

*Systematic Analysis
of Cyber-Attacks on CPS*

Evaluating Applicability of DFD-based Approach



Mark Yampolskiy, Peter Horvath, Xenofon D. Koutsoukos, Yuan Xue, Janos Sztipanovits
Institute for Software Integrated Systems (ISIS) at Vanderbilt University

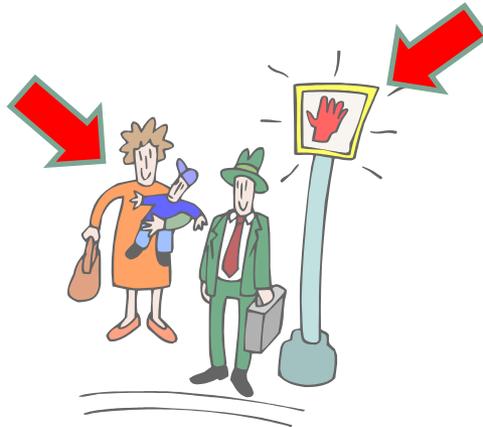
New CPS, Old Concerns...

- Old Concern: Vulnerability Assessment
 - How to identify vulnerabilities?
 - What information is important?
 - How can it be used to improve CPS?



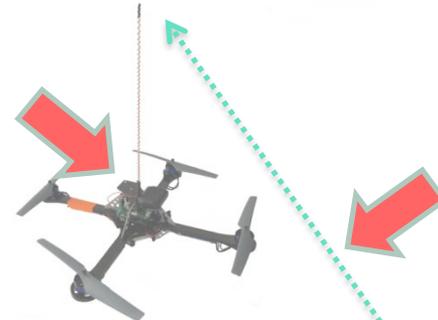
Concerns Applied to Small-Scale UC

- What Attacks are possible against ...
 - Communication Channel?
 - UAV? Base Station?
 - Operator? Environment?
- Can we Analyze this in a Systematic Manner?



Our Proposal

- What Attacks are possible against ...
 - Communication Channel?
 - UAV? Base Station?
 - Operator? Environment?
- **Can we Analyze this in a Systematic Manner?**
 - Modeling CPS [-interactions] with Extended DFD (xDFD)
 - xDFD-based Systematic Vulnerability Analysis

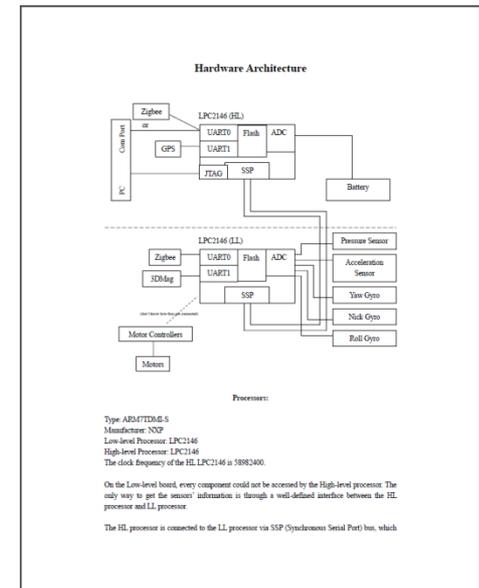


Selected UC: Quad-rotor UAV

- Comparatively detailed Documentation available
 - Modeling and Analysis of existing CPS possible
- Comparatively Simple
 - Suitable for manual in-depth Analysis
- Contains Elements common for other CPS
 - Results/Experience applicable for other CPS

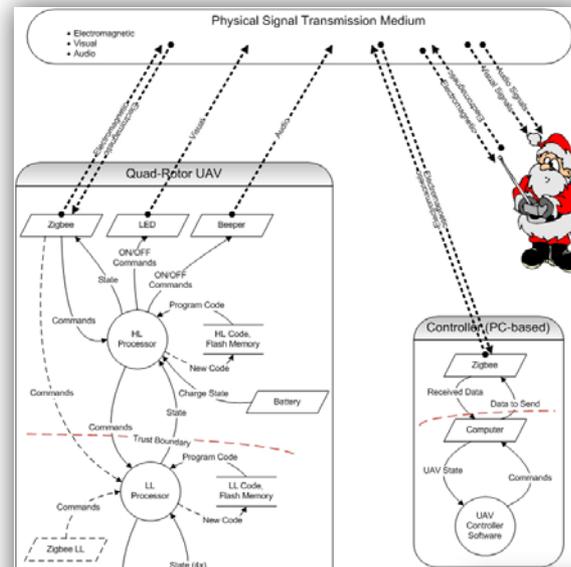


[image: <http://www.ascotec.de>]

