DEEPSEC

Anforderungen an autonome Systeme

René Pfeiffer

DeepSec In-Depth Security Conference

 https://deepsec.net/ | https://blog.deepsec.net/

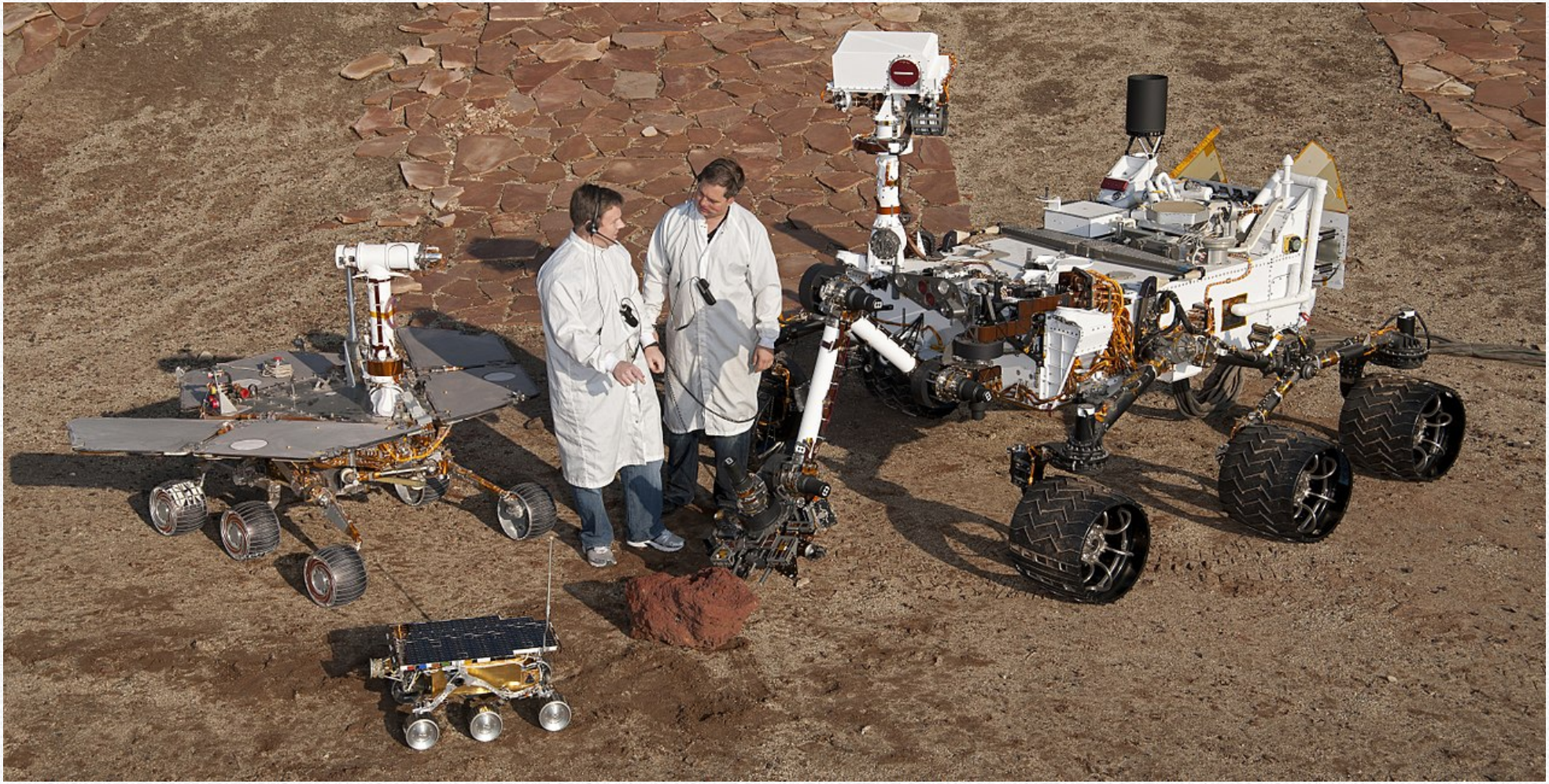
IT-Security Community Exchange 2019 (IT-SECX 2019)

Autonom?

