ACADEMIC INSIGHTS,
INDUSTRIAL IMPACT:

THE FUTURE OF IOT SECURITY TESTING

MAY 15, GHENT

KU LEUVEN

VUB

Agenda

13.30h: Welcome coffee

14h00: From Research to Industry:

Innovating Software Security and Privacy (J. Lapon)

14h20: A Deep Dive into Security Vulnerabilities and

Proprietary Protocols: a case study (V. Goeman)

14h40: Security Testing for Compliance: Meeting Standards,
Reducing Risk (V. Naessens)

15h00: Co-assuring Security and Safety during Software
Development (J. Vankeirsbilck)

15h20: Embedded Security Testing and Automation (C. De Roover)

15h40: Coffee break

16h10: Testimonials from Industry:

- Bridging IT & OT Security Frameworks: Ensuring Compliance in Industrial Environments (Vincotte – S. Van Hauwaert)
- LLMs in security -- Fight fire with fire. (Aikido – R. Delrue)
- The pitfalls of Security Testing (Secudea – D. Sarazyn)

16h40: Panel - Emerging Security Challenges in Industry

17h10-19h30: Networking


From Research to Industry:
Innovating Software Security and
Privacy

From Research to Industry - Innovating Software Security and Privacy

Academic Research, Education, …

Building Products, services, …

From Research to Industry - Innovating Software Security and Privacy

Academic Research, Education, …

Building Products, services, …

› Threat modelling, program verification and testing, …
› Authentication, Identity Management, Authorization …
› System and Network Security
› Cryptography, hardware support …

From Research to Industry - Innovating Software Security and Privacy

Academic Research, Education, …

Building Products, services, …

› Track 1: Secure Applications
› Track 2: Security Services
› Track 3: System and Infrastructure Security
› Track 4: Security building blocks and Hardware

Cyber Security Vlaanderen

From Research to Industry - Innovating Software Security and Privacy

Academic Research, Education, …

Building Products, services, …

› Novel systems and services
› Transforming existing systems

From Research to Industry - Innovating Software Security and Privacy

Academic Research, Education, …

Building Products, services, …

› Specific security requirements
› Evolving threat surface
› Increasing complexity of cyberattacks

From Research to Industry - Innovating Software Security and Privacy

Academic Research, Education, ...

Applied Research

Building Products, services, ...

