Satellite communication and cybersecurity

Juha-Matti Liukkonen

Director, Space & Robotics

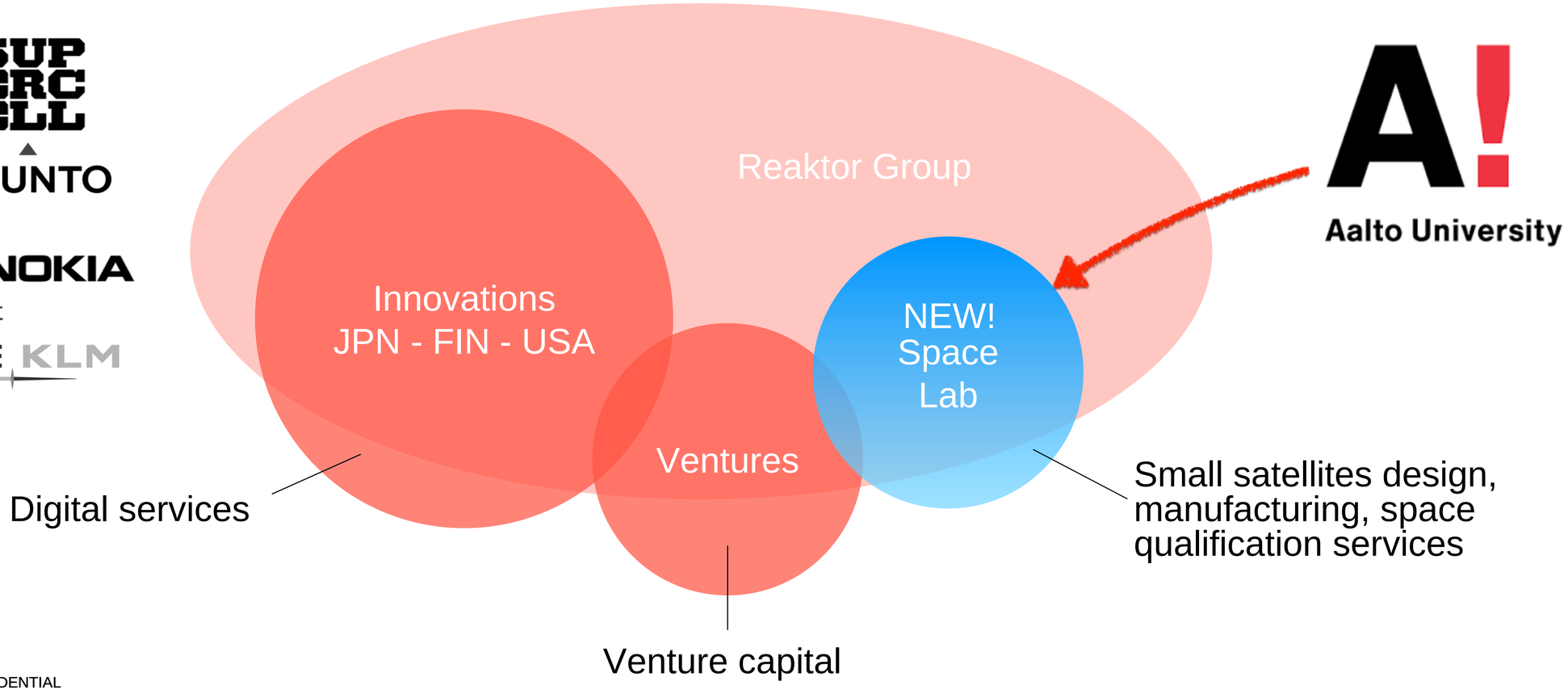
Reaktor

About Reaktor

Established in 2000, revenue 2015 €43M, operating in Tokyo - Helsinki - New York, 350+ specialists.

We build exceptional digital services and help our customers to grow their business.

HBO
SUPERCELL
NASDAQ
SUUNTO
FINNAIR
AIRBUS DEFENCE & SPACE
NOKIA
AIRFRANCE KLM
MICHAEL KORS
Rakuten



SATCOM AND CYBERSECURITY

Reaktor Space Lab

Reaktor Space Lab is a New Space start-up, offering **small satellite design, manufacturing** and **space qualification services**.

The Space Lab team comes from the Aalto University satellite lab where they have already built and space qualified the Aalto-1 and Aalto-2 cubesats, and are now working on a 3rd generation, reusable nanosatellite platform.

Space Lab has also built a fully automated ground station and cloud based C&C solution perfectly suited for cost sensitive small satellite IoT applications.

