# Security Team minutes

Not all discussions are / have been minuted but this is a page that is available to keep some public notes.

**Minutes September 19, 2019**

**Participants:**

- Erika Anden
- Dirk Leopold (Itemis)
- Till Fischer (Itemis)
- Bevan Watkiss (Irdeto)
- Gunnar Andersson (GENIVI)
- Philippe Robin (GENIVI)
- Steve Crumb
- Ziv Levi (Arilou) (was not introduced. Participated part of the time)

Minutes

Dirk: I think the primary motivation for participating (in the Security Evaluation Framework project) is that the ISO/SAE 21434 will basically make it mandatory.

...Is it truly mandatory?

Erika: To my understanding it is at first optional to follow this, but over time this might change.

Dirk: Yes, I think it becomes a kind of expected behavior. If some companies do this analysis, others will be expected to also do it (to be protected in case of a problem). Also, (*things like this)* tends to enter the value chain, so OEMs require it from suppliers, etc.

There is a flowchart from 21434 that is very useful and roughly the basis. The ISO spec content should not be reproduced to parties that have not licensed a copy of it. The flow chart is useful for discussion but should be avoided for a future publication of the (sub)project charter.

We worked to improve the draft charter/description of this subproject (limited access to active group participants for the moment). Results are shown on the page.

**Minutes September 05, 2019**

**Participants:**

- Bastien Kruck (Itemis)
- Mike Nunnery
- Bevan Watkiss (Irdeto)
- Bastian Kruck (Itemis)
- Till Fischer (Itemis)
- Gunnar Andersson (GENIVI)
- Philippe Robin (GENIVI)
- Steve Crumb (part time)

**1. Security Evaluation Framework**

Discussed and worked to improve the Security Evaluation Framework page. (This draft is accessible for Security Team only - ask for access if you want to participant). This took the majority of the meeting time today. Results are on the page.

**2. Automat and other related security frameworks as identified in Cloud & Connected Services project**

Info about the review we did on the Automat-developed security framework

Big Data and privacy - if interested, make sure to read the link provided. http://www.bdva.eu/sites/default/files/BDVA%20DataSharingSpace%20PositionPaper_April2019_V1.pdf

Other related work: SAREF - work on data ontologies to produce common standard.
https://www.etsi.org/newsroom/press-releases/1620-2019-06-etsi-releases-3-new-ontology-specifications-for-smart-cities-industry-4-0-and-smart-agriculture

Also W3C Web of Things. https://www.w3.org/WoT/

Finally comparison of ISO 27001-vs-NIST .
ISO 27001 & 27002 on security and ISO 27701 on data privacy (former ISO 27752) which is a privacy extension of ISO 27001

Please review: US NIST cybersecurity work that addresses the security according to the lifecycle, i.e. the possible threats and countermeasures are structured according to the various stages of the lifecycle of the product (identify, protect, detect, respond, recover) – Look for instance at https://blog.compliancecouncil.com.au/blog/iso-27001-vs-nist-cybersecurity-framework
*TBC other links for the actual NIST specifications?*

**AUTOMAT**:

The interesting feature of the Automat cybersecurity work is that it relies on existing standards (at the time of the project execution timeline).

Action: Review Petar's summary presentation (and also the original Automat security specification). Both are linked from here.

Antonio works in a WG (unknown which one?) on meta-architecture (for vehicle data)

Antonio mentions also the work done Industrial Internet Consortium (IOC) on IOT 4.0 / IIOT, look at: https://www.iiconsortium.org/vertical-markets/transportation.htm

Conclusion:
The work done in automat on cybersecurity is good and relates to a big data architecture, We recommend the GENIVI security team to review it and amend it w.r.t. US NIST work and extract possibly use cases to benchmark the MoRa tool.

**Minutes August 22, 2019**

**MoRA tooling**

- Dirk ask for a new recurring invitation and earlier warning for meetings.
  Yes, the new invitation series should come starting from next meeting.
- Offer to license temporarily for GENIVI team
- If we start analyzing it would be possible to share the results
  - Idea: to share the threat catalog
- Gunnar: How is it shared in practice?
- Dirk: Can be stored in version control, such as git.
- Steve: Could we apply this to for example a communication protocol like SOME/IP?
- Dirk: It would be mapped onto the item types that the tool uses: Components, Connections, Dataflows and Functions

- Dirk: Is there a reference architecture we could analyze?
- Gunnar: We have the infotainment-focused compliance specification, but we're more interested in the newer projects. The Vehicle Data reference architecture for vehicle data
- Dirk: We are open to any proposals from members
- Mike: Are there possibilities to rate your system at the end, get a "scoring" of the security level?
- Dirk: A group like GENIVI could agree on some common standards and baselines. But the acceptable security/risk/etc depend a lot on projects, industry, company risk exposure, etc.
- Dirk: ...But theoretically a "GENIVI reference framework" would be possible.
- Gunnar: I want to point out that it needs to start by looking at what already exists, and focus on filling the gaps.

If companies help us define the problem then the incentive for them is that their technology may be part of the solutions

- Dirk: 21434 will require documentation to prove that security analysis has been done. It would be better to have documentation coming out of tool support.

Opportunities for collaborators:

- Learn how to do security analysis (using MoRA methodology as the working method during this learning opportunity)
- Sharing of experience how to actually implement the requirements of 21434
- Collaboratively develop a shared "reference" security evaluation framework.
  - Note: the Safety evaluation frameworks should give some guidance about good processes here

Ideas for new topics / subprojects:

- Analysis and testing
- Surveys
- Whitepapers, MRDs
- Security contributions into current GENIVI projects

Other advantages of participating:

- We have a lot of opportunity to give participating members information and unique opportunities about Events, speaking opportunities, etc.

Marketing of course supporting all of these activities.

Mike: I'd like to see a shared description of this analysis tooling and what we are aiming for in the reference evaluation framework.