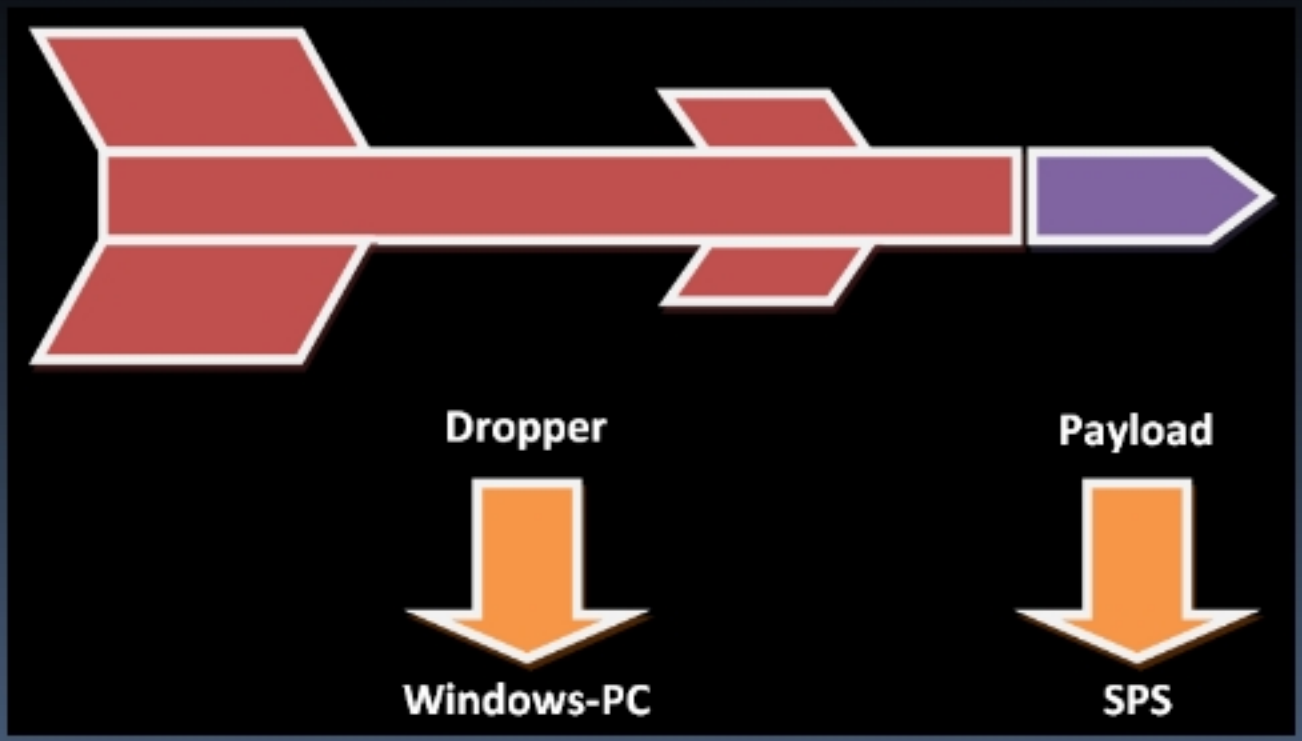
Stuxnet redux

Ralph Langner
Langner Communications GmbH, Hamburg

- USB-Sticks
- Geteilte Verzeichnisse
- Lokale Print-Spooler
- Sehr begrenzte, „lokale“ Verbreitung