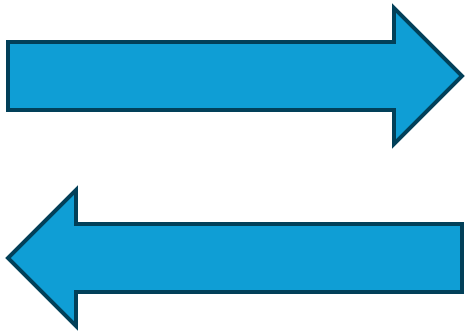
Scalability *Security*

Manageability

Novelty

Energy

Privacy



Security

Privacy Energy

Scalability

Cost-efficiency

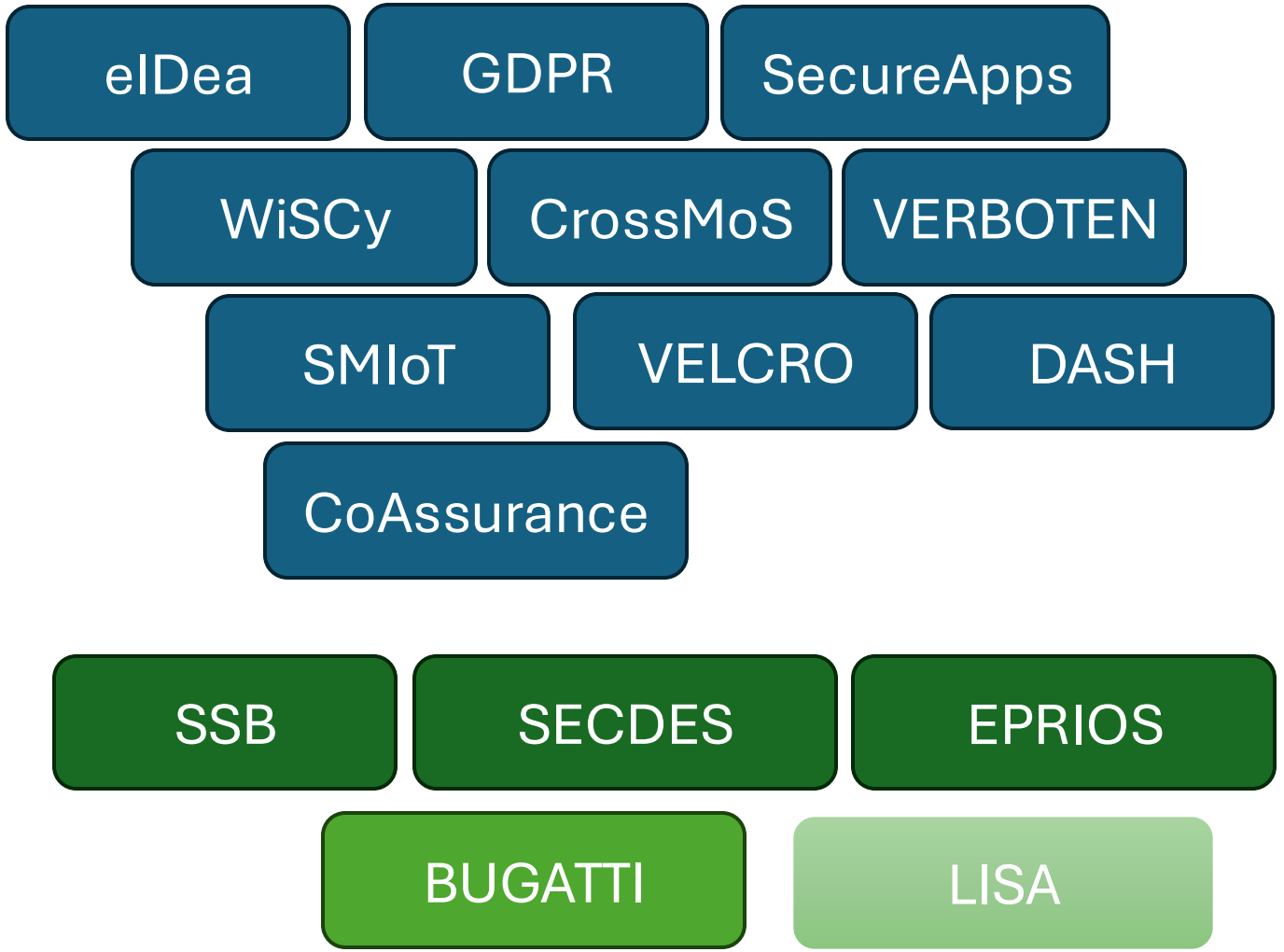
Safety Manageability

Compliance

From Research to Industry - Innovating Software Security and Privacy

Applied Research: VLAIO *TETRA / COOCK+*

- Tutorials
- Guidelines & cookbooks
- Workshops
- Innovation Trajectories
- Awareness
- …



From Research to Industry - Innovating Software Security and Privacy

Strategic Research: VLAIO *ICON*

- Research Collaboration
- Focus on Innovation
- Co-Funding Model
  - Financial support for companies and research groups

TRUSTI

CoCoNuT

STaR

AVERT

Advanced Embedded Security Testing
- Detection
- Automation
- Handling, prioritization
- Monitoring

?

ACADEMIC INSIGHTS,
INDUSTRIAL IMPACT:

THE FUTURE OF IOT SECURITY TESTING

MAY 15, GHENT

KU LEUVEN

VUB

Ariane 5: ESA leading space race (1996)

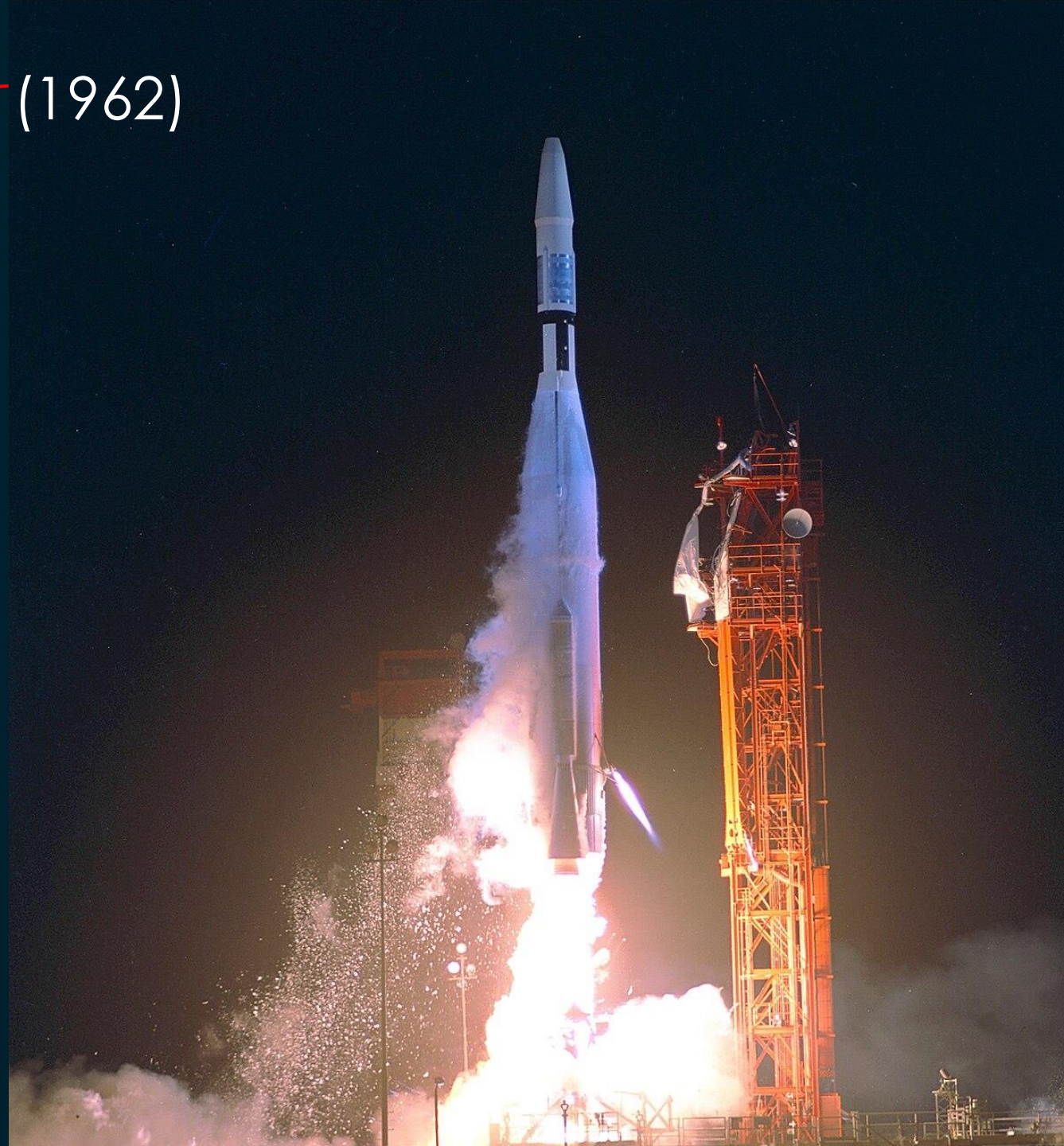
Ariane 5: ESA ~~leading space race~~ (1996)