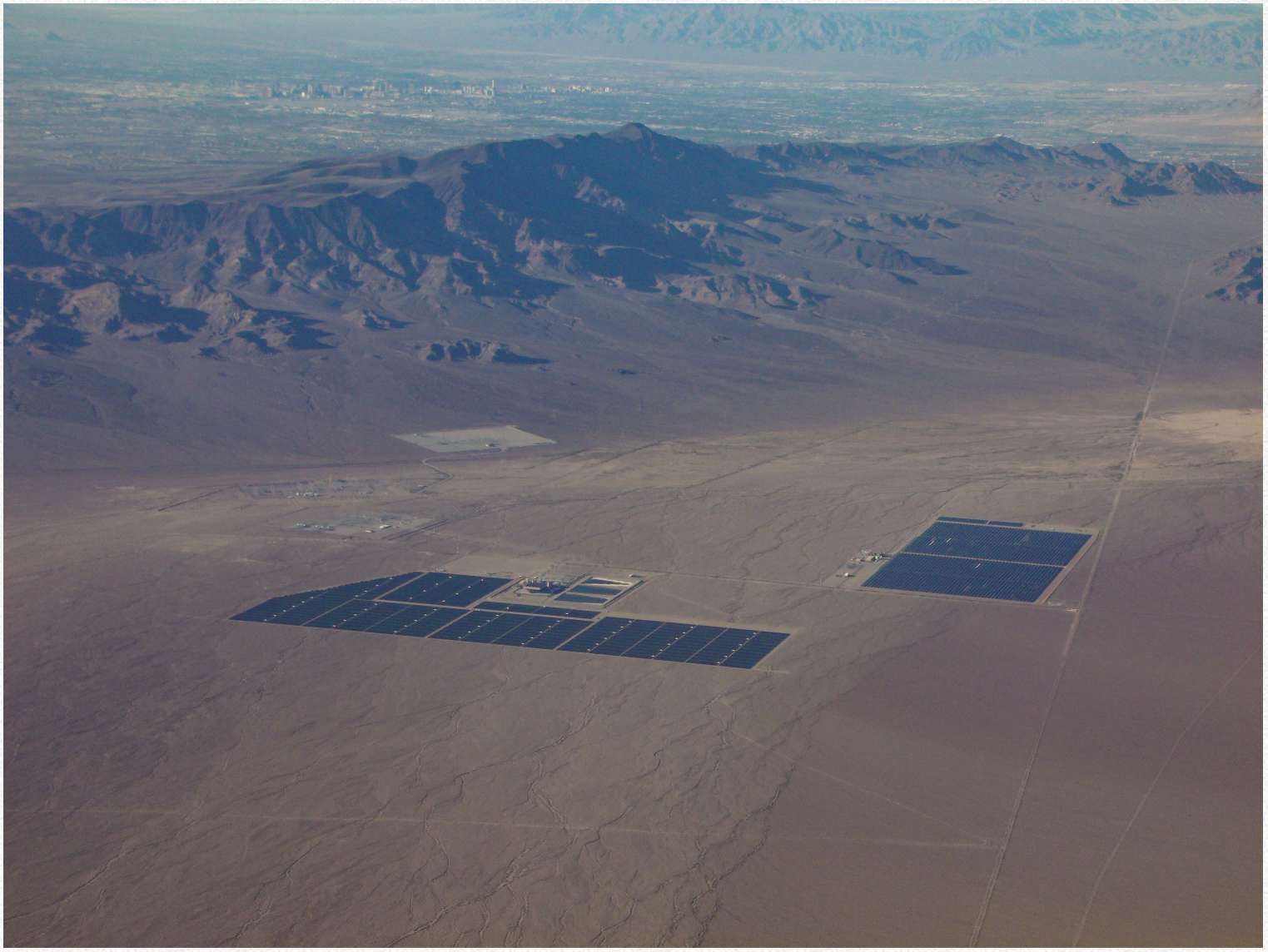
Quelle: Google Waymo, Wikipedia, Dllu

Autonom?