Dropper
Payload
Windows-PC
SPS

Dropper auf Windows-PCs

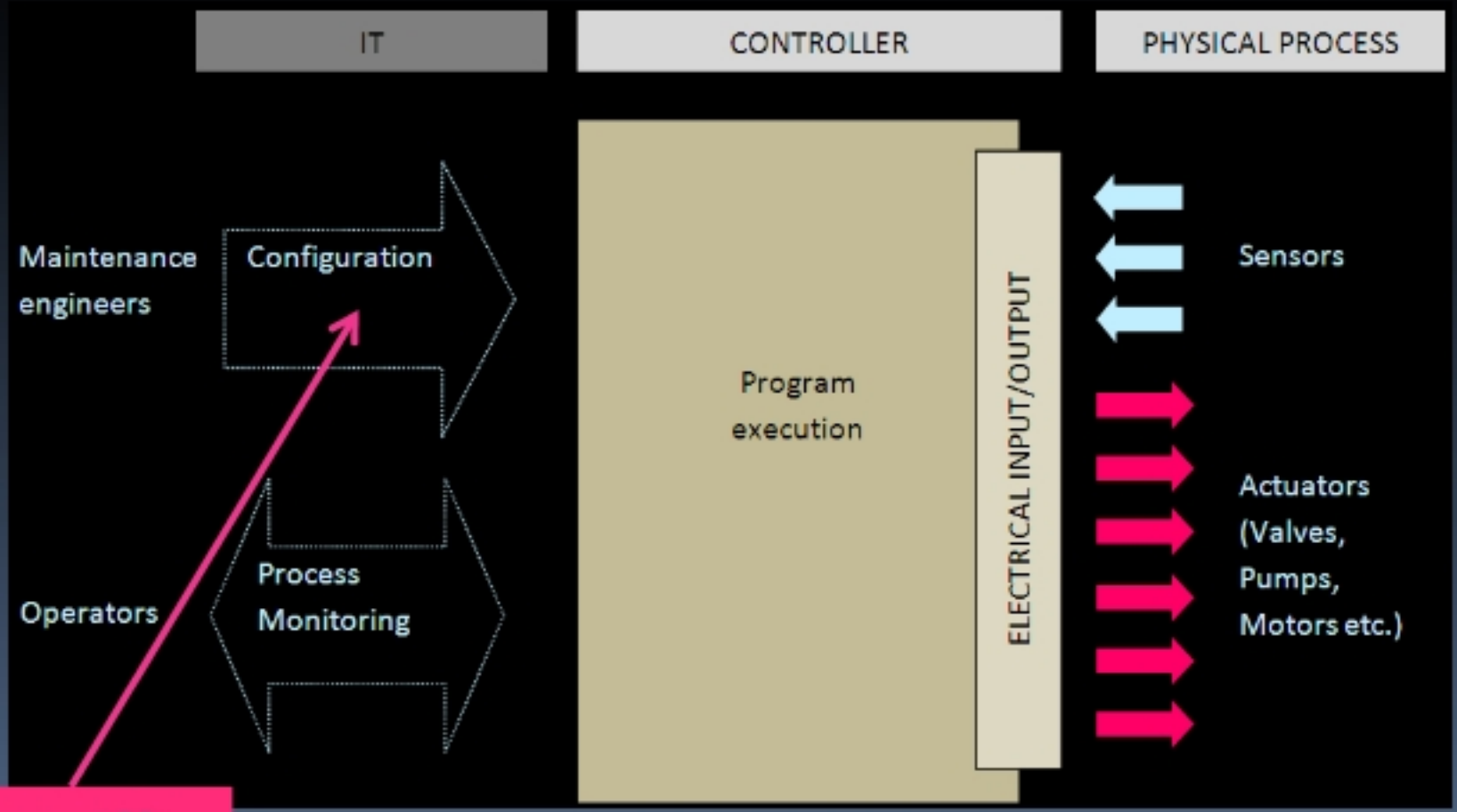
- infiziert jeden PC in der Nähe
- komplex