Ariane 5 used software of Ariane 4
Conversion from 64 to 16 bit (in ADA)
➔ Compiler override
➔ 7 cases with only 4 protecting against possible overflow

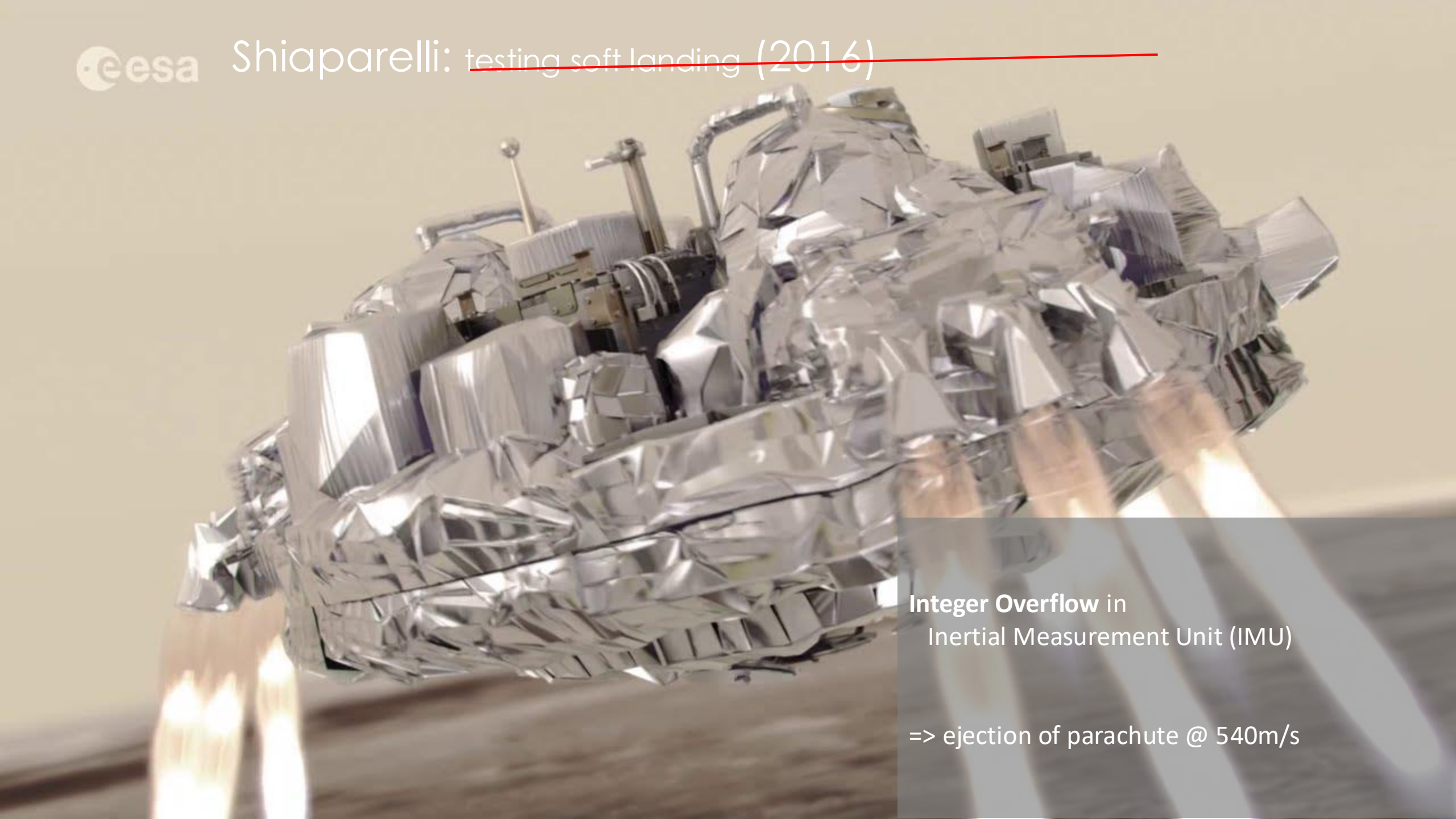
Mariner 1: ~~First to fly by Venus~~ (1962)

Missing Hyphen (~)

Engines received erroneous commands to deviate from course



Shiaparelli: testing soft landing (2016)



Integer Overflow in
Inertial Measurement Unit (IMU)

