Artemis Compliant Security

by

Balázs Berkes, Josef Noll

presented at

nSHIELD Review Meeting

October 2012, Rome

nSHIELD system security design

- Top-down approach:
  - Collect security features intended for the system
  - Specify and develop secure environment
  - Derive requirements for embedded devices
- Bottom-up approach:
  - Collect use cases and security requirements of embedded devices and applications (→scenarios)
  - Specify common security functionality and design the environment around that
  - Specify and develop system enveloping various embedded devices
- Evaluate novel software alternatives

nSHIELD

nSHIELD integration levels

Logical categorization of Embedded System Devices (ESDs) in nSHIELD system:

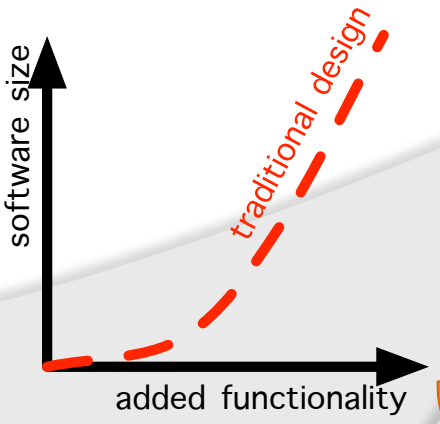
- Legacy Embedded System Device (L-ESD)
  - Will not utilize nSHIELD security functionality directly
- nSHIELD Embedded System Device (nS-ESD)
  - Support minimal SPD capabilities, without utilizing Overlay
- nSHIELD Embedded System Device Gateway (nS-ESD-GW)
  - Gateway for bridging legacy devices
- nSHIELD SPD Embedded System Device (nS-SPD-ESD)
  - fully nSHIELD-enabled device utilizing all nSHIELD security services

(based on nSHIELD WP2 T2.3 Architectural Design)

nSHIELD

Main challenges

- Assessment of **security, privacy,** and **dependability** status via pre-defined sets of **metrics** values
- nSHIELD Semantic Overlay layer:
  - dynamic matching of *available* SPD metrics to *required* SPD metrics via composition (quantitative solutions still under evaluation)
- Certifiable software
  - Autonomous operation
  - Certification (UAV), 50US$/line



nSHIELD

Way ahead – Artemis standards

- Measurable security through metrics
  - Reference architecture for measurable security through Artemis tools?
- Semantic Overlay and Implementation
  - Guidelines for industrial awareness of security?

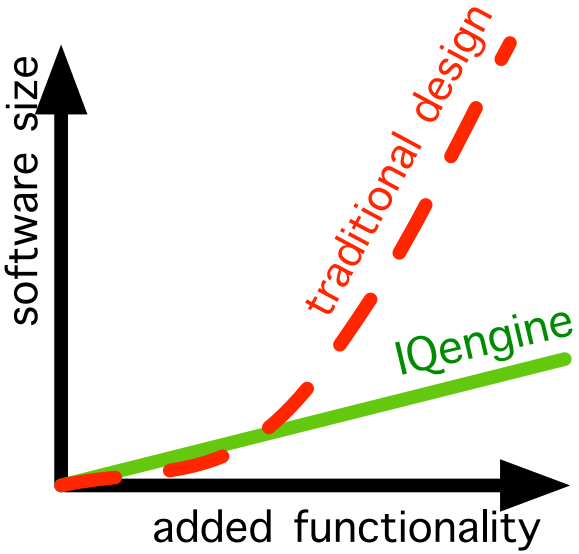
Artemis Contribution?

