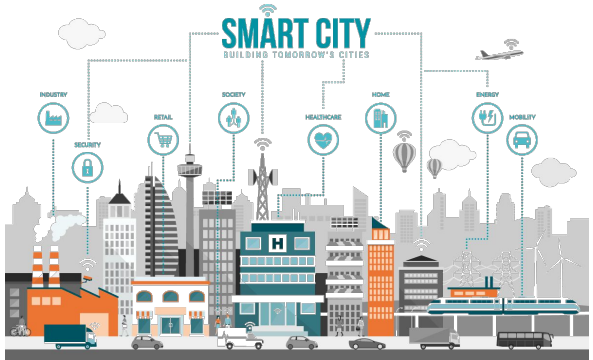
Security Analysis of Cyber-Physical Systems

Nate Olsen (nso4wg), Soneya Hossain (sh7hv), Matt Jordan (mrj3dd),Daniel Perez Lazarte(dep7sc)

Problem and Importance

- As we see the emergence of CPS systems being integrated into many fields such as Smart Cities and Smart Health. A big issue that is discussed in these complex systems is security and privacy.
    - Being that these systems are safety critical, it is important to verify there security.
- This is an important task because as these systems evolve and become more complex, it is important that we catch these vulnerabilities early and assess them rather than catching them later on when systems have become too interconnected and are already in use.



Experiment

- Bandit
  - Python Static Analysis Tool that finds security issues in Python Code.
  - Takes in Python files and develops an abstract syntax tree from the files, from this it uses the nodes in the abstract syntax tree to develop a security report.
- 21 CPS Platforms
  - Ranging from Autonomous Steering Models and Drones to IoT Systems