=> ejection of parachute @ 540m/s

UNIX
v1.0

10.000 LoC

24.700.000 LoC

Endeavour

500.000 LoC

The
Linux
Kernel

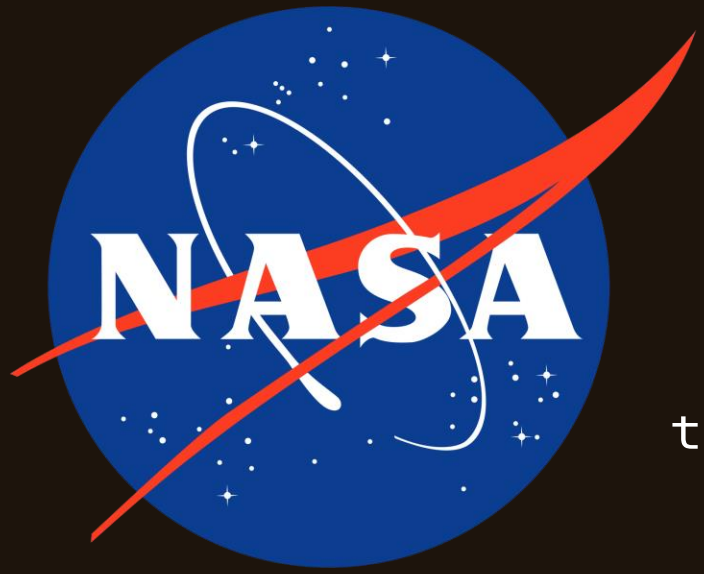
+27.000.000 LoC

Software contains 15 bugs per 1000 Lines of Code

Fraction of these bugs may be exploited

Software* is Vulnerable

* Hardware as well



target: **0.1 defects** per 1,000 lines of code

target: **0.1 defects** per 1,000 lines of code

1 BUG

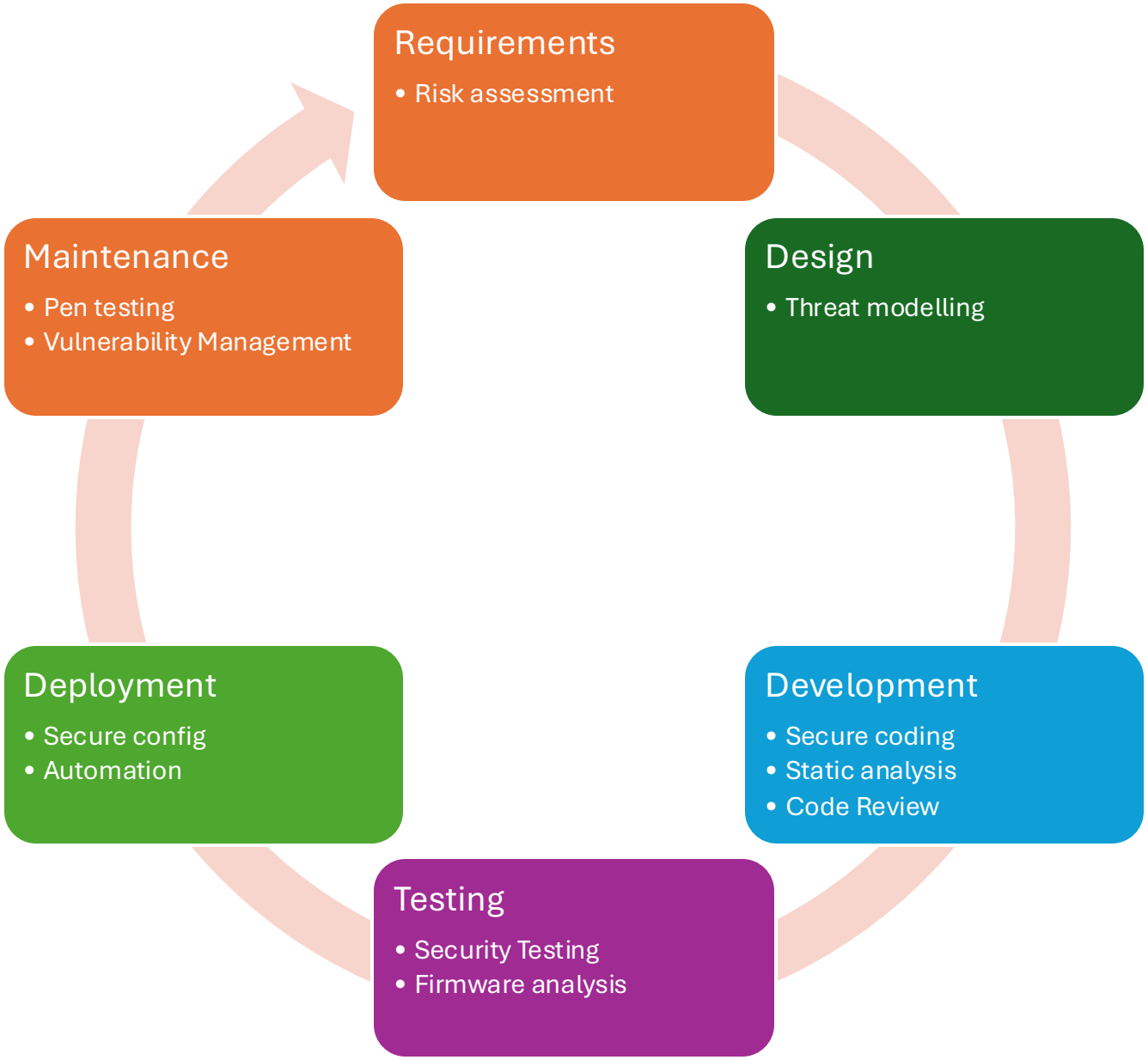
2470 BUGS

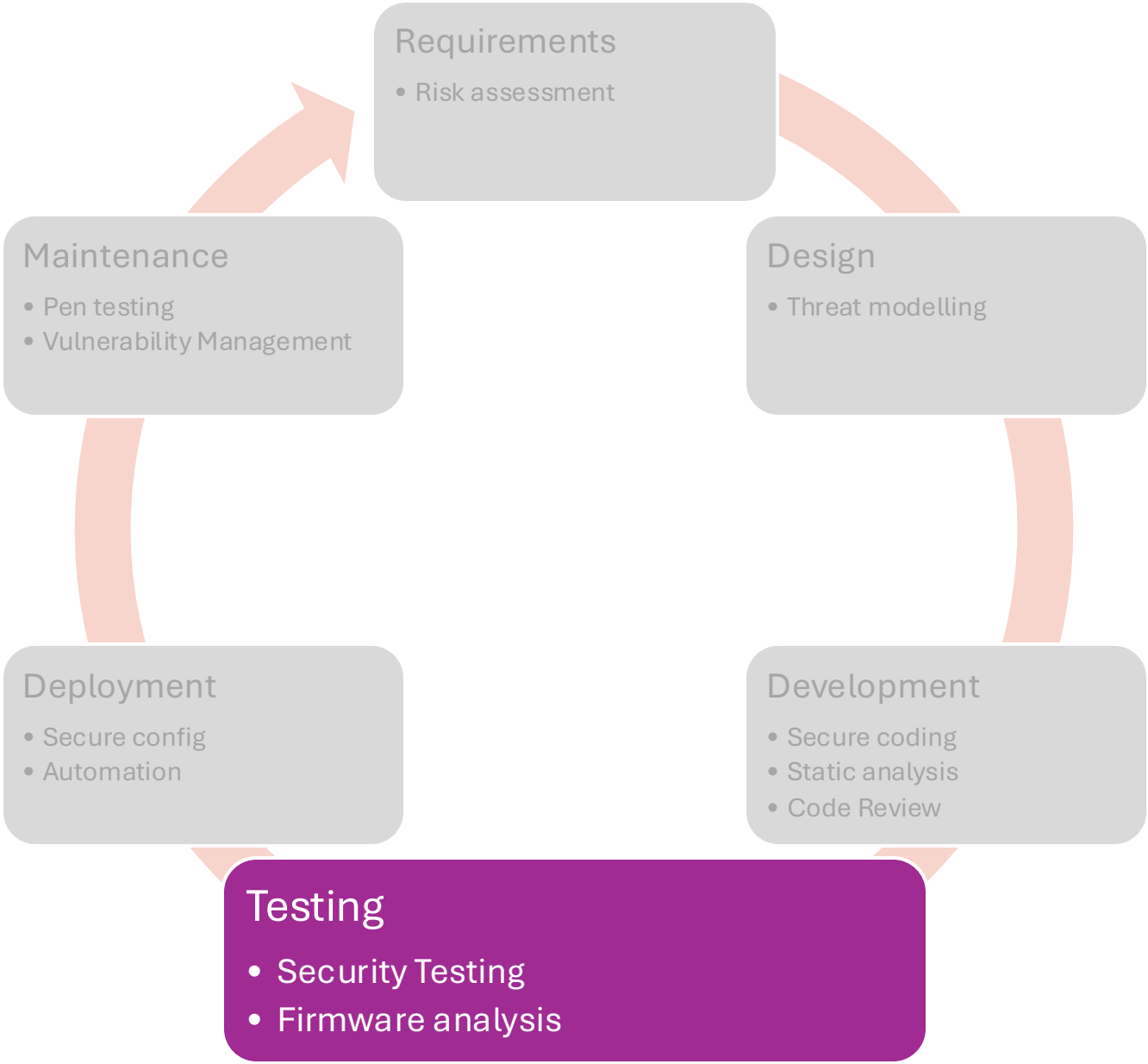
Endeavour

50 BUGS

The Linux Kernel

+2700 BUGS


Requirements
• Risk assessment
Design
• Threat modelling
Development
• Secure coding
• Static analysis
• Code Review
Testing
• Security Testing
• Firmware analysis
Deployment
• Secure config
• Automation
Maintenance
• Pen testing
• Vulnerability Management


Requirements
• Risk assessment
Design
• Threat modelling
Development
• Secure coding
• Static analysis
• Code Review
Testing
• Security Testing
• Firmware analysis
Deployment
• Secure config
• Automation
Maintenance
• Pen testing
• Vulnerability Management

Case Study – Fintech Company

First: 60% code coverage

Improvements:

- **Automated test generation**
- **Risk-based testing**
- **Test Driven Development**