Quelle: NASA



Quelle: NASA Jet Propulsion Laboratory



Quelle: Nevada Solar One

Kommunikation – Latenz

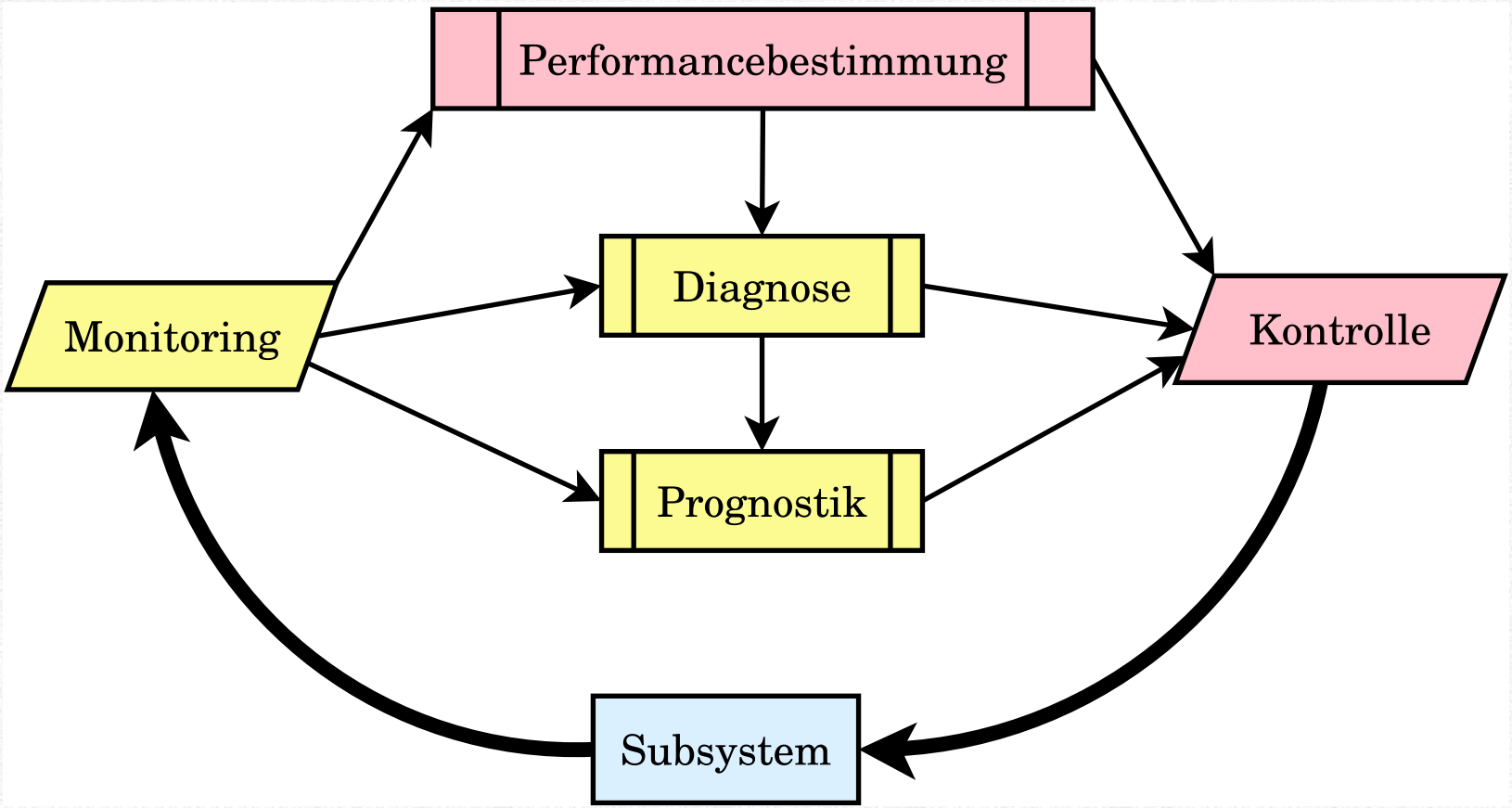
DEEPSEC

Circuit	Distance	Delay Time
HF link (UK-NZ)	~20,000 km	0.07 s (67 ms)
Submarine cable(UK-NZ)	~20,000 km	0.07 s (67 ms)
Geosat Link (US-Aus)	~80,000 km	0.25 s
Earth-Moon	384,000 km	1.3 s
Earth-Mars	55 - 378 million km	3 - 21 minutes
Earth-Jupiter	590 - 970 million km	33 - 53 minutes
Earth-Pluto	~5800 million km	5 hours
Earth-Nearest Star	~40 million million km	4 years

Quelle: Australian Space Academy

- normale Interaktion bei wenigen Sekunden Latenz
- lokale Behandlung taktischer Situationen bei Minuten
  - Warten auf Steuerung / Eingaben unmöglich
