WIBU SYSTEMS

Softwareschutz nach Kerckhoffs‘ Prinzip

Dr. Peer Wichmann

IT-Sicherheitsbeauftragter

Auguste Kerckhoffs

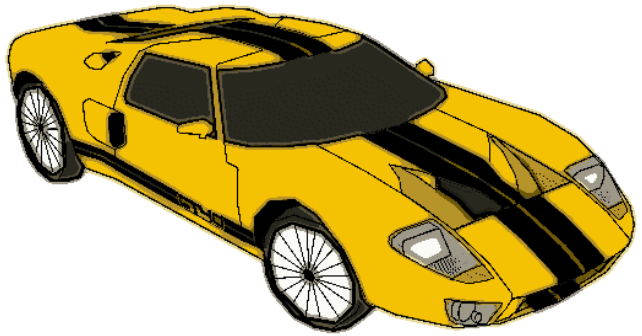
Beispiele Kerckhoffs Prinzip

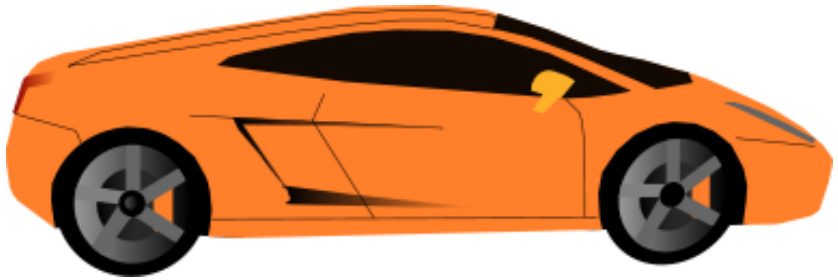
Gegenbeispiele Kerckhoffs´ Prinzip

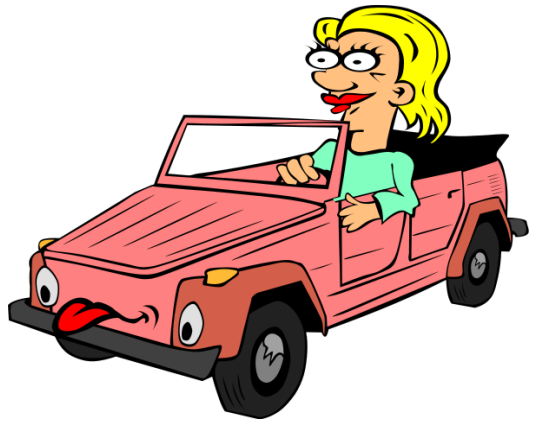
Software

Traditioneller Softwareschutz - Anbietersicht

Softwareschutz – Vertriebliche Sicht