Space Lab can leverage the 350 seasoned software professionals of Reaktor Innovations in building integrated end-to-end business solutions with cost-efficient space elements.

Together, we provide turn-key small satellite missions to LEO and beyond.

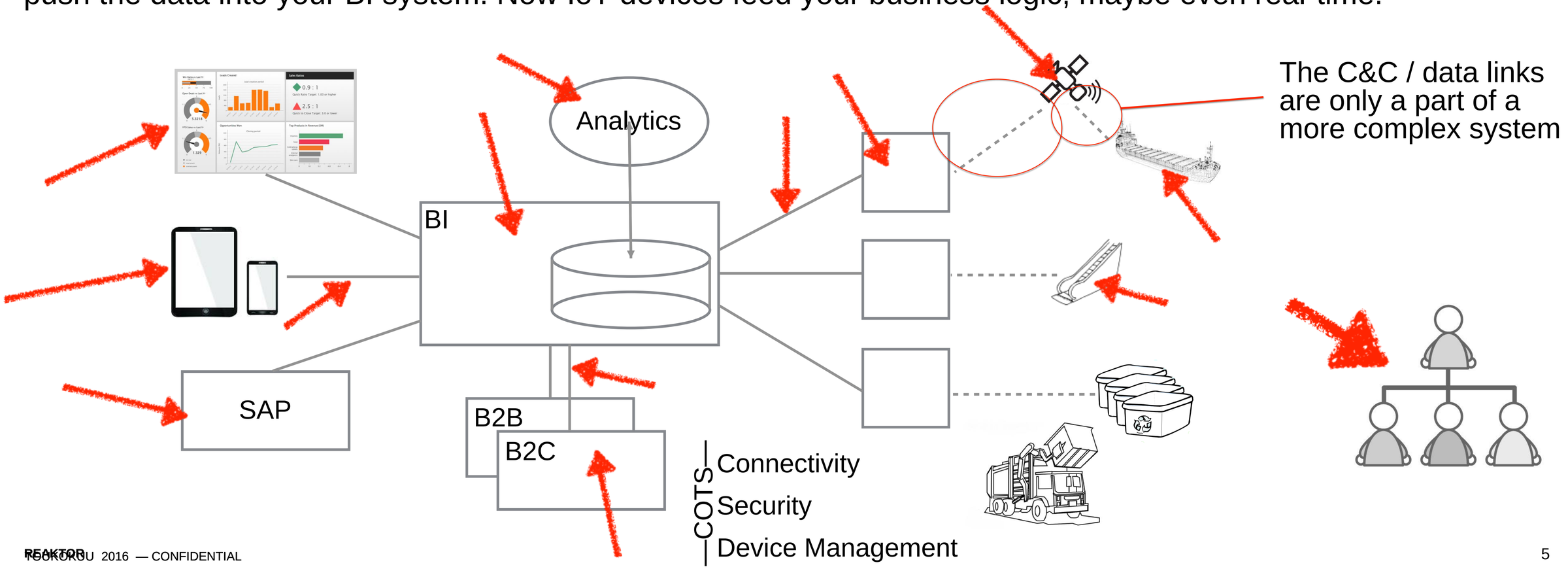
Reaktor Space
May 2016

Satellite communication link threats

- Ground Station - satellite link
  - Denial of C&C Service - e.g. physical damage to GS or antennas
  - Falsifying of C&C traffic
  - Unauthorized C&C access
  - Unauthorized access to data traffic
  - Falsifying of data traffic
  - Denial of data Service
- Basic protections: intrusion & fault detection; multiple ground stations; digital signatures; replay attack prevention; data encryption

Field assets produce business relevant data

IoT enables your business to be based on data from your field assets - be it trash cans, elevators, ships or satellites. You need to install sensors, provide connectivity & security termination and device management, and push the data into your BI system. Now IoT devices feed your business logic, maybe even real-time.



Basic tools for cybersecurity

- Threat analysis -> conscious decisions of trade-offs
- A great modeling tool: attack trees (Bruce Schneier, Counterpane)
  - goals = root nodes
  - attacks = leaf nodes
  - classify leafs: (Im)Possible, (No) Special Equipment, € Cost
  - attacker likely to choose P+NSE+lowest path cost attack
- Build security in from design: security specialists as team members

Reaktor Space & High Security

- High Security project teams with security clearances
- Over 100 engineers trained in cybersecurity
- No High Security for Space offering yet - is there need for it?

Director, Space & Robotics

Juha-Matti Liukkonen
juha-matti.liukkonen@reaktor.com
+358 40 5280142