  - Telemetrie / strategische Entscheidungen möglich
- lokale Ressourcen für Verarbeitung Sensordaten
- Entscheidungen auf Basis „lokalen Wissens“

Management Loops

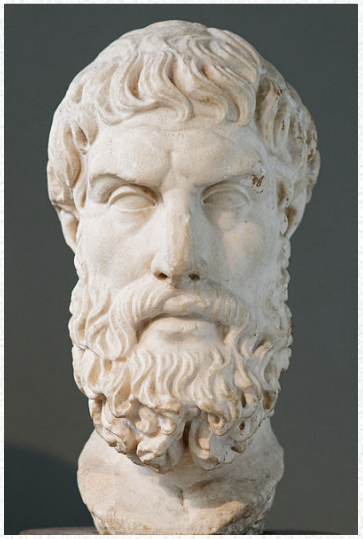


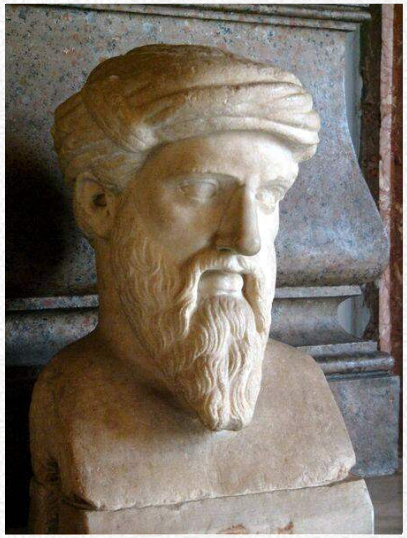
Quelle: System Engineering of Autonomous Space Vehicles, NASA Technical Reports

Implementationen

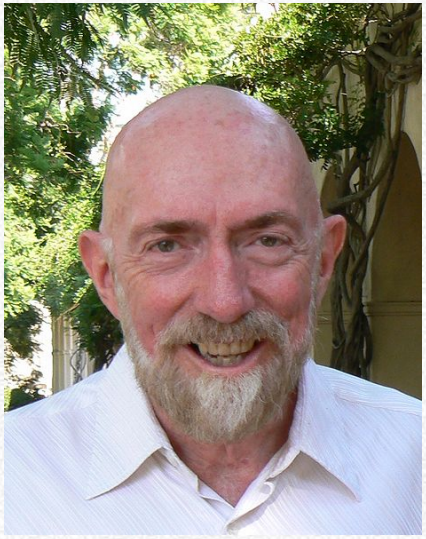
„Artificial Intelligence“

DEEPSEC







Quelle: Wikipedia

- System State
  - Managementsysteme
  - Movement Control (wenn vorhanden)
  - Thermal Management (wenn vorhanden)
  - Strukturelle Integrität
  - Stromversorgung
  - Kommunikationssysteme
- Wechselwirkungen erfassen
- Situationen & Operationen definieren