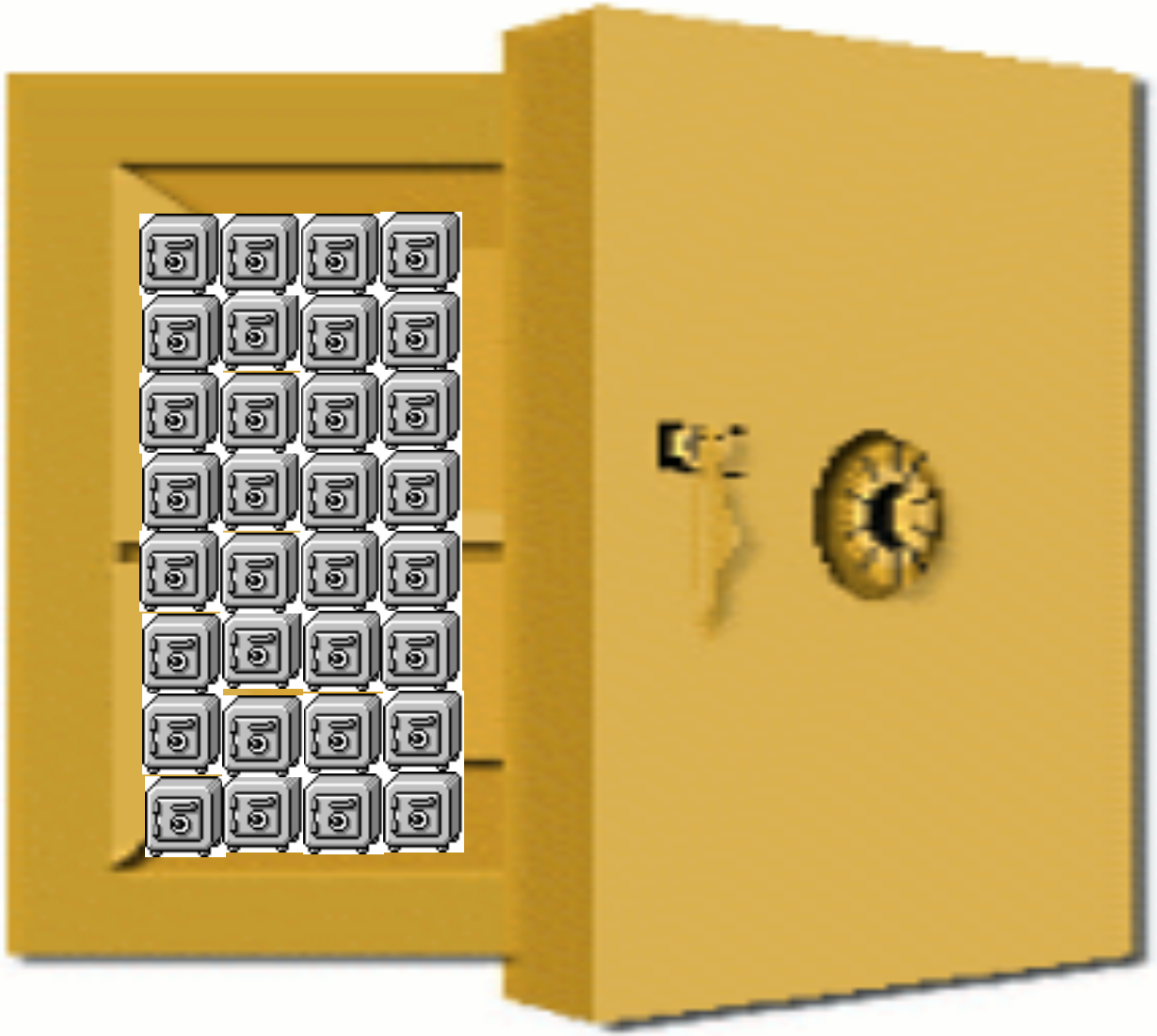




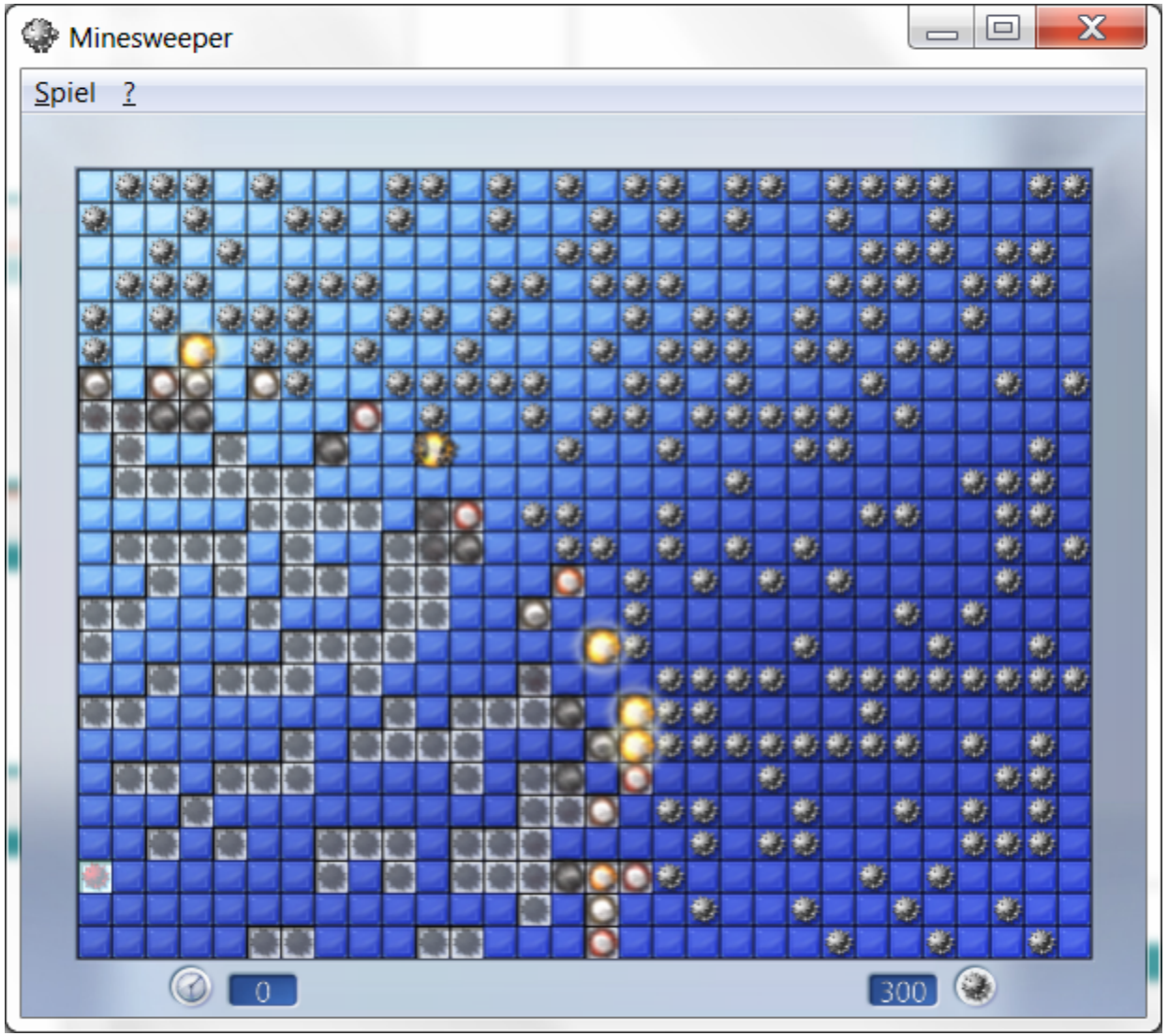
Softwareschutz - Angreifersicht

Auguste Kerckhoffs

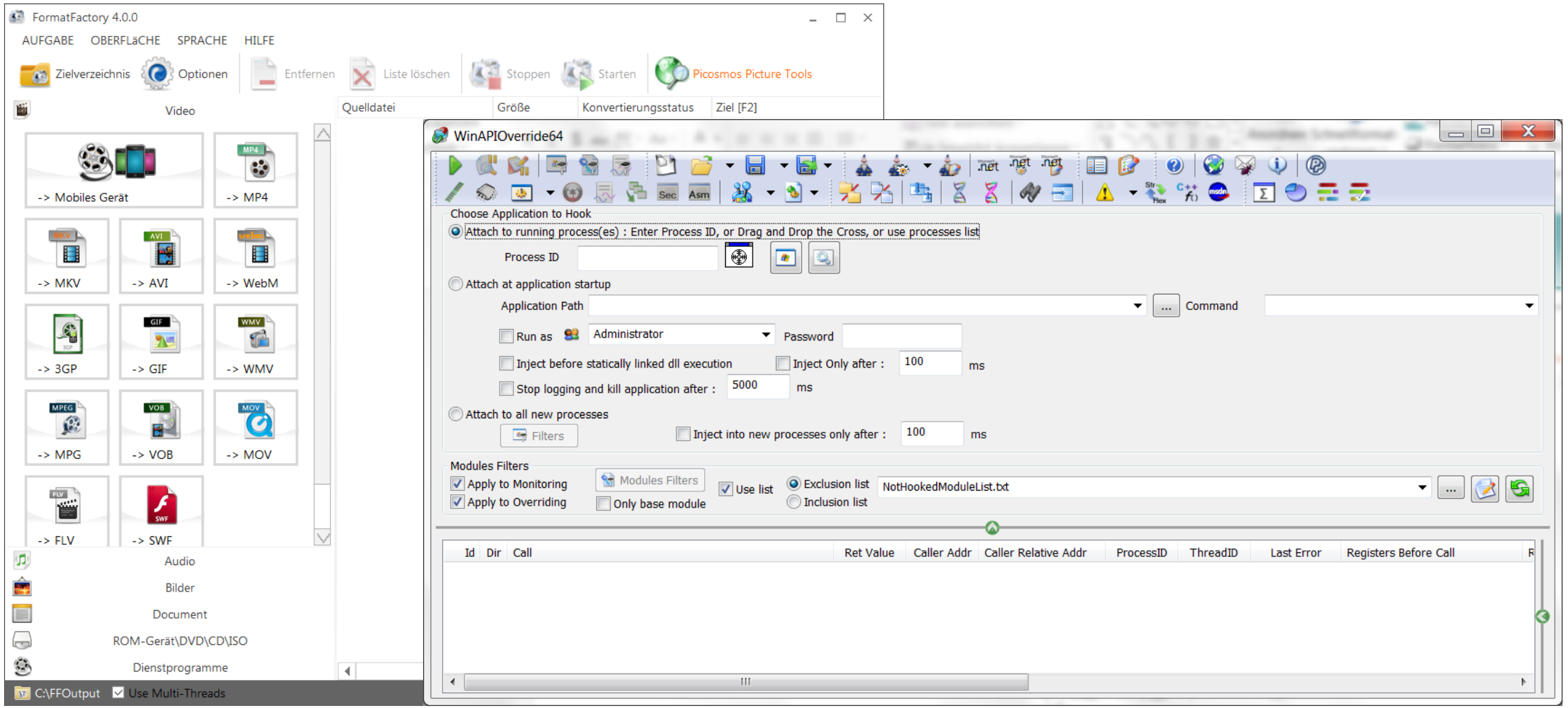
Neue Mechanismen – Mehrfache Verschlüsselung