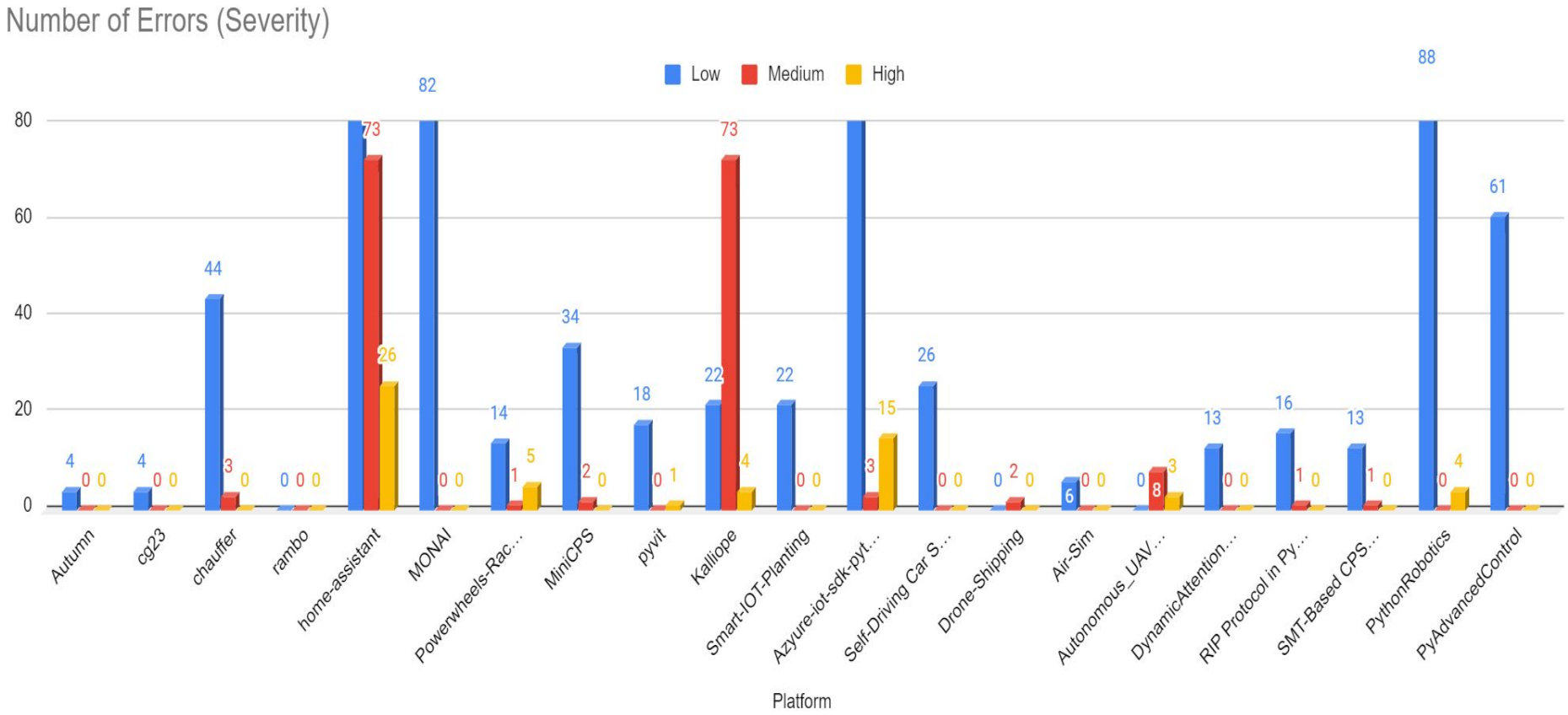
Approach

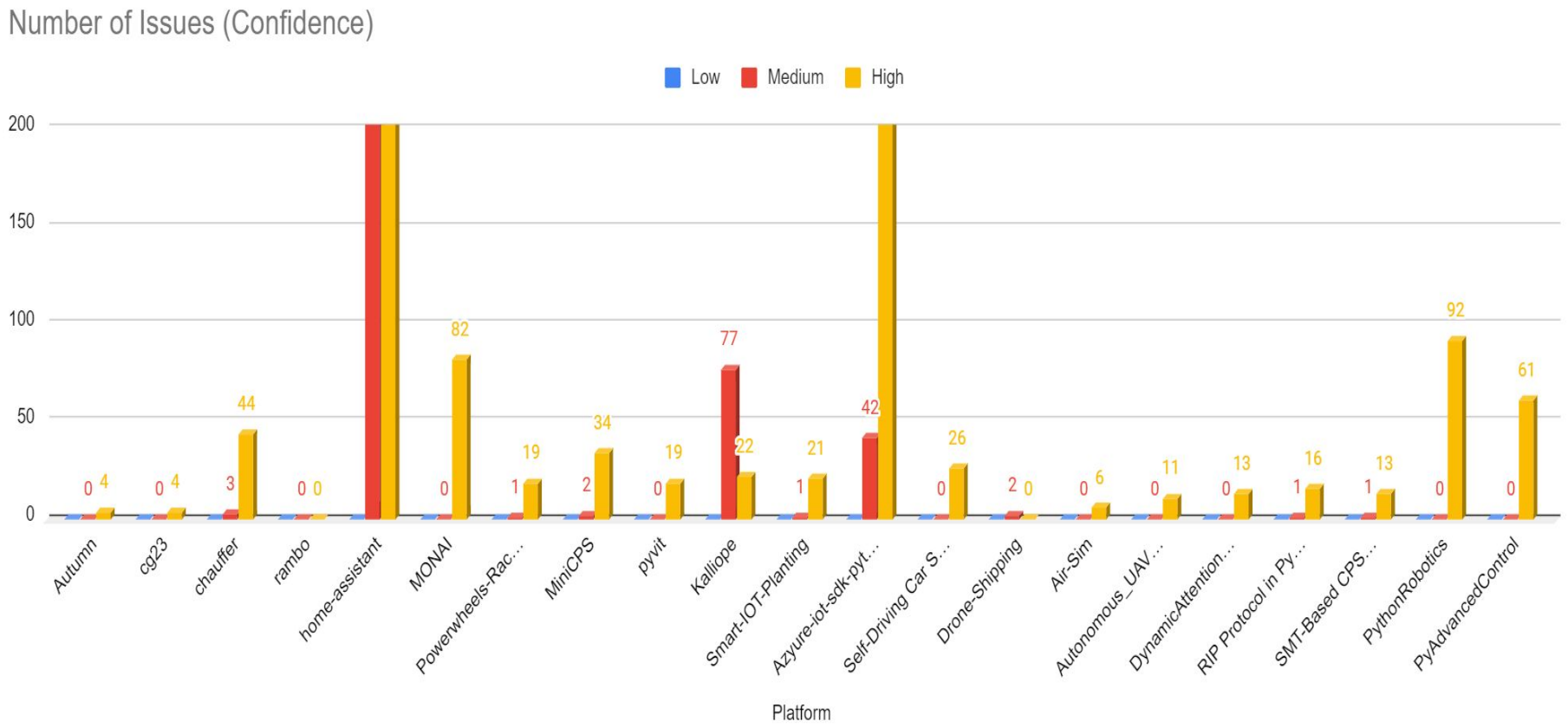
1. Researched and found popular github repositories that are/use cyber-physical systems.
2. Run the static analysis on the repositories using the bandit tool
3. Manual analysis of the reported issues
4. Report/Graph data