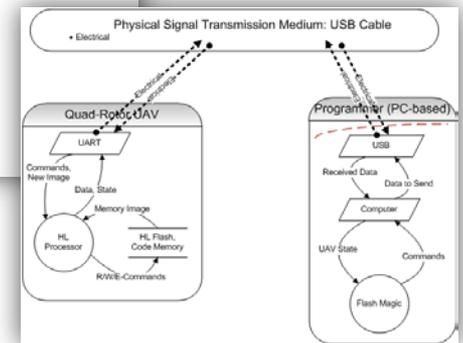


Extended Data Flow Diagrams (xDFD)

- Extended DFD contains
 - Cyber and Physical Components
 - Cyber and Physical Data Flow between Components
 - Communication Flow and Medium
- Approach: for every xDFD element analyze...
 - How it can be attacked?
 - What are consequences?

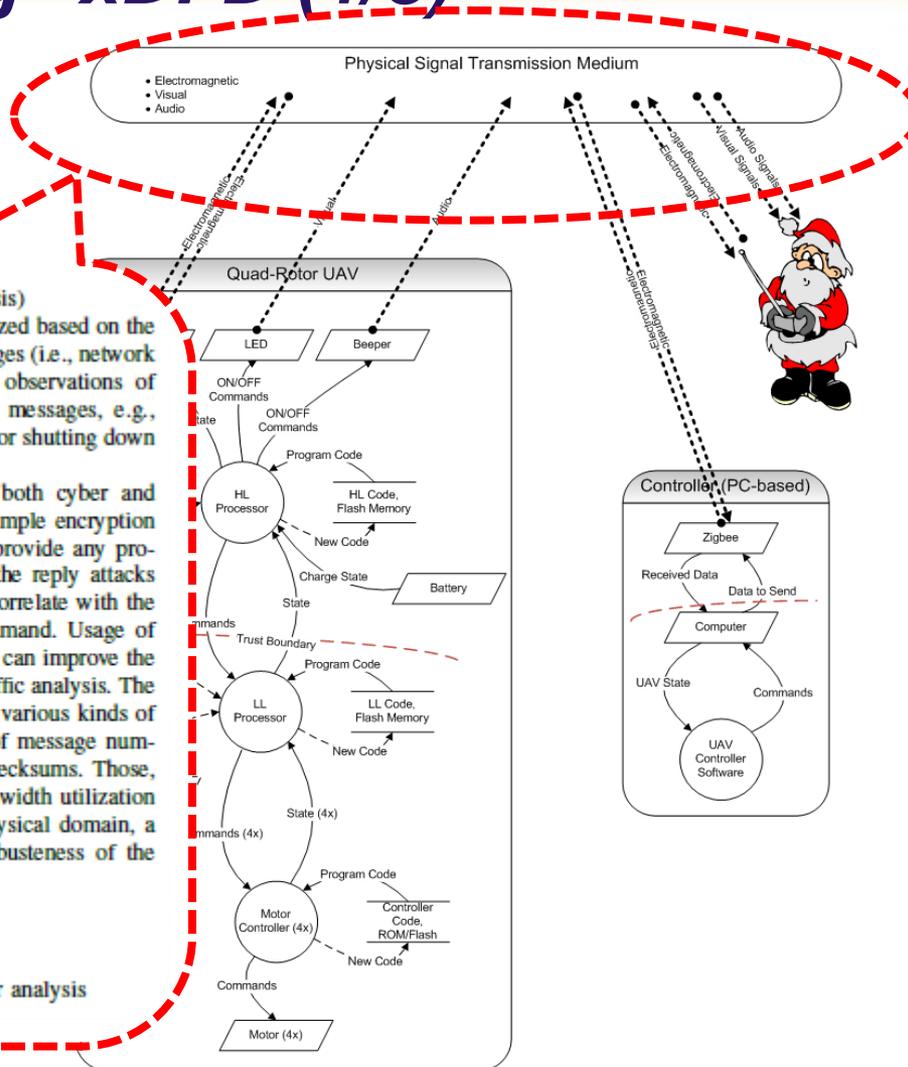


Operations



Maintenance

“Traversing” xDFD (1/3)



Attack ID: PPA (Physical - Protocol Analysis)

Description: The used protocol can be analyzed based on the correlation between eavesdropped messages (i.e., network layers in the cyber domain) with the observations of the UAV's physical reactions to these messages, e.g., increasing/decreasing of thrust, rotation, or shutting down the engine.