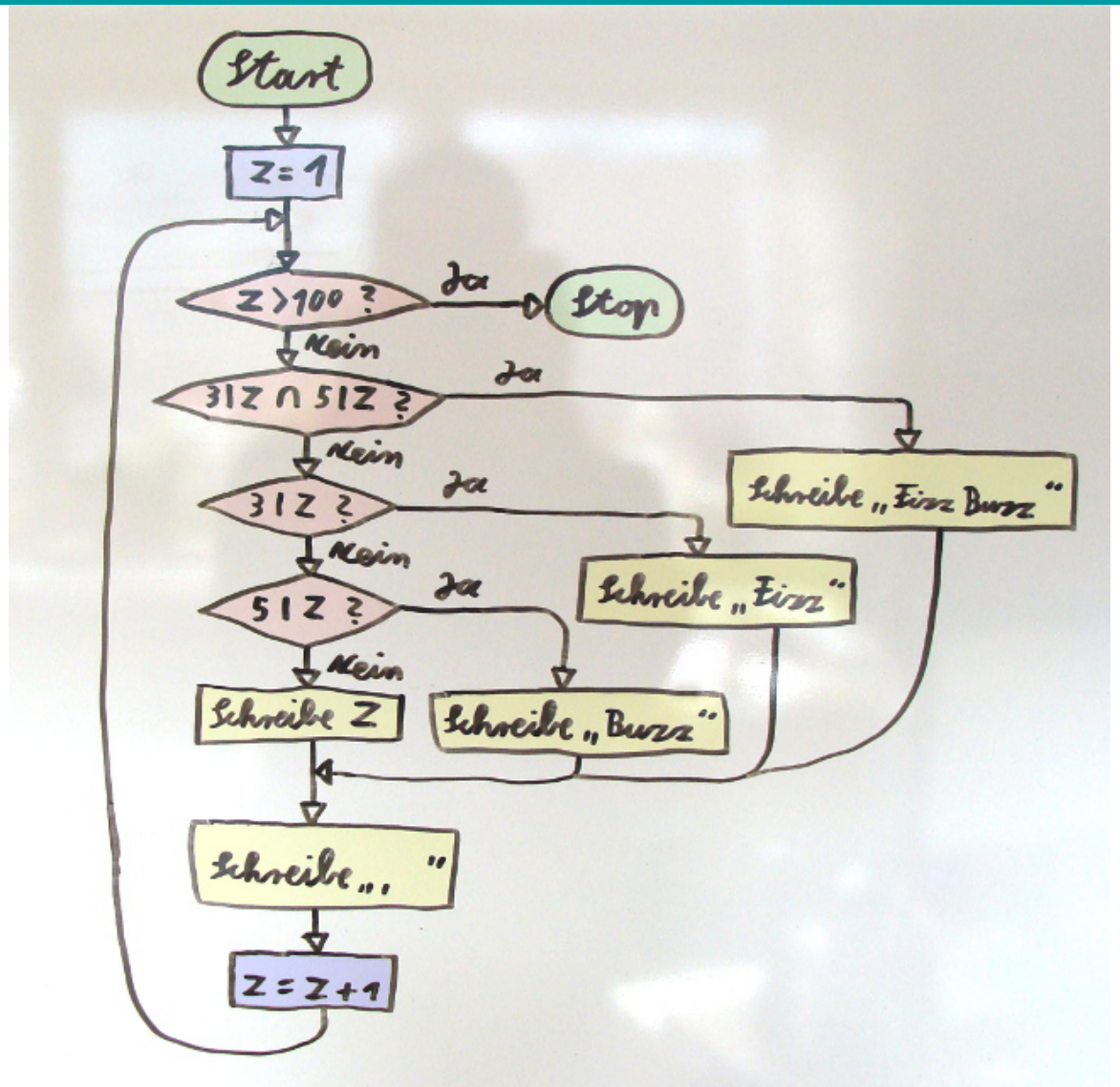
Mehrfache Verschlüsselung mit „Traps“



Fachlichkeit der Applikation



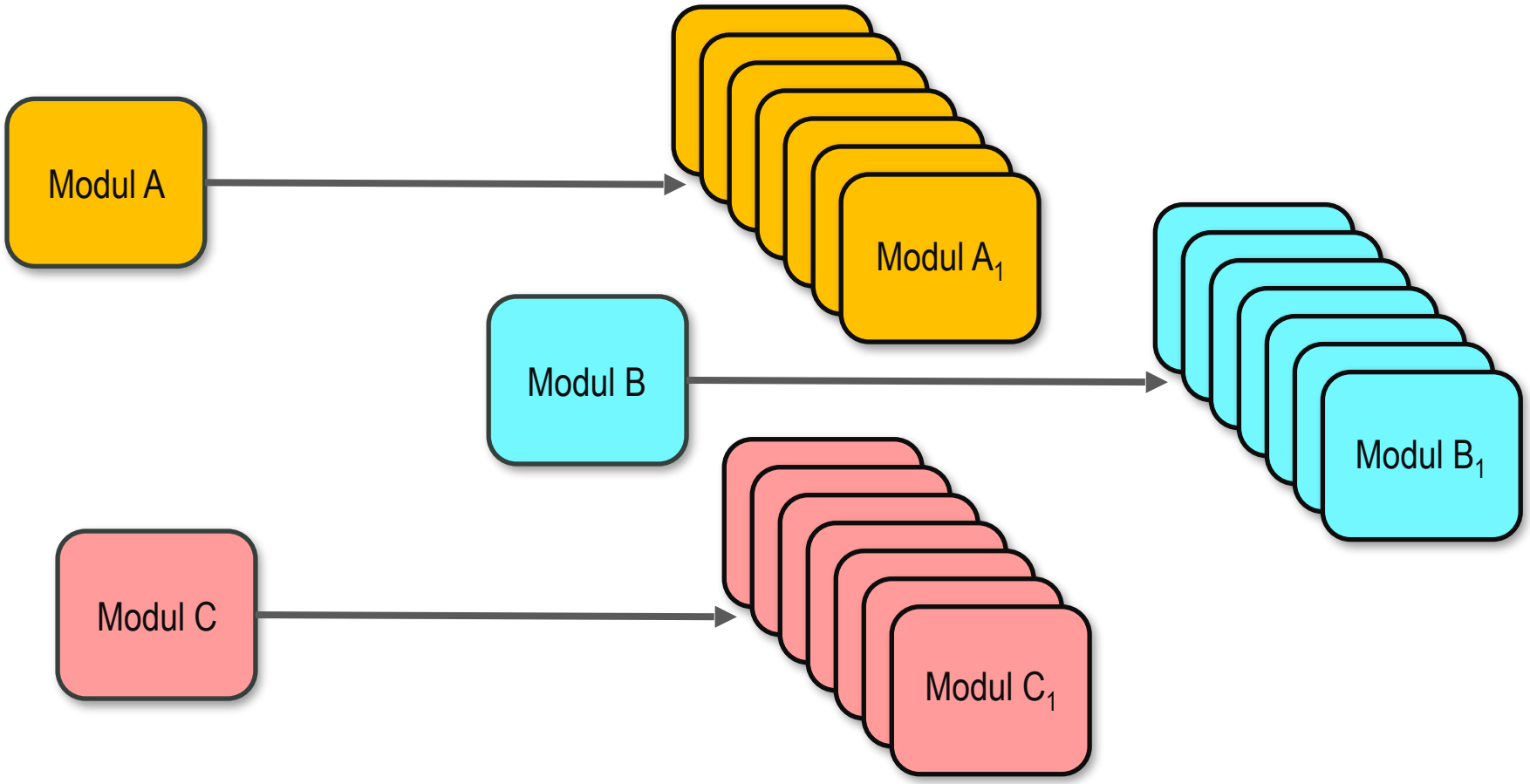
Überwachung des Programmablaufes



Überwachung des Programmablaufes

- Sicherheitsanker verwaltet den aktuellen Programmstatus
- Jeder Aufruf an den Anker gibt an von wo nach wo sich der Status ändern darf / muss
- Wildcards möglich
- Wird ein ungültiger Zustandsübergang erkannt, so wird die Lizenz gesperrt