Payload auf Industriesteuerungen

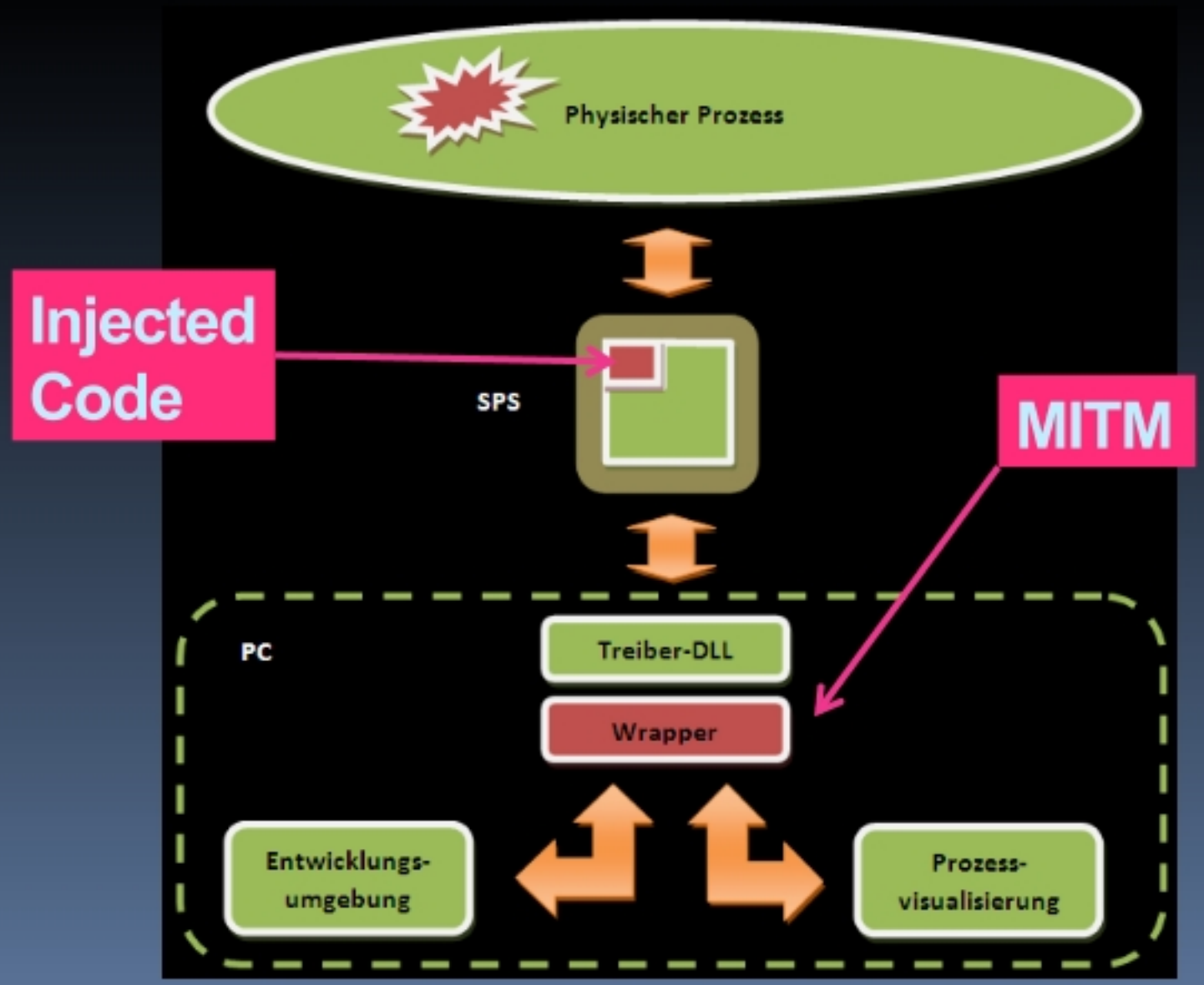
- nur für ein einziges Ziel aktiviert
- hyperkomplex

