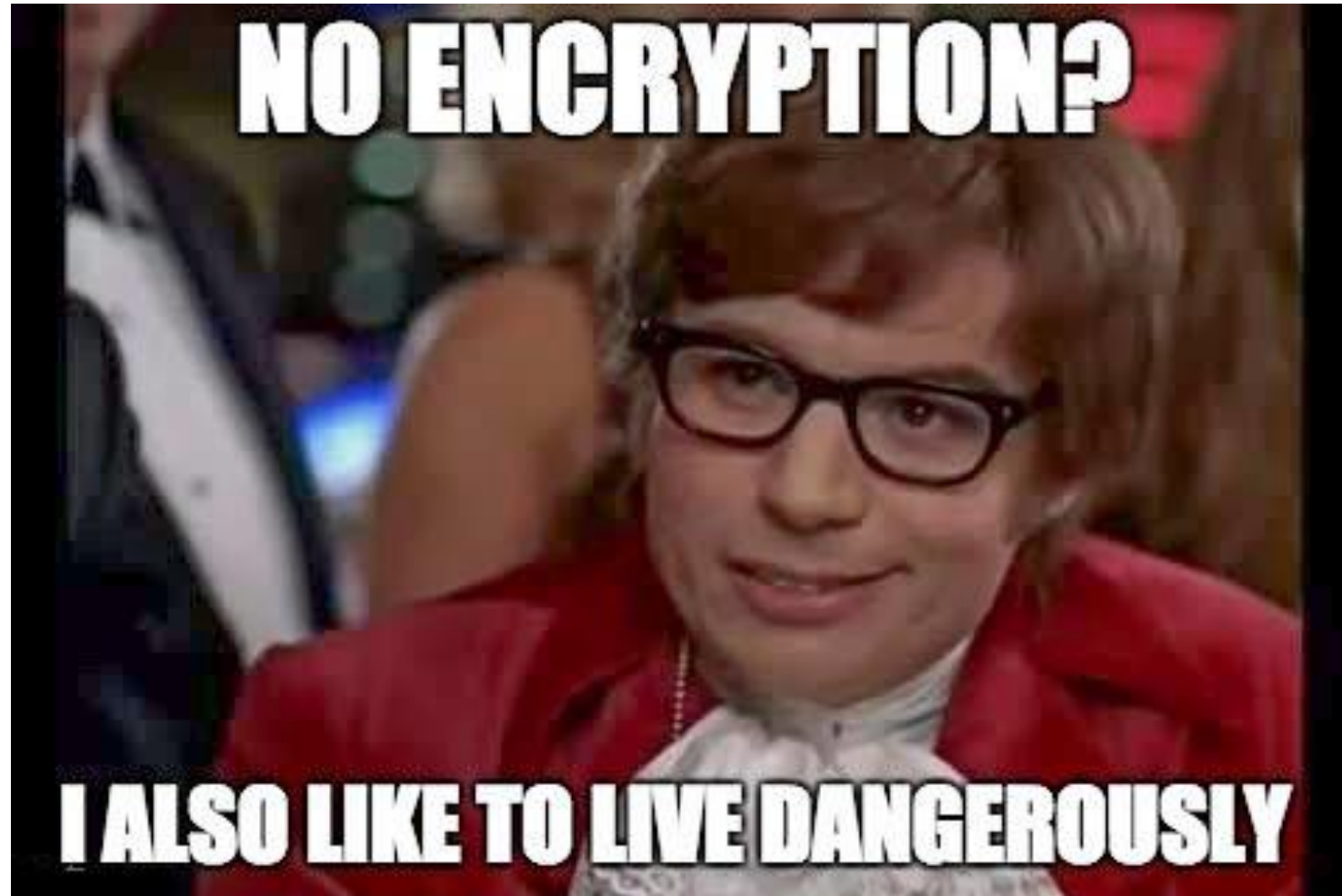
What about the programmer?