Defense: Countermeasures are possible in both cyber and physical domains. In cyber domain, a simple encryption of the sent commands does not really provide any protection from the protocol analysis and the reply attacks because in this case the adversary can correlate with the physical reaction on the encrypted command. Usage of cypher block chaining encryption modes can improve the robustness of the protocol against the traffic analysis. The well-established countermeasure against various kinds of record-[modify]-reply-attacks is usage of message numbers, as well as of the cryptographic checksums. Those, however, come at costs of reduced bandwidth utilization and increased CPU consumption. In physical domain, a frequency hopping can increase the robustness of the protocol to the analysis.

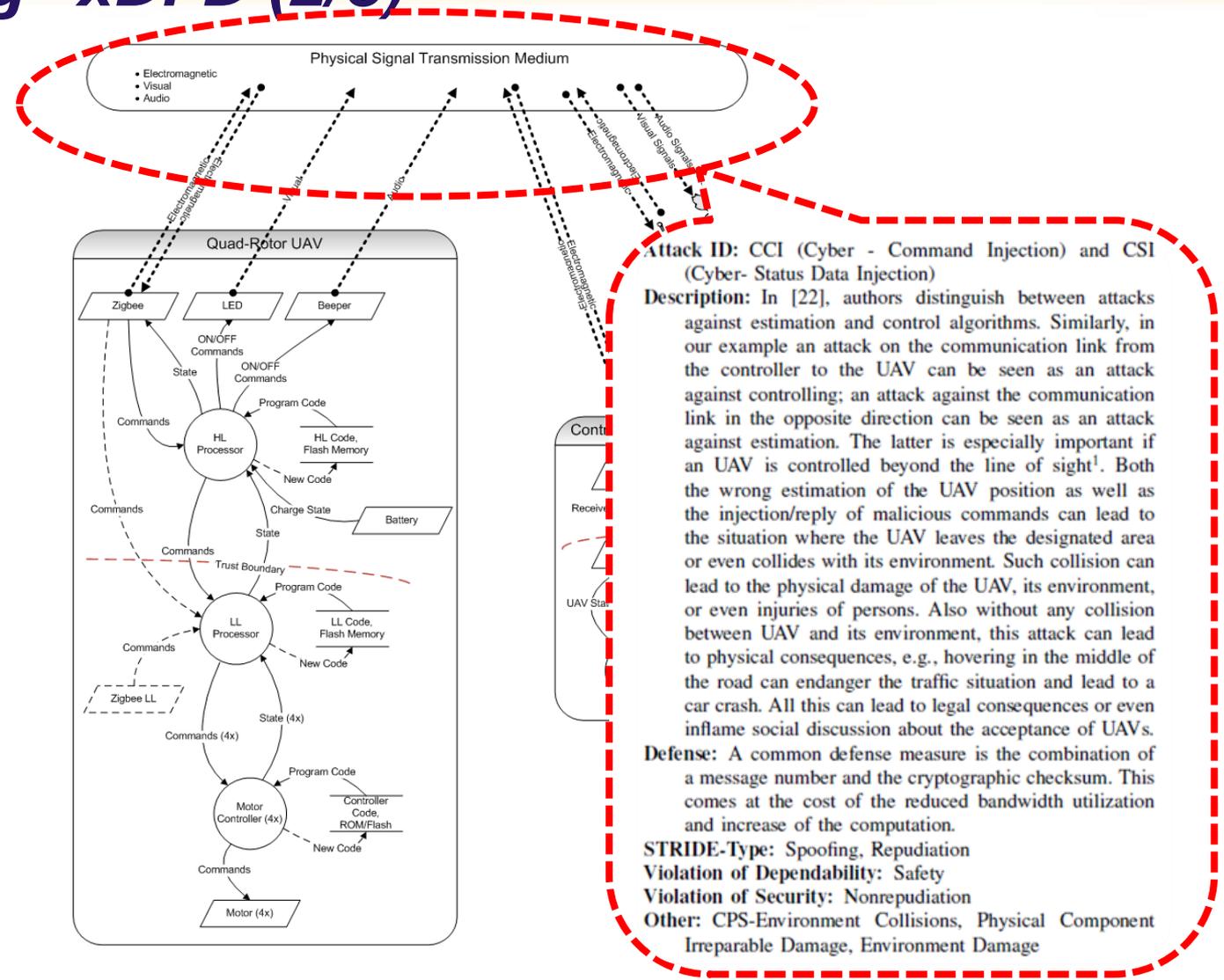
STRIDE-Type: Information Disclosure

Violation of Dependability: N/A

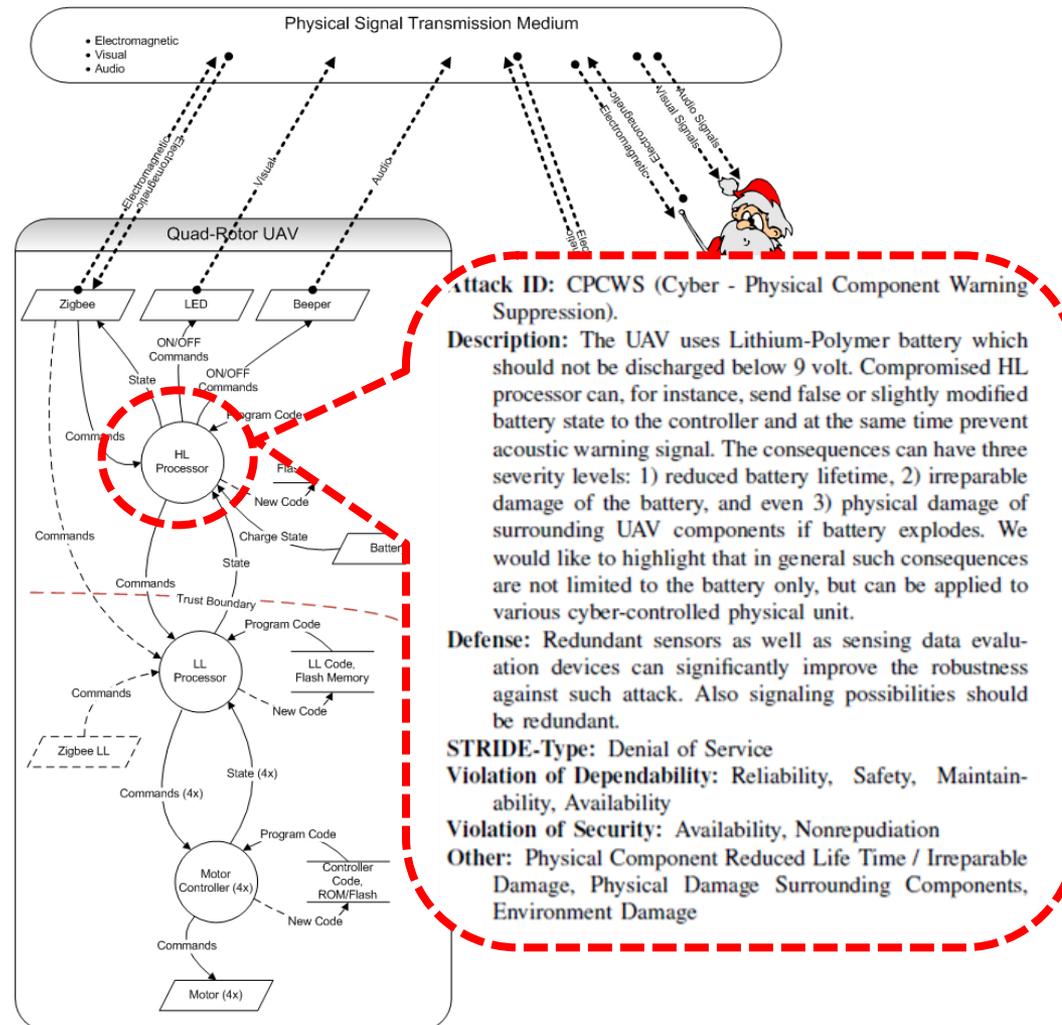
Violation of Security: Confidentiality

Other: Can use CPS' Physical Reactions for analysis

“Traversing” xDFD (2/3)



“Traversing” xDFD (3/3)



xDFD-based Analysis: Outcome

- List of Identified Attacks
 - Textual Description
 - Purpose-based Blocks
- Important Questions
 - What Information is Important/Useful?
 - Description Structure



Taxonomy &

Attack Description Language

Attack ID: CCI (Cyber - Command Injection) and CSI (Cyber- Status Data Injection)
Description: In [22], authors distinguish between attacks against estimation and control algorithms. Similarly, the communication link from the communication link from the UAV can be seen as an attack against the communication link. This attack can be seen as an attack on the communication link. This attack is especially important if the UAV is in the line of sight. Both the UAV position as well as the UAV commands can lead to a collision in the designated area. Such collision can lead to the destruction of the UAV, its environment, and the mission. Also without any collision in the designated area, hovering in the middle of the traffic situation and lead to a legal consequences or even the acceptance of UAV's mission. The combination of the cryptographic checksum. This attack leads to a high bandwidth utilization in the communication link.