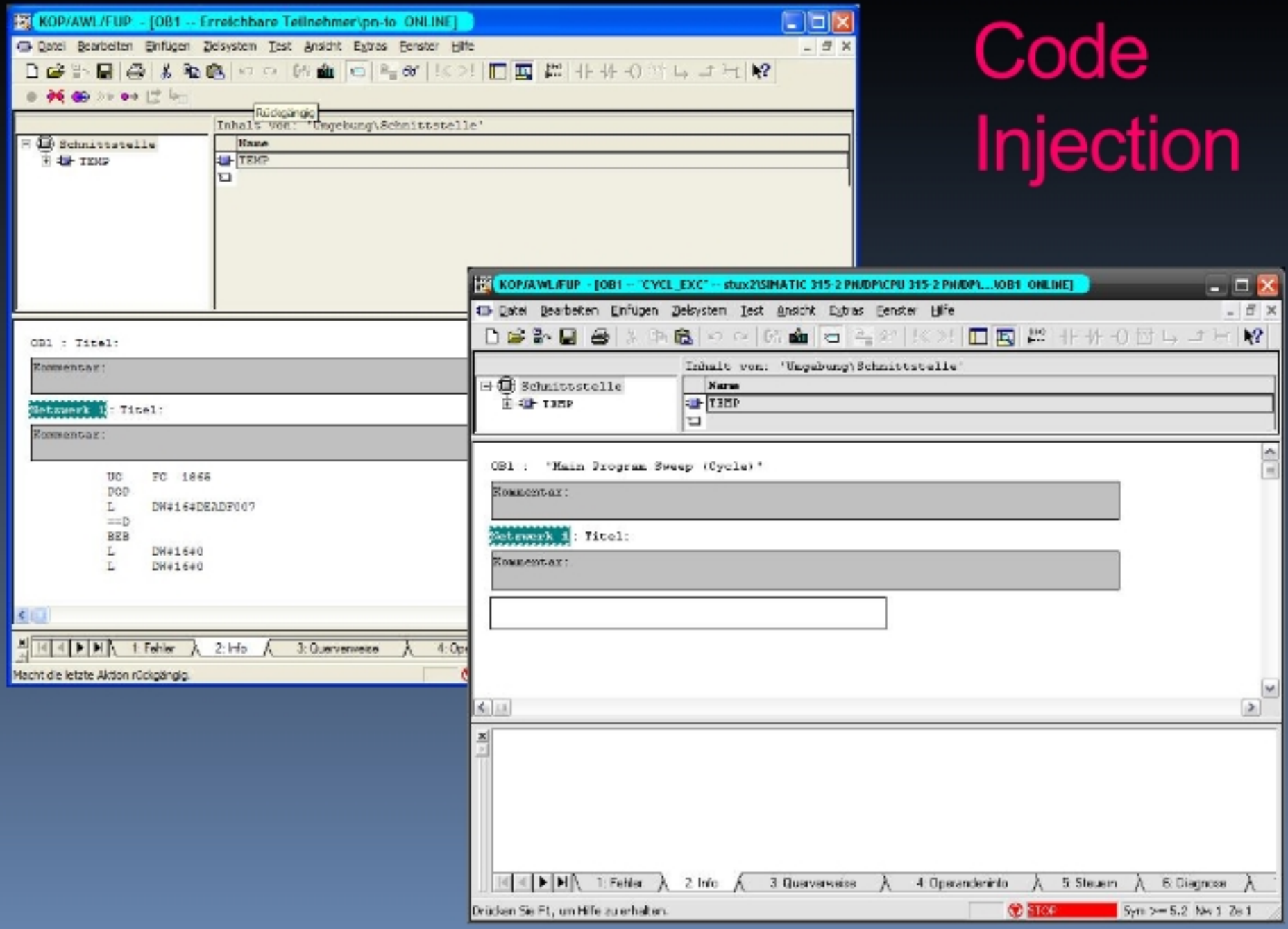
Was ist eine SPS?

- Kein Computer
- Echtzeitbetrieb
- Elektrisch verschaltet mit Sensoren und Aktoren
- Keine IT-Sicherheitsmaßnahmen
- Universell einsetzbar



Angriffs-vektor


Physischer Prozess
Injected Code
SPS
MITM
PC
Treiber-DLL
Wrapper
Entwicklungs-umgebung
Prozess-visualisierung