	<p>St. Jude Medical 3510 Pacemaker Programmer with Warranty!! Pre-Owned</p> <p>\$1,000.00 or Best Offer +\$67.37 shipping</p>	<p>From United States Customs services and international tracking provided</p>
	<p>ST.Jude Medical Model 3510 programmer System Pre-Owned</p> <p>\$585.00 or Best Offer +\$665.37 shipping</p>	<p>From United States</p>
	<p>St. Jude Medical Pacemaker Programmer Model 3510 with Warranty!! Pre-Owned</p> <p>\$2,200.00 or Best Offer +\$78.29 shipping</p>	<p>From United States Customs services and international tracking provided</p>

Tell us what you think



Removable HDD



Merlin@Home as attack device

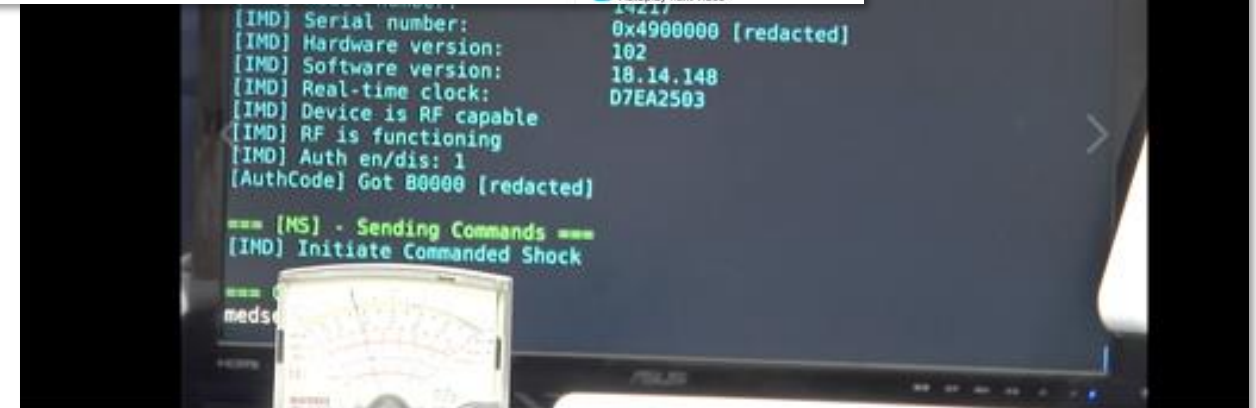
- Emergency shock
- Disable Tachy
- Vibrate
- T-Shock



VIBRATE

More from Muddy Waters Capital LLC

Autoplay next video



EMERGENCY SHOCK

More from Muddy Waters Capital LLC

Autoplay next video

This violates ...

8.5 CR 4.3 – Use of cryptography

8.5.1 Requirement

If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.

6.4 CR 2.2 – Wireless use control

6.4.1 Requirement

If a component supports usage through wireless interfaces it shall provide the capability to integrate into the system that supports usage authorization, monitoring and restrictions according to commonly accepted industry practices.

Which message authentication code (MAC) is used?

- A. No authentication
- B. Proprietary (*Let's build our own „crypto“*)
- C. Hardcoded 24 bit RSA
- D. 56bit DES
- E. 1024bit RSA



Which message authentication code (MAC) is used?

- A. No authentication
- B. Proprietary (*Let's build our own „crypto“*)
- C. **Hardcoded 24 bit RSA**
- D. 56bit DES
- E. 1024bit RSA



Which message authentication code (MAC) is used?

- A. No authentication
- B. Proprietary (*Let's build our own „crypto“*)
- C. **Hardcoded 24 bit RSA**
- D. 56bit DES
- E. 1024bit RSA



Other crypto mistakes?

- A. “homebrewed” cryptographic algorithm
- B. Hardcoded “Universal Key” as backdoor
- C. one 32-bit RSA public key for all devices
- D. Truncate calculated keys because of memory



Other crypto mistakes?

- A.** “homebrewed” cryptographic algorithm
- B.** Hardcoded “Universal Key” as backdoor
- C.** one 32-bit RSA public key for all devices
- D.** Truncate calculated keys because of memory



Technical Summary

- Critical vulnerabilities with potentially lethal impact discovered
- Unauthorized user could remotely access a patients implanted cardiac device over wireless interface
- Very easy debug access to Merlin@home device using an insecure hardware interface
- Insecure storage of source code on the home device/programmer
- Simple replay attacks for battery depletion
- Reprogramming of the pacemaker using wireless
- Static keys everywhere