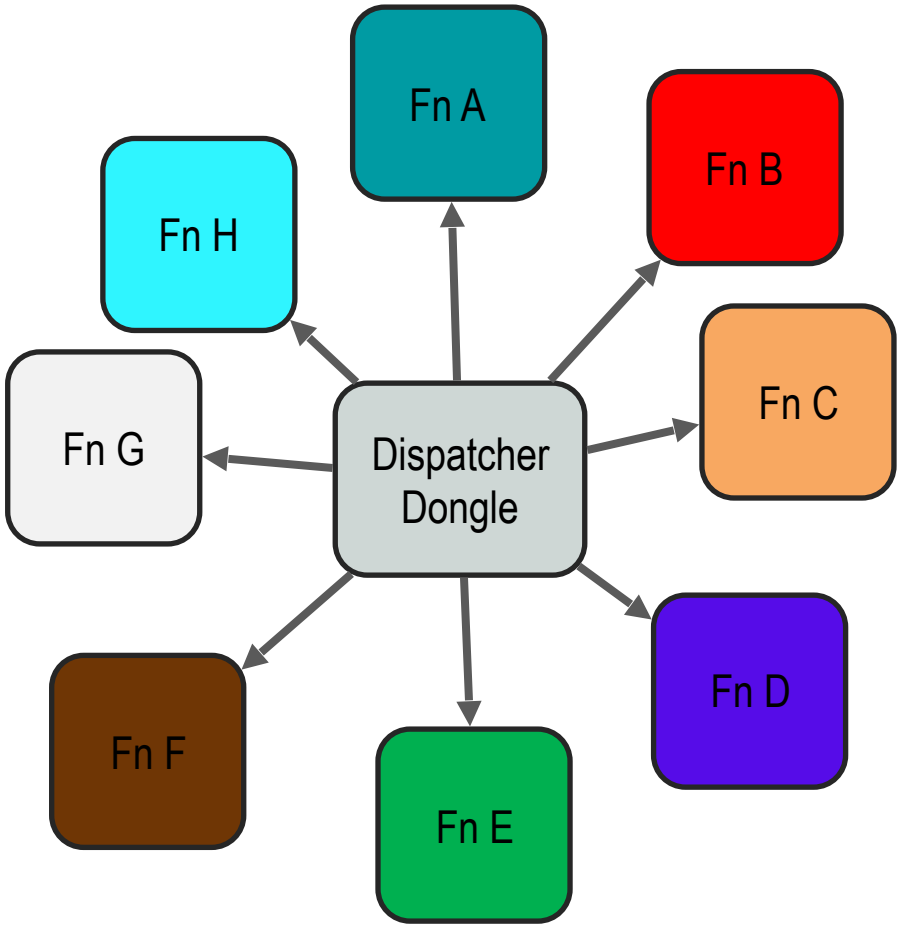
Module und Varianten



Module und Varianten

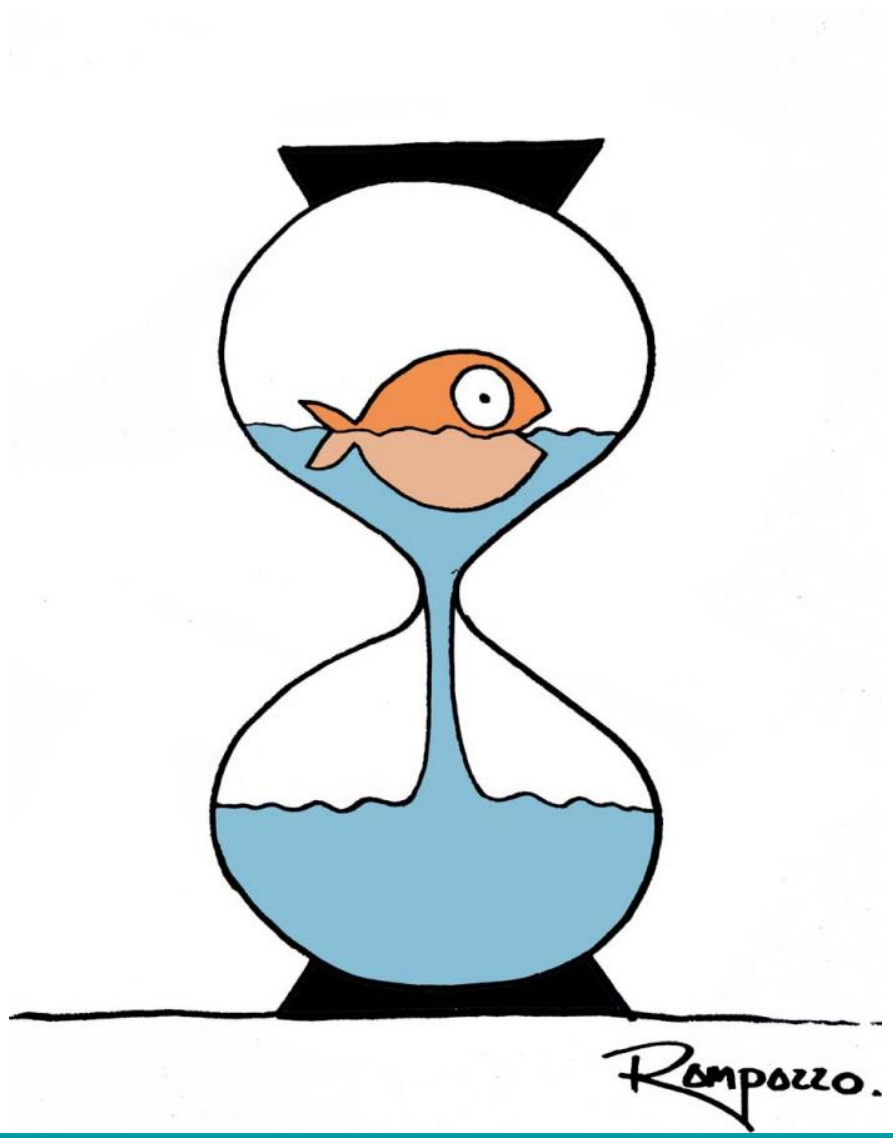
- Ersetzen von Modulen durch eine Vielzahl von Varianten
- Auswahl der Variante über Sicherheitsanker
- Funktional ist die Variante nur lokal gültig
- Die Variante überprüft ob gültige Parameter gegeben

Ablaufsteuerung



Orakel

Tempus fugit



WIBU SYSTEMS

#hackBB