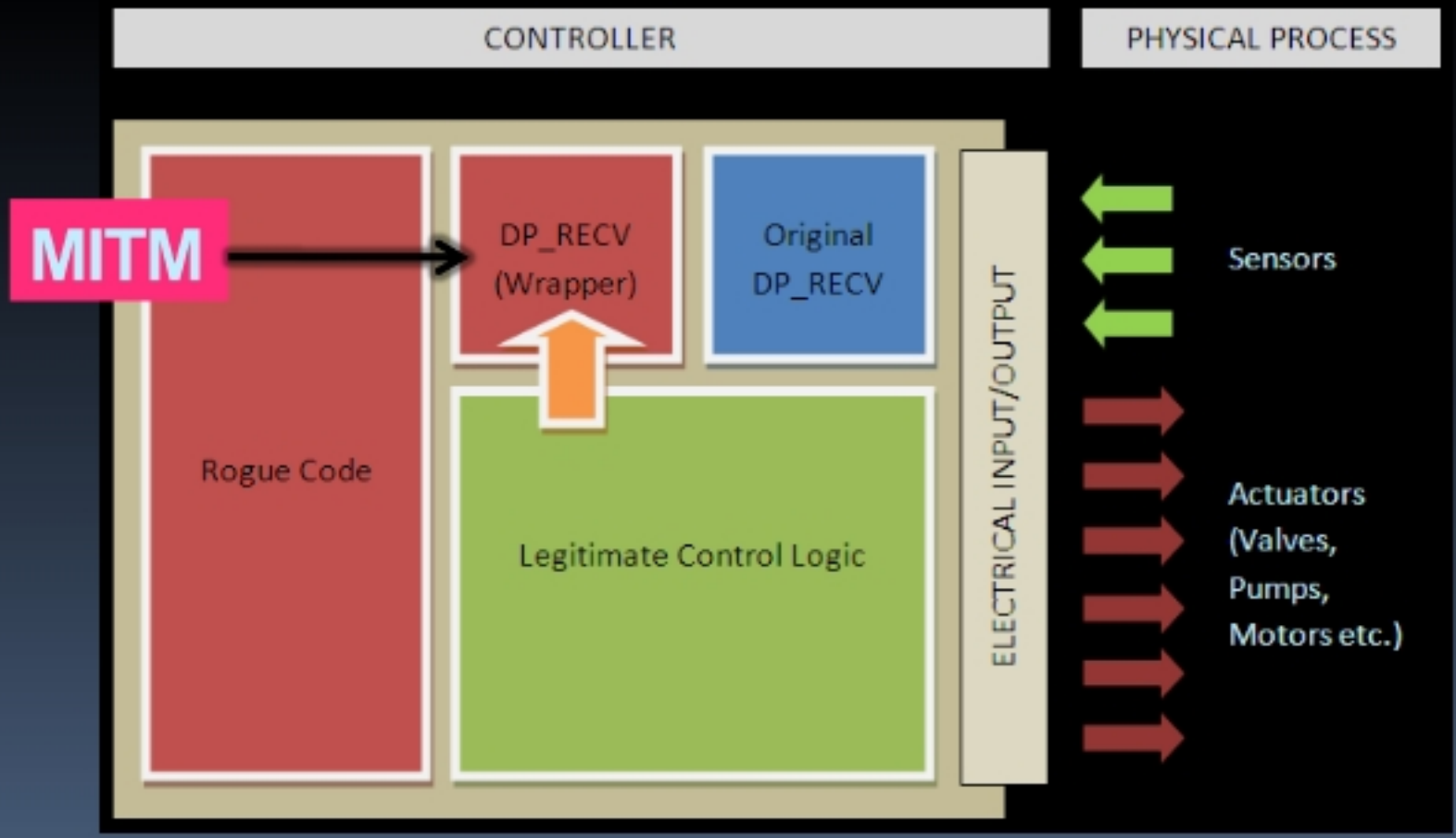


Code Injection

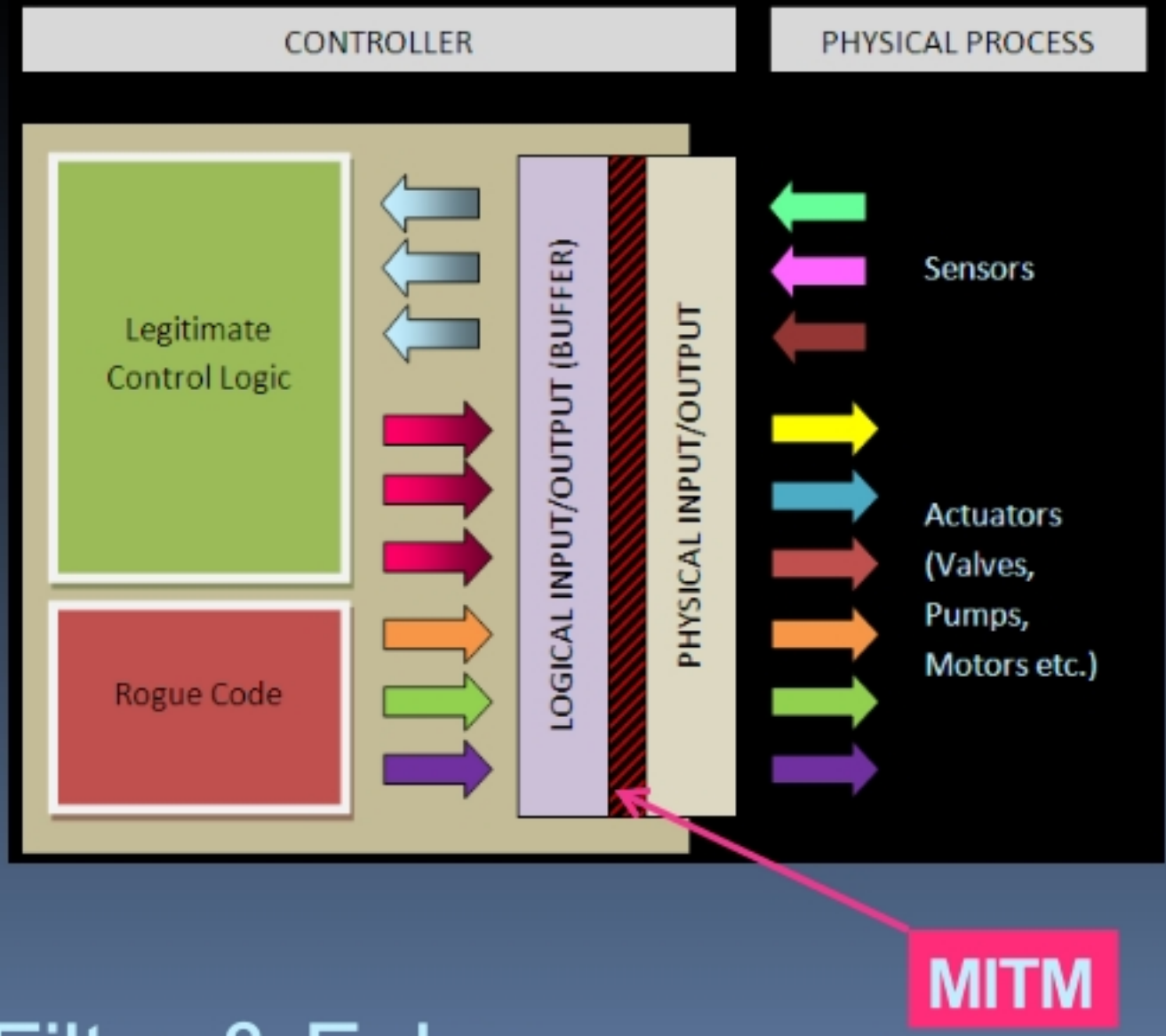
SPS-Angriffscode

- ca. 15.000 Zeilen
- 2,5 Module
- entwickelt von Top-Experten
- Teile ziel-spezifisch, andere Teile generisch

```
M117:  L      LW0
       L      164
       <=I
       SPBN   M101
       L      LW0
       L      1
       >=I
       L      LW0
       L      2
       =      L14.2
       <=I
       U      L 14.2
       SPBN   M102
       L      LW0
       ITD
```



System Function Intercept



I/O Filter & Faker

„Virtuelle Chinesische Wasserfolter“

- Zerstörung von IR-1 Zentrifugen
- Schleichend, nicht offensichtlich
- Angriff angelegt
  auf mehrere Jahre