This code is not violating a requirement – but highly insecure

- This is client side code!

```
bool flag = true;
Authentication.Logger.DebugFormatFast("{0}.Authenticate: calling this.UserProvider.GetUserCredentials(\"{1}\")", base.GetType().Name, user);
IUserData userCredentials = this.UserProvider.GetUserCredentials(user);
Authentication.Logger.DebugFormatFast("{0}.Authenticate: done this.UserProvider.GetUserCredentials(\"{1}\")", base.GetType().Name, user);
if (userCredentials != null && userCredentials.Password != null)
{
    if (password == null)
    {
        password = string.Empty;
    }
    if (Hash.PasswordHash(userCredentials.UserName, userCredentials.Password, userCredentials.CustomerNumber, false).Equals(Hash.PasswordHash(user, password, customerNumber, false)))
    {
        flag = false;
    }
}
else if (userCredentials != null && string.IsNullOrEmpty(userCredentials.Password) && string.IsNullOrEmpty(password))
{
    return this.accountManagementHelper.CreateGenericIdentity(userCredentials.UserName);
}
if (flag)
{
    string message = "User or password is incorrect.";
    Authentication.Logger.Warn(new InvalidCredentialException(message));
}
```

Draft: 62443-6-2

Security evaluation methodology for IEC 62443-4-2

- Repeatabile and reproducible evaluation results for IACS 168 components against IEC 62443-4-2 requirements