Komponenten

- Expertensysteme
- Neuronale Netzwerke (NN)
- Fuzzy Logic
- Model-Based Reasoner (MBR)
- Bayesian Belief Networks (BBN)

Expertensysteme

- Regelsatz für Missionsparameter
- Messen / Gegensteuern / Regeln
- Beobachten / Einhalten von Grenzwerten
- enthalten „Basiswissen“ über System

- geeignet für nichtlineare Systeme
- nützliche als Backup, schnelle Reaktion, Fehlerausgleich
- gut parallelisierbar
- rechenintensiv
- „Lernschwächen“ (steuerbar durch Trainingsbedingungen)

Fuzzy Logic

- Theorie älter als Internet, gut erforscht
- Fahrzeugsteuerung
- Regelung Umgebung (Temperatur, Leistung, …)
- verwendet in Software und Hardware
- Frameworks vorhanden

Model-Based Reasoner

- Expertensystem mit Domain Knowledge
- benötigt Modell und Struktur des Systems, sowie Ziele
- Beobachtung wird mit tatsächlichem Zustand verglichen
- Diskrepanz löst Diagnose und Gegenmaßnahmen aus

Bayesian Belief Networks

- BBN erfassen (nicht) zustandsabhängige Beziehungen zwischen zufälligen Variablen
- Training durch Experten und mit Testdaten möglich
- Schätzung von kausalen oder zukünftigen Ereignissen
- konservative Erstellung des Graphen
- Datenquelle für Expertensystem / MBR
- können Meßdaten qualifizieren

- Autonome Systeme müssen sich selbst verteidigen
- schärfere Definition von Anomalien
- keine Abhängigkeiten von vernetzten Resourcen
- hoher Grad an Qualität notwendig
  - reduzierte Komplexität
  - extremes Secure Design/Coding
- „everything onboard“

Anomalien

- Anomalien sind variabel, Definition schwierig
- Analyse „normaler“ & „anormaler“ Daten notwendig
- Baseline messbar
- Quellen für messbare Abweichungen
  - Zero Trust Umgebungen (Internet, öffentliche Plätze, …)
  - Traffic Analysis / Deep Packet Inspection
  - Fehlerzustände
  - nicht erwartete Ausnahmesituationen

Zusammenfassung

- Beschränkungen notwendig (diktiert *Mission Profile*)
- Systeme im Feld haben keine „Cloud“
- konservative Auswahl von Technologie
- sorgfältige Auswahl von Algorithmen
- Orientierung an Extremfällen
- Erfahrung/Tests benötigen Zeit – siehe Anomalien („*Rome wasn‘t burnt in a day.*“ 😀)
- Secure Design ist Grundbedingung

? Fragen ?

DEEPSEC

Quelle: https://imagearchives.esac.esa.int/picture.php?/8167/category/65
ESA/Rosetta/NAVCAM – CC BY-SA IGO 3.0

✉ Kontakt 📲☎

DEEPSEC

- 💘 rpfeiffer@deepsec.net
- 🔐 0x518A0576C3A9FF76
- 🔐 9EKKN34F
- 📲 +43.676.5626390
- 📲 +807.949.050.59 (GSMK Cryptophone™)
- ☎ +43.720.349387
- 🕸 https://deepsec.net/
- 🕸 https://blog.deepsec.net/

Über die DeepSec Konferenz

Die DeepSec GmbH veranstaltet seit 2007 jährlich im November die *DeepSec In-Depth Security Conference* in Wien. Die DeepSec bringt als neutrale Plattform die Sicherheitsexperten aus allen Bereichen zum Gedanken- und Erfahrungsaustausch zusammen. Dort erhalten IT- und Security-Unternehmen, Anwender, Behördenvertreter, Forscher und die Hacker-Community in über 42 Vorträgen und zweitägigen Trainings die Chance, sich über die aktuellen und zukünftigen Sicherheitsthemen auszutauschen. Die Konferenz möchte insbesondere dem weit verbreiteten Vorurteil entgegen wirken, dass Hacker, Studierende sowie Sicherheitsexpertinnen zwangsläufig Kriminelle sind.