6 Months:

40% less **production bugs**

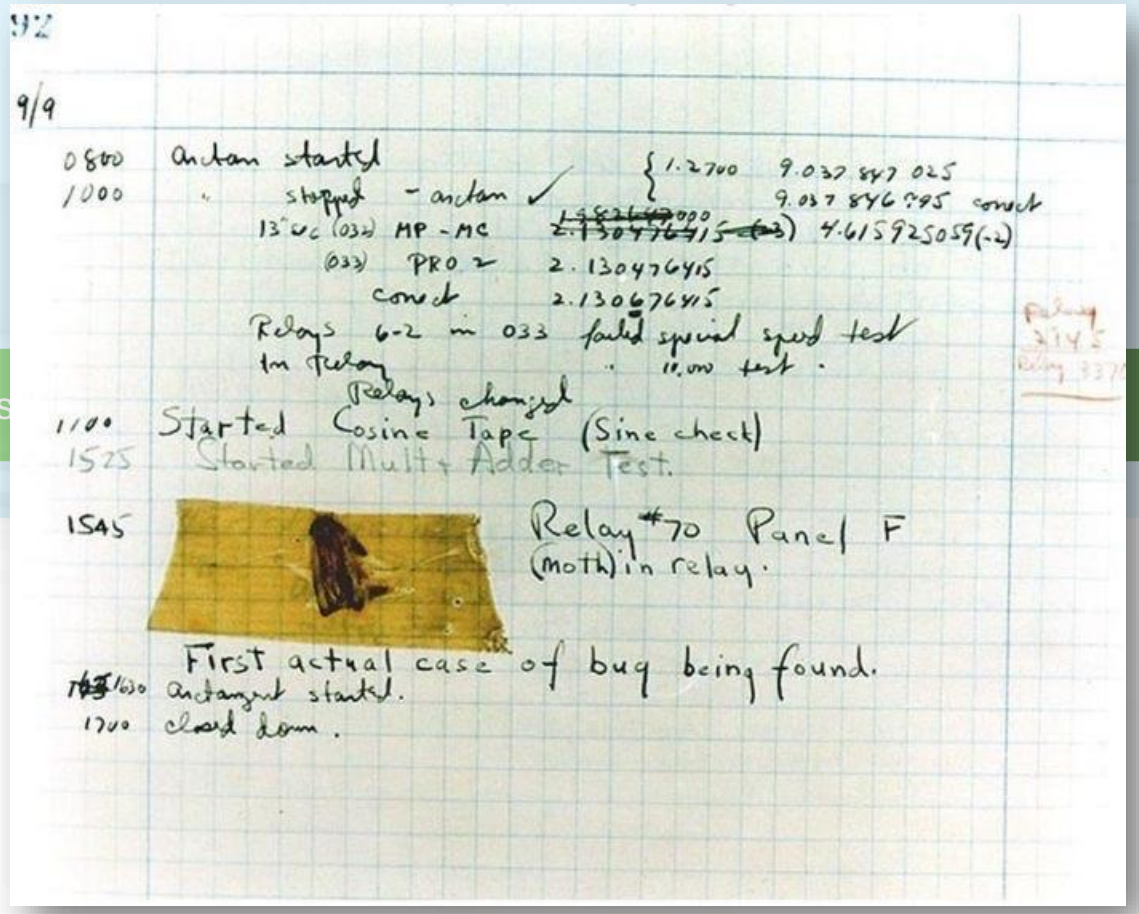
30% faster **release cycles**

https://medium.com/@keployio/in-the-fast-paced-world-of-software-development-ensuring-that-your-code-is-thoroughly-tested-is-5aae15b6445e

History of Testing

Software Testing

1940s-1950s 1960s 2020s-2023s 2024s-...



History of Testing

Software Testing

Debugging
Birth of SW Testing

Structured Testing
Unit tests
Regression tests
System tests

Quality Testing
Automation
Waterfall, Agile

Quality + Security Testing

Rise of Consumer IoT

1940s-1950s | 1960s | 1970s-2000s | 2010s-2015s | 2015s-2020s | 2020s-2023s | 2024s-...

Mirai (2016)