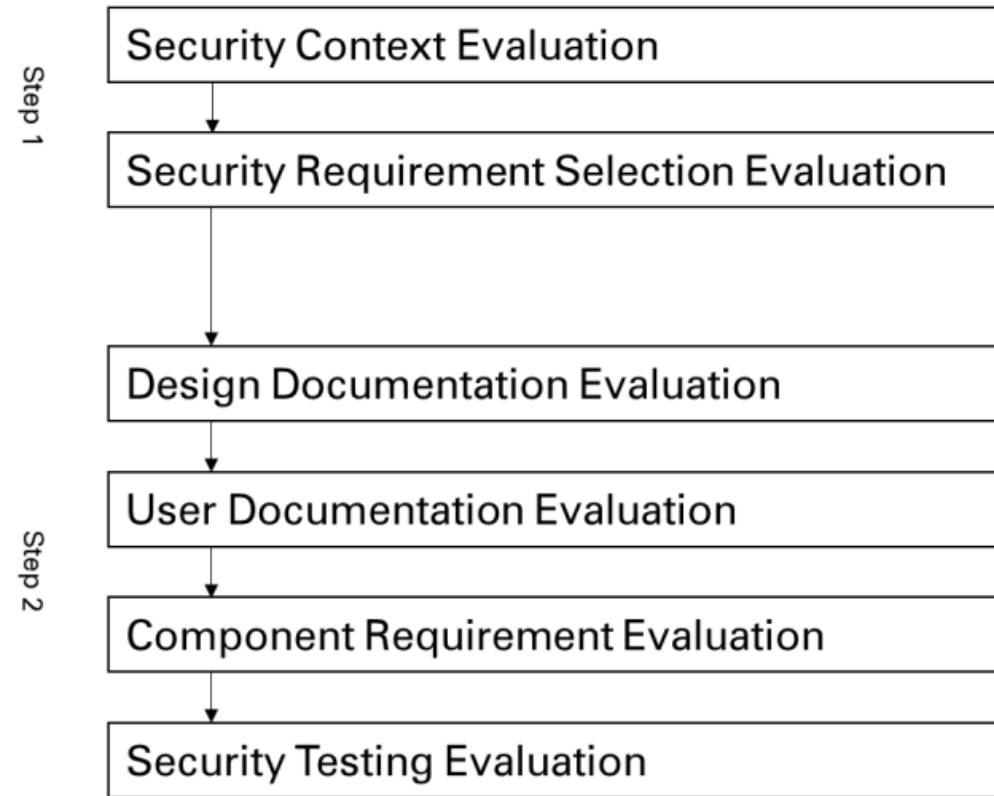


Figure 4 Evaluation process

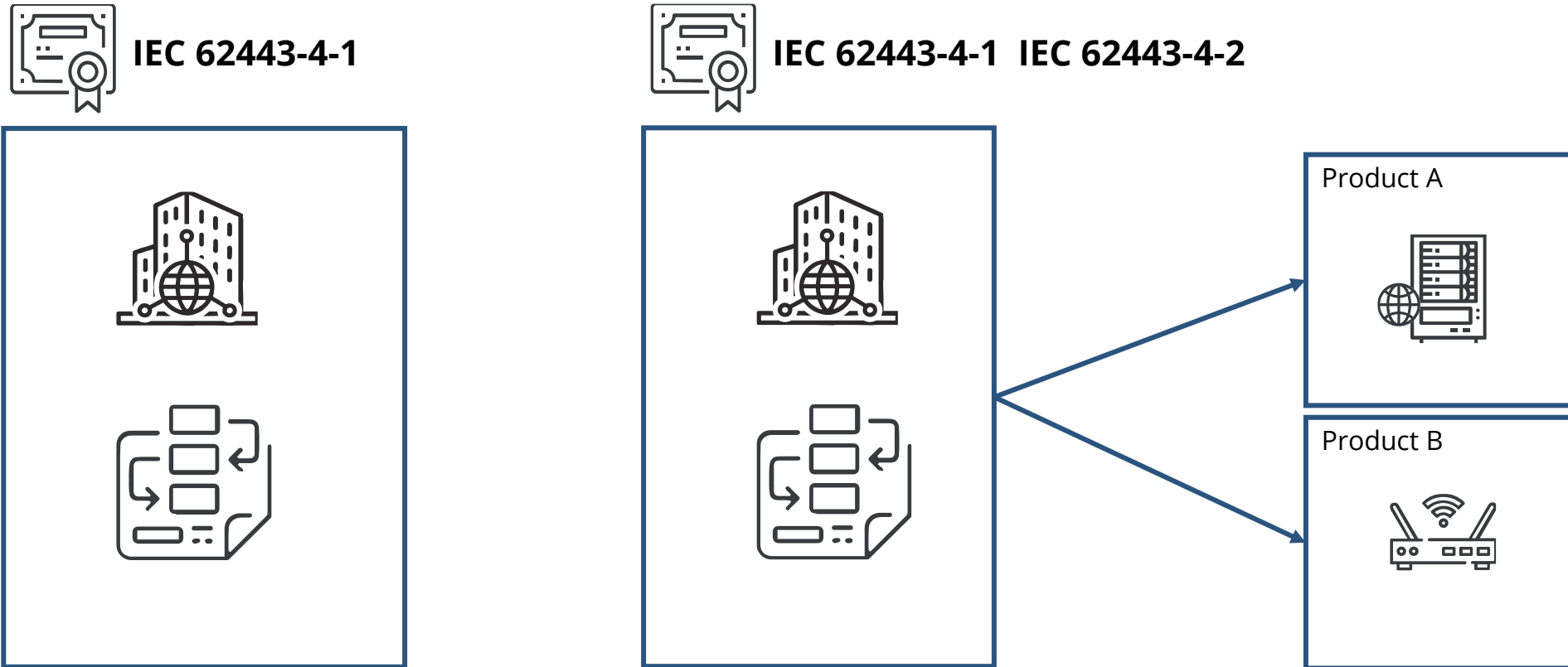
Beginner's Toolbox

There are some tools that are in common use and provide an easy start to cover the basics

- **nmap**: The most used port scanner. It is mainly used to identify the open ports on a system from the outside and to compare them with the (hopefully existing) list of necessary ports
- **Nessus**: The most widely used vulnerability scanner. Mainly finds known misconfigurations and missing updates in standard components (mainly the platform: OS, DB, web server, standard services). Can also be used to evaluate the hardening of a system according to a certain standard, e.g. CIS benchmarks. Can also test web applications, but with mixed quality.
- **OpenVAS**: Open source alternative to Nessus. Our experience with it is worse than with Nessus.
- **Sslyze**: Console tool to check server-side TLS configurations
- **qsslcaudit**: Console tool to check client-side TLS configurations
- **Burp Proxy**: Very good tool for manual, but also automatic testing of web applications.
- **Firmware Analysis and Comparison Tool (FACT)**: Automatic analysis of firmware images

IEC 62443 Product Certification

Product certification does not work without process certification



How to get started

1. Follow the practices defined in the IEC 62443-4-1, especially create the artefacts security context, threat model and guidelines
2. Ensure to have all interfaces listed
3. Select the appropriate requirements from the IEC 62443-4-2 based on risks
4. Implement and verify the requirements

IEC 62443 Summary

Our IEC 62443 summary contains terms, definitions and basics of IEC 62443. Use our expertise to efficiently upgrade your company in terms of security.



Download your IEC 62443 Poster

<https://limesecurity.com/en/iec-62443/>