APT

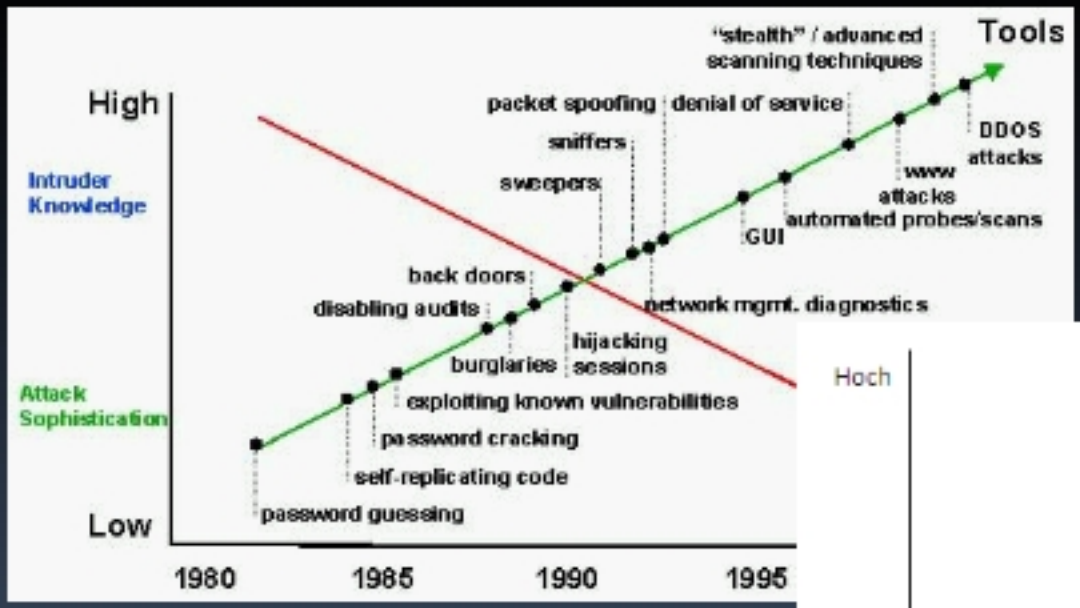
Exploit cost/value

OS
- 2 Digital Certs $
- 4 0Day Vulns $$
- PtP Update $$$

Applications
- DLL Hijacking $$$
- SQL Injection $
- Code Exec $$$

PLC system level
- Step7 Injection $$$$
- SFC Wrapping $$
- IO Filter/Faker $$$$$

PLC app level
- IR-1 Rotor Cracking Code $$$$$



Entwicklung der Angriffskomplexität

Resultat Cyber-Angriff:

- Zeitgewinn: ~ 2 Jahre
- Tote + Verletzte: Null
- Kosten: ~ 7 Millionen Euro

Resultat Luftschlag (hypothetisch):

- Zeitgewinn: 2-3 Jahre
- Tote + Verletzte: Viele Tausend
- Kosten: Viele Milliarden Euro