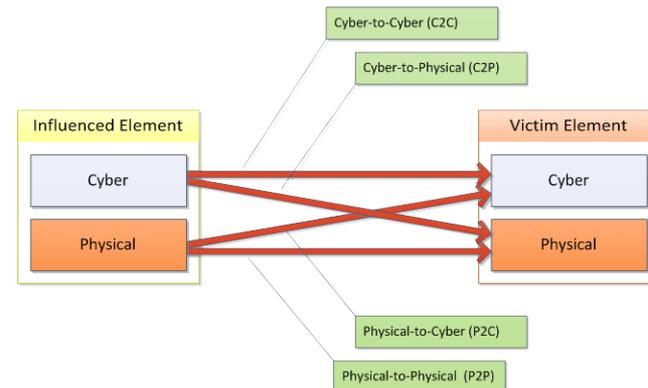
Attack ID: PPA (Physical - Protocol Analysis)
Description: The used protocol can be analyzed based on the correlation between eavesdropped messages (i.e., network layers in the cyber domain) with the observations of the UAV's physical reactions to these messages, e.g., increasing/decreasing of thrust, rotation, or shutting down the engine.
Defense: Countermeasures are possible in both cyber and physical domains. In cyber domain, a simple encryption of the sent commands does not really provide any protection from the protocol analysis and the reply attacks because in this case the adversary can correlate with the physical reaction on the encrypted command. Usage of cypher block chaining encryption modes can improve the robustness of the protocol against the traffic analysis. The well-established countermeasure against various kinds of attacks is the use of message numbers.

Attack ID: CPCWS (Cyber - Physical Component Warning Suppression).
Description: The UAV uses Lithium-Polymer battery which should not be discharged below 9 volt. Compromised HL processor can, for instance, send false or slightly modified battery state to the controller and at the same time prevent acoustic warning signal. The consequences can have three severity levels: 1) reduced battery lifetime, 2) physical damage of the battery, and even 3) physical damage of the surrounding UAV components if battery is damaged. We would like to highlight that in general such attacks are not limited to the battery only, but can be applied to various cyber-controlled physical units.
Defense: Redundant sensors as well as status monitoring devices can significantly improve the robustness against such attack. Also signaling to the controller can be redundant.
STRIDE-Type: Denial of Service
Violation of Dependability: Reliability, Integrity, Availability
Violation of Security: Availability, Non-repudiation
Other: Physical Component Reduced Lifetime, Physical Damage, Physical Damage Surrounding Environment Damage

Attack ID: CCI (Cyber - Connected Devices Injection)
Description: Currently, it is common to connect various external devices via USB interface. Even though the AscTec Hummingbird is supposed to be booted in the special mode for the flash read/write/erase operations, it might happen that the cable is connected during the UAV's HL processor code is running in normal mode and the malicious code is active. This enables all kinds of attacks via USB connection which became very common in the recent years. More complex systems which don't require such boot sequence are even more vulnerable to this kind of attack.
Defense: Automatically stop of the code execution at the CPS in the case if an external device is connected might appear to be a good idea. However, we would like to dissuade the reader from this point of view. The reason is that it can be misused by an adversary, who can gain physical access to the CPS. Therefore, the only viable option is the presence of firewall and antivirus software on the maintenance computer.
STRIDE-Type: Tampering, Elevation of Privileges
Violation of Dependability: Maintainability
Violation of Security: Authorization
Other: N/A

Taxonomy – Preliminary Results

- Two Dimensions: Distinction between...
 - Influenced Element
 - Victim Element
- Advantages: Description of...
 - Cross-Domain Effects
 - Cross-Layer Effects
 - Various Abstractions
- Taxonomy: What Missing?
 - Further Dimensions
 - Relationships between Dimensions
 - Attack Description Language



Questions?

