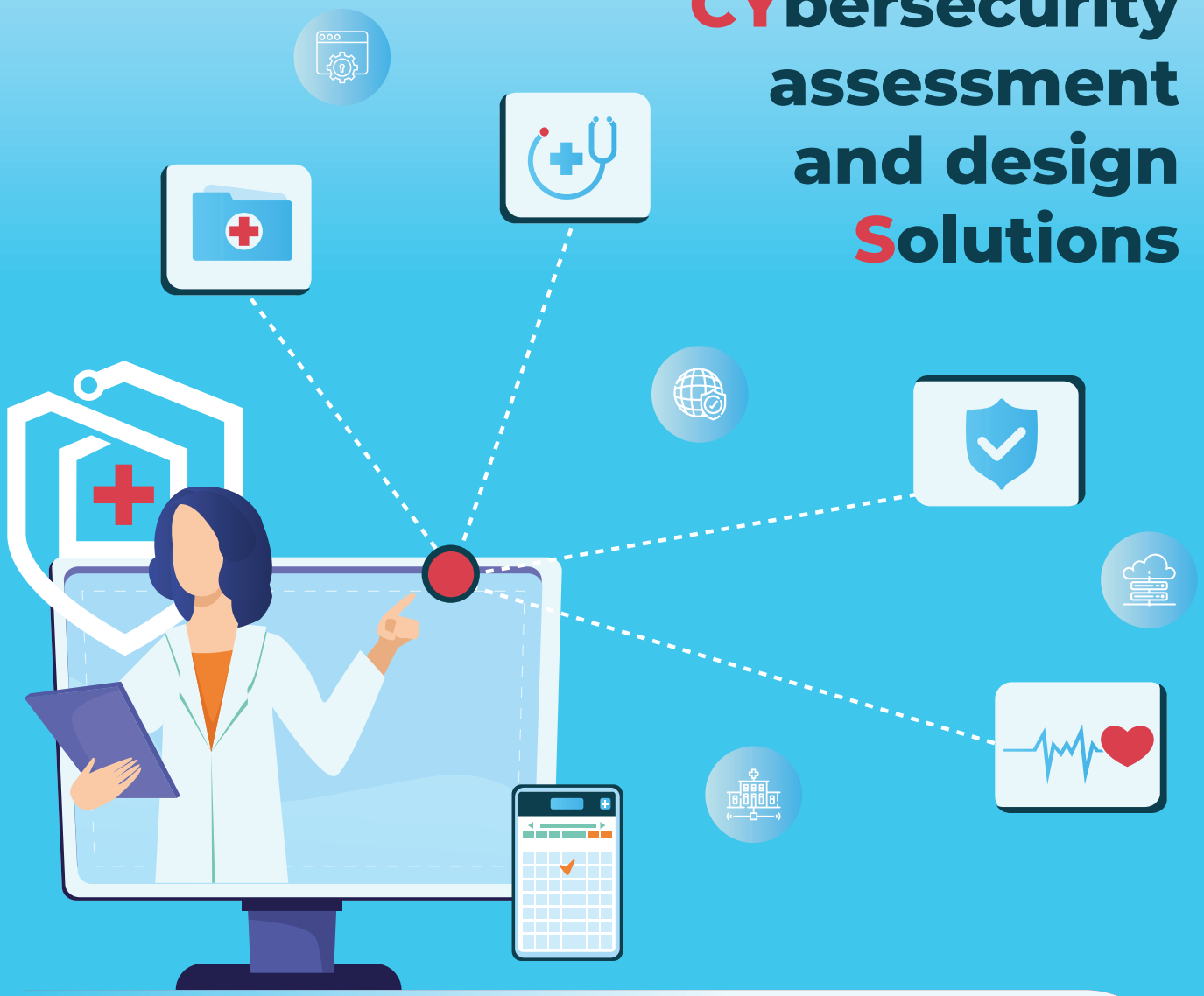
NEMECYS

New Medical Cybersecurity and design Solutions

NEw MEdical CYbersecurity assessment and design Solutions



NEMECYS Toolbox:
Firmware fuzzing tool

Developed by SINTEF

The purpose of the NEMECYS fuzzing tool is to improve the cybersecurity of connected medical devices by enhancing firmware vulnerability detection and making the security assessment process more efficient. Built on **Fuzzware**, the tool utilizes **firmware re-hosting** to emulate the hardware environment of the target firmware, allowing for in-depth security testing without requiring a complete hardware setup as a test bed.

By running firmware in an emulated environment, the tool can provide deep insight into how embedded systems respond to unexpected or malformed inputs. This helps identify critical vulnerabilities that could compromise device security, patient safety, or data integrity. The tool automates the fuzzing process, thereby improving the speed and effectiveness of security testing while reducing manual effort.

One of the key benefits of the fuzzing tool is its ability to detect vulnerabilities early in the development lifecycle, helping manufacturers **proactively strengthen their firmware against potential cyber threats**. Given the critical nature of connected medical devices, even minor security flaws can have severe consequences, so efficient detection of flaws and vulnerabilities is important to maintain and improve overall device security.

Ultimately, our goal is to **empower medical device manufacturers** with cutting-edge security testing capabilities, making it easier to detect and remediate vulnerabilities early in the development lifecycle. With an emphasis on automation and repeatability, our firmware fuzzing tool represents an important step forward in securing the next generation of embedded medical devices.

Technical Inquiries for the Tool

If you are interested in learning more about the tool, its capabilities, or technical details, please contact **egil.wille@sintef.no**

Scan to access the tool

www.nemecys.eu | **@NEMECYS_eu** | **nemecys-horizon-eu-project**

SINTEF · mode · IBM · ATC Athens Technology Center · ribera · I.R.C.C.S. Ospedale San Raffaele, Gruppo San Donato · Med&Lab · ICE Information Catalyst · University of Southampton · pd neurotechnology medical solutions · DEBIOTECH

Co-funded by the European Union

The NEMECYS project is co-funded by the European Union under grant agreement ID 101094323, by UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee grant numbers 10065802, 10050933 and 10061304, and by the Swiss State Secretariat for Education, Research and Innovation (SERI). The information and views set out in this publication are those of the author(s) only and do not necessarily reflect hose of the European Union, HADEA, UKRI or SERI. Neither the European Union nor the granting authorities can be held responsible for them.