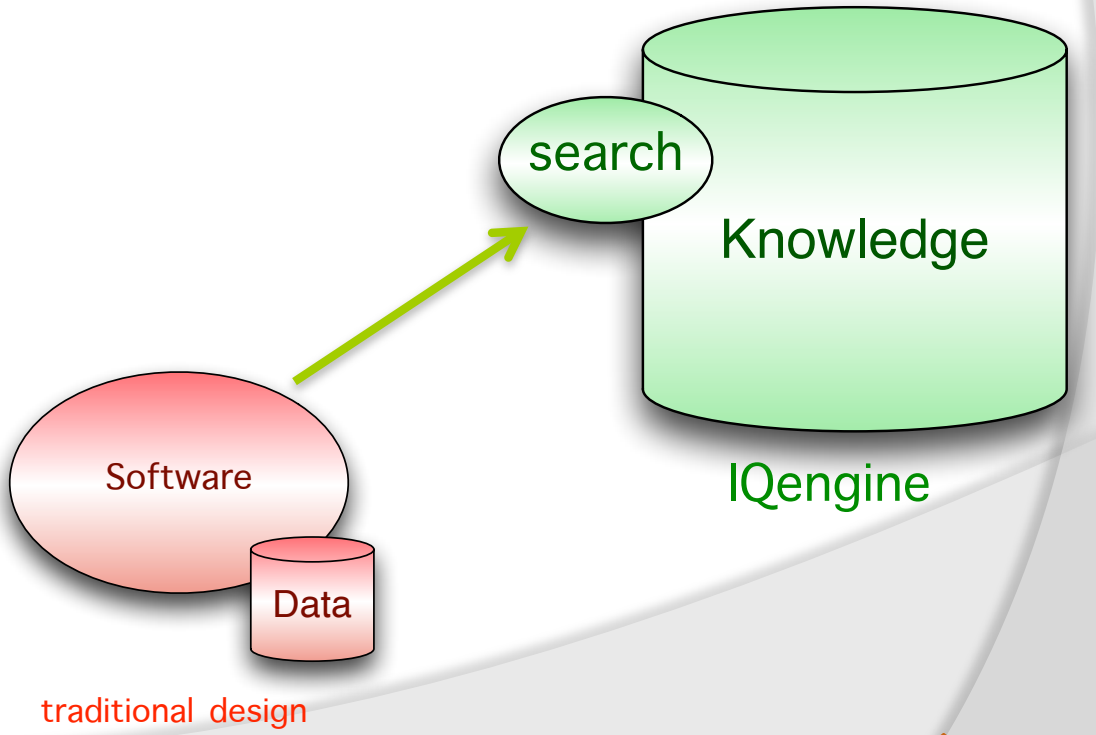
- *Targeting multiple goals laid out in SRA 2012 (ARTEMIS-GB-2011-D.33 – Annex 2, chapter 3.6):*
  - *ES support for critical applications*
  - *High availability of operations and systems (i.e., uninterrupted services in the presence of threats, power failures, accidents and natural disasters).*
  - *Exploiting new opportunities for reconfigurable ESs and sensor networks for variable requirements of ad-hoc security coverage.*
  - *Creating standards, devices and protocols effective to the homeland security market.*
  - *Increase the competitiveness of the European ES industry through methods that will allow a more effective process for the certification of ES security features.*

nSHIELD

Way ahead – novel SW concepts

- Semantic System of System modelling
  - nSHIELD: Overlay and Implementation
- Evaluate novel software concept: IQengine



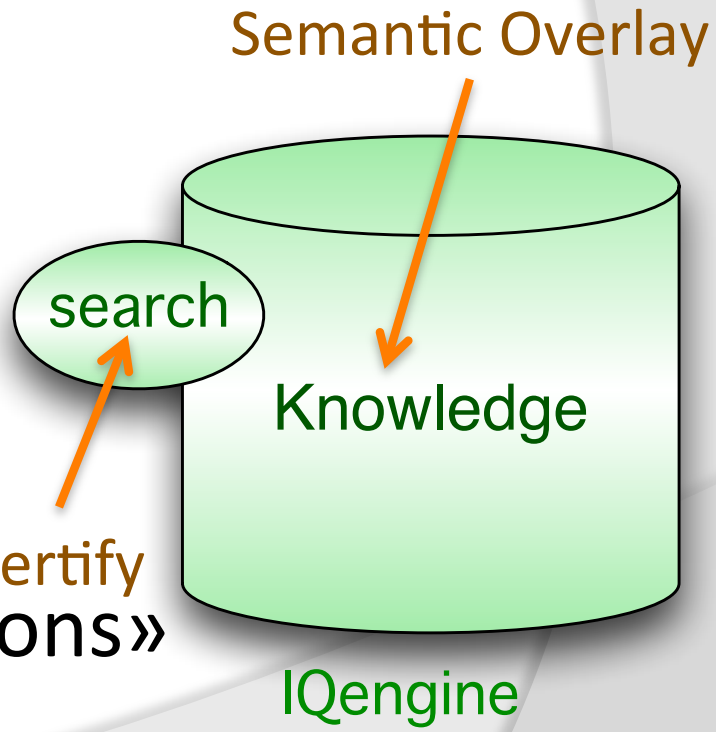


nSHIELD

nSHIELD challenge:

A European civil UAV

- Artemis compliant security for civil UAV
- New nSHIELD partner: Alfatroll
- Evaluate challenges
  - Linear independent processes
  - Consistency of Knowledge base
  - Semantic modeling
- Towards «autonomous operations»



nSHIELD

Conclusions

- Help from JU Artemis on Measurable Security
- Guidelines for industrial awareness of security?
- New SW solution for autonomous operation(?)