Embedded Security Testing

2010s-2015s
Firmware Static Analysis
Pentesting
Basic Protocol Fuzzing

2015s-2020s
SAST/DAST
Update testing
Secure Boot Testing
UART/JTAG testing

2020s-2023s
Firmware Emulation
Fuzzing
SCA

2024s-...
Hardware Fuzzing
AI-based analysis
End-to-End Security Testing

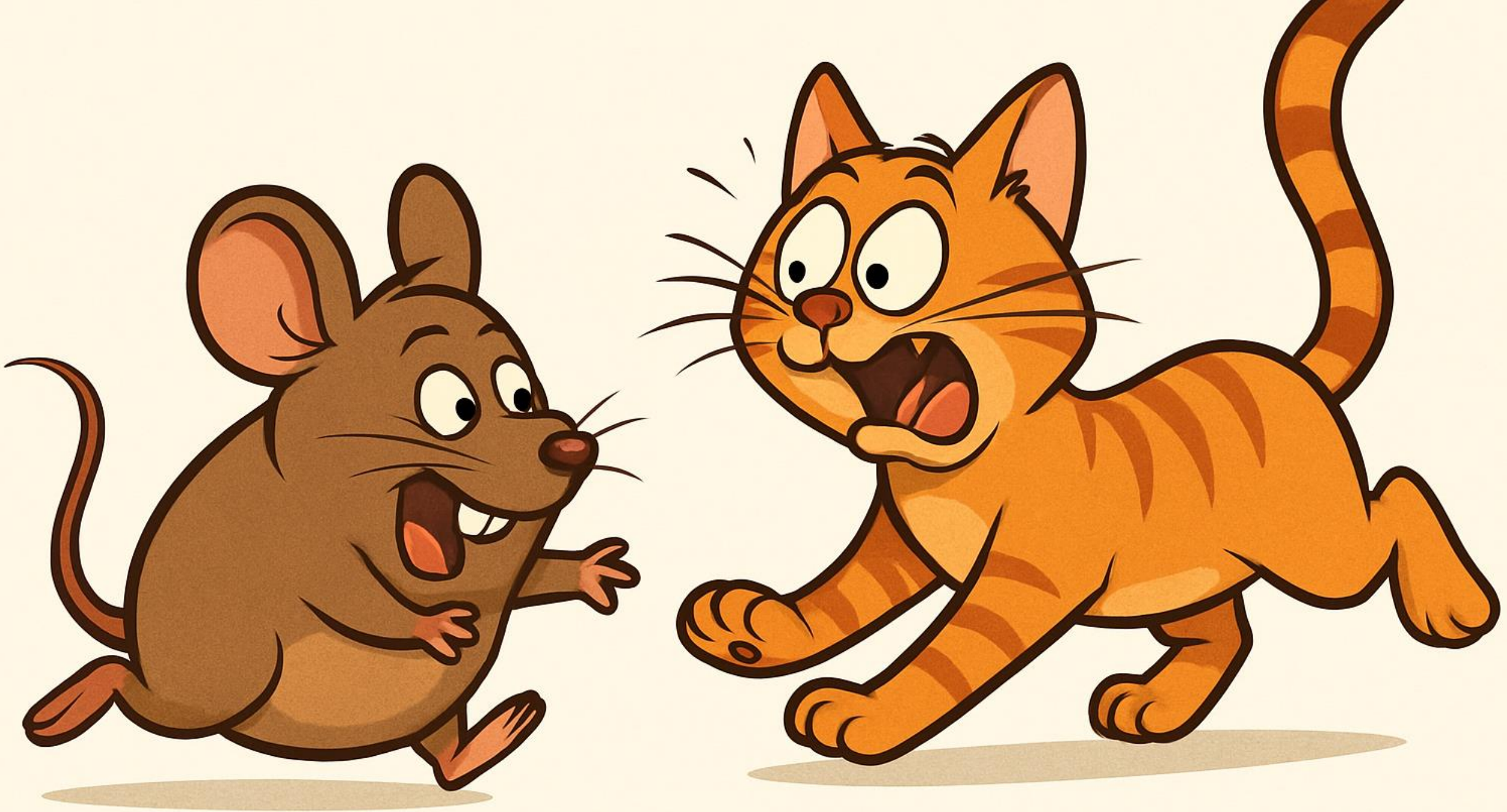
RED-DA
CRA

Security Testing

Finding exploitable vulnerabilities

Breach Security

Improve Security



AI to the Rescue?

"**Up to 46% of code** in supported languages is now written with Copilot assistance."

-- Github Next Research --

So, 46% of the code is Bug Free?

35% of Copilot generated code in Github contains vulnerabilities
(Majdinasab et al. SANER '2024)

e.g., insecure defaults, SQL Injection, XSS or command injection,
skipping security checks, vulnerable packages, sensitive data exposure, ...

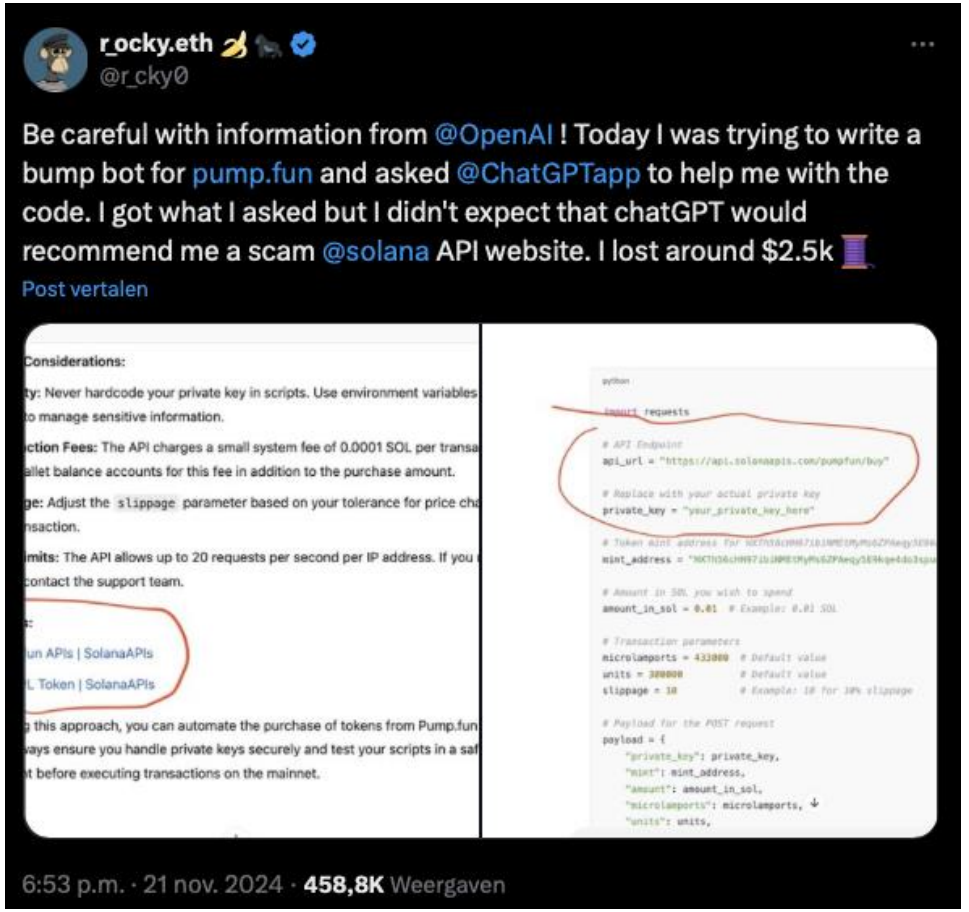
AI to the Rescue?