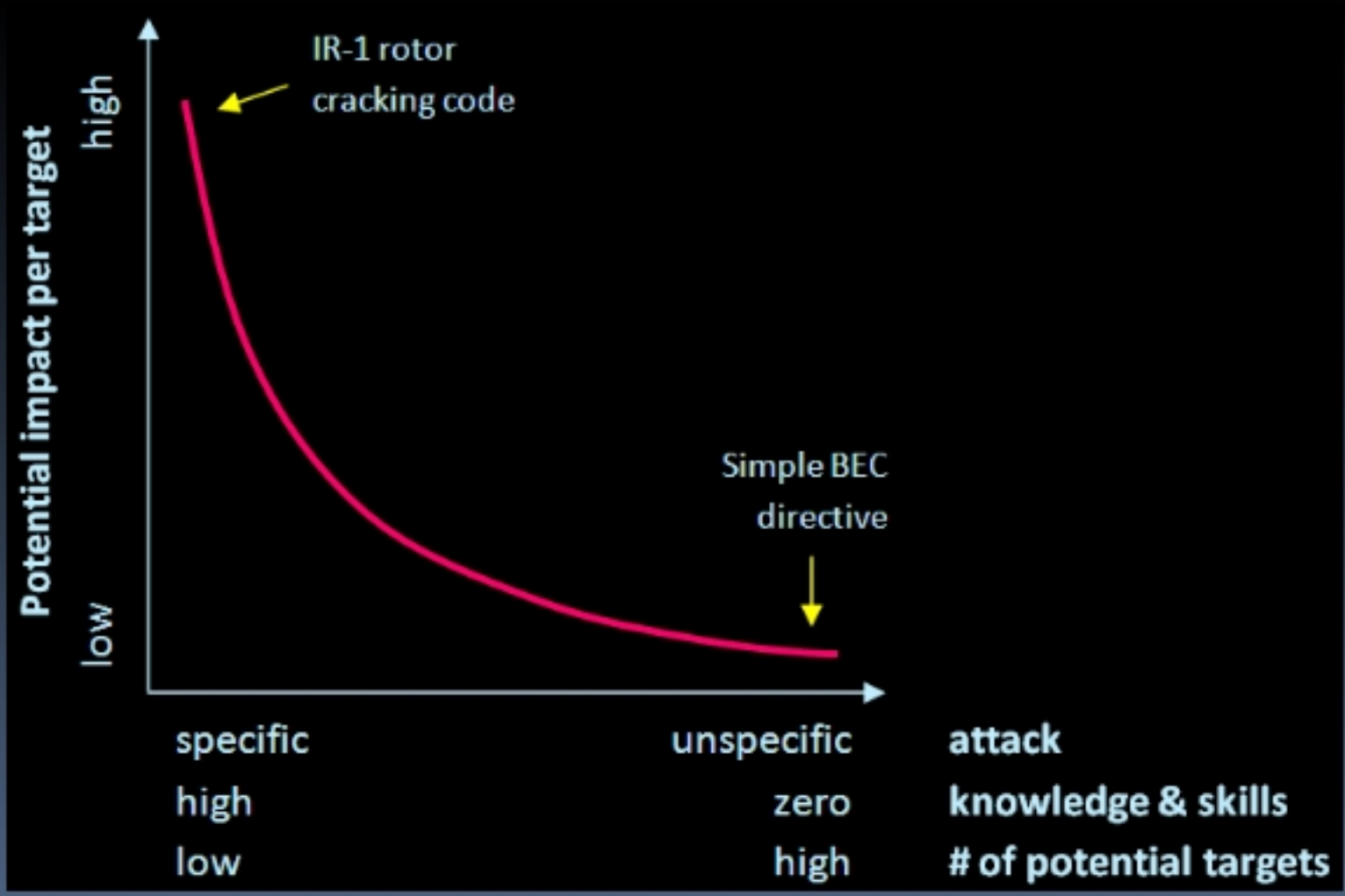
Automatisierbare Exploits

OS
- 2 Digital Certs ✗
- 4 0Day Vulns ✓
- PtP Update ✓

PLC system level
- Step7 Injection ✓
- SFC Wrapping ✓
- IO Filter/Faker ✓

Applications
- DLL Hijacking ✓
- SQL Injection ✓
- Code Exec ✓

PLC app level
- IR-1 Rotor Cracking Code ✗



Spezifische vs. unspezifische Angriffe

Spezifische vs. unspezifische Angriffe

Security-Maßnahmen

	IT	AT
User-ID + Passwort	✓	✗
Verschlüsselung	✓	✗
Antivirus	✓	✗
Sicherheits-Patches	✓	✗
Digital signierter Code	✓	✗
Firewalls	✓	✗
Intrusion Detection	✓	✗
Network Monitoring	✓	✗
Störfestigkeit (Resilience)	✓	✗
Policys	✓	✗
Standards	✓	✗

Fragen

Homepage: www.langner.com

Blog: www.langner.com/en/blog

Kontakt: info@langner.com

Buch: *Robust control system networks.*
How to achieve reliable control after Stuxnet.
(Momentum Publishing, New York 2011)