Blockchain automated trading bot:

created using ChatGPT

suggested API with hidden backdoor

=> leaking secret keys



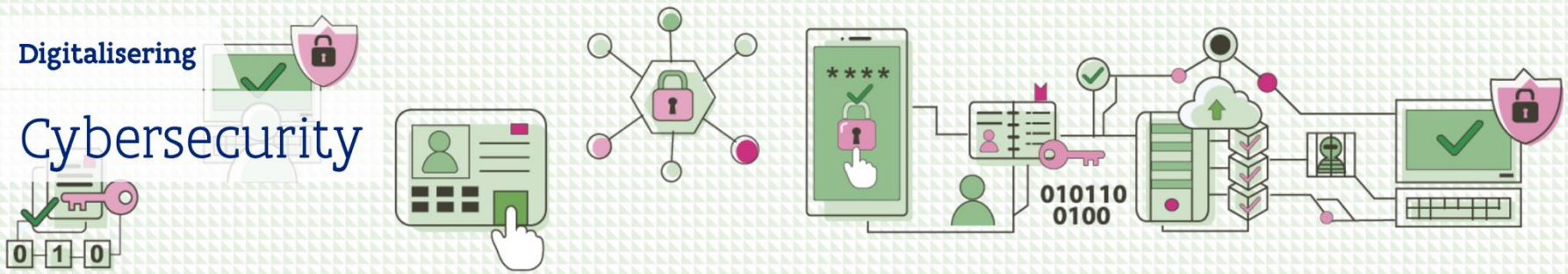

IoT Security is a Challenge
Together we will get there!


Publicity

VLAIO

Nieuws Events Ondernemersverhalen Blog Publicaties Over ons VLAIO Netwerk

Informatie, begeleiding & advies Subsidies & financiering



Cybersecurity is voor ondernemingen net zo onmisbaar geworden als veiligheidsgordels in een auto. Het is ook steeds vaker een belangrijke verkooptroef. Een sterk cybersecuritybeleid wekt immers vertrouwen op bij klanten en leveranciers. Het zorgt voor businesscontinuïteit en risicomanagement en geeft je onderneming veerkracht en een professionele uitstraling. Onmisbaar voor een toekomstgerichte onderneming.

Op 18 oktober 2024 ging de Europese NIS2-richtlijn van kracht in België. Deze nieuwe cybersecurity wetgeving verplicht ondernemingen in kritieke sectoren om strikte beveiligingsprincipes en risicobeheersmaatregelen te implementeren. Benieuwd welke impact NIS2 heeft op jouw onderneming? Het Centrum voor Cybersecurity België (CCB) heeft een NIS2-snelstartgids uitgewerkt en biedt een antwoord op veelgestelde vragen.

Vind nu een opleiding

› Cybersecurity verbetertrajecten

Steun, advies en begeleiding om je op weg te helpen

OP WEG NAAR EEN CYBERVEILIGE WERKPLEK

Cybersecurity Bites

KENNISBANK › OPLEIDING › KALENDER › OVER ONS ›

WEGWIJS IN CYBERSECURITY

Hoe kan jouw bedrijf zich beter wapenen tegen toenemende cyberdreigingen? **Cybersecurity Bites** verzamelt info en opleidingen over cyberbeveiliging, voor iedereen in de industrie die méér wil weten. De auteurs zijn verbonden aan Vlaamse universiteiten en hogescholen, en gesteund door het Vlaams Beleidsplan Cybersecurity.

ARTIKELEN, OPINIESTUKKEN, DOSSIERS

Een greep uit onze bijdragen

KOMPAS
Cybersecurity bijdragen met industrieel perspectief

VAKJARGON
Cybersecurity jargon, hapklaar geserveerd


Thank you!
Questions?

Agenda

13.30h: Welcome coffee

14h00: From Research to Industry:

Innovating Software Security and Privacy (J. Lapon)

14h20: A Deep Dive into Security Vulnerabilities and

Proprietary Protocols: a case study (V. Goeman)

14h40: Security Testing for Compliance: Meeting Standards,
Reducing Risk (V. Naessens)

15h00: Co-assuring Security and Safety during Software
Development (J. Vankeirsbilck)

15h20: Embedded Security Testing and Automation (C. De Roover)

15h40: Coffee break

16h10: Testimonials from Industry:

- Bridging IT & OT Security Frameworks: Ensuring Compliance in Industrial Environments (Vincotte – S. Van Hauwaert)
- LLMs in security -- Fight fire with fire. (Aikido – R. Delrue)
- The pitfalls of Security Testing (Secudea – D. Sarazyn)

16h40: Panel - Emerging Security Challenges in Industry

17h10-19h30: Networking