Experimental Results

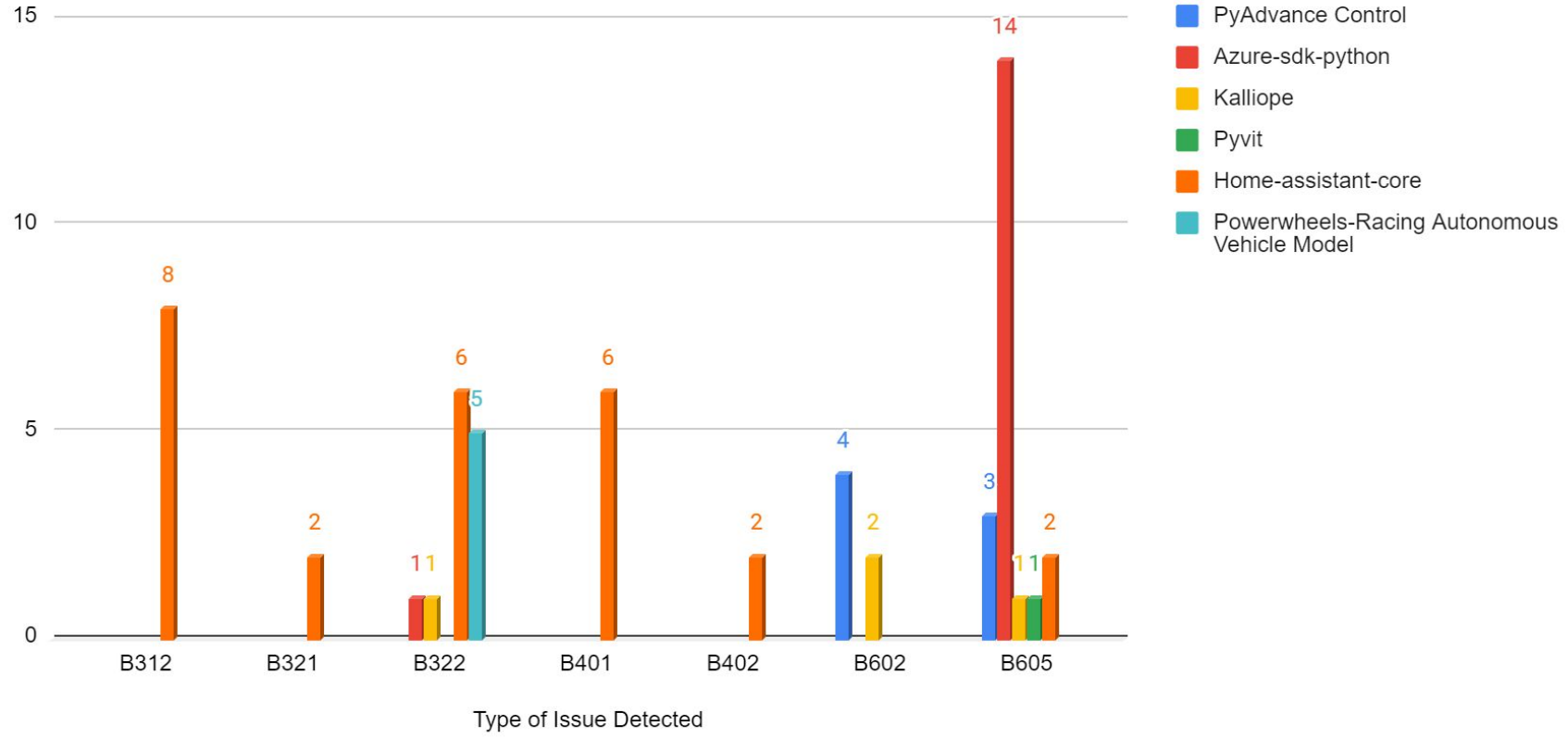
Severity	**Number of Issues**
Undefined	0
Low	34150
Medium	166
High	58

Confidence	**Number of Issues**
Undefined	0
Low	0
Medium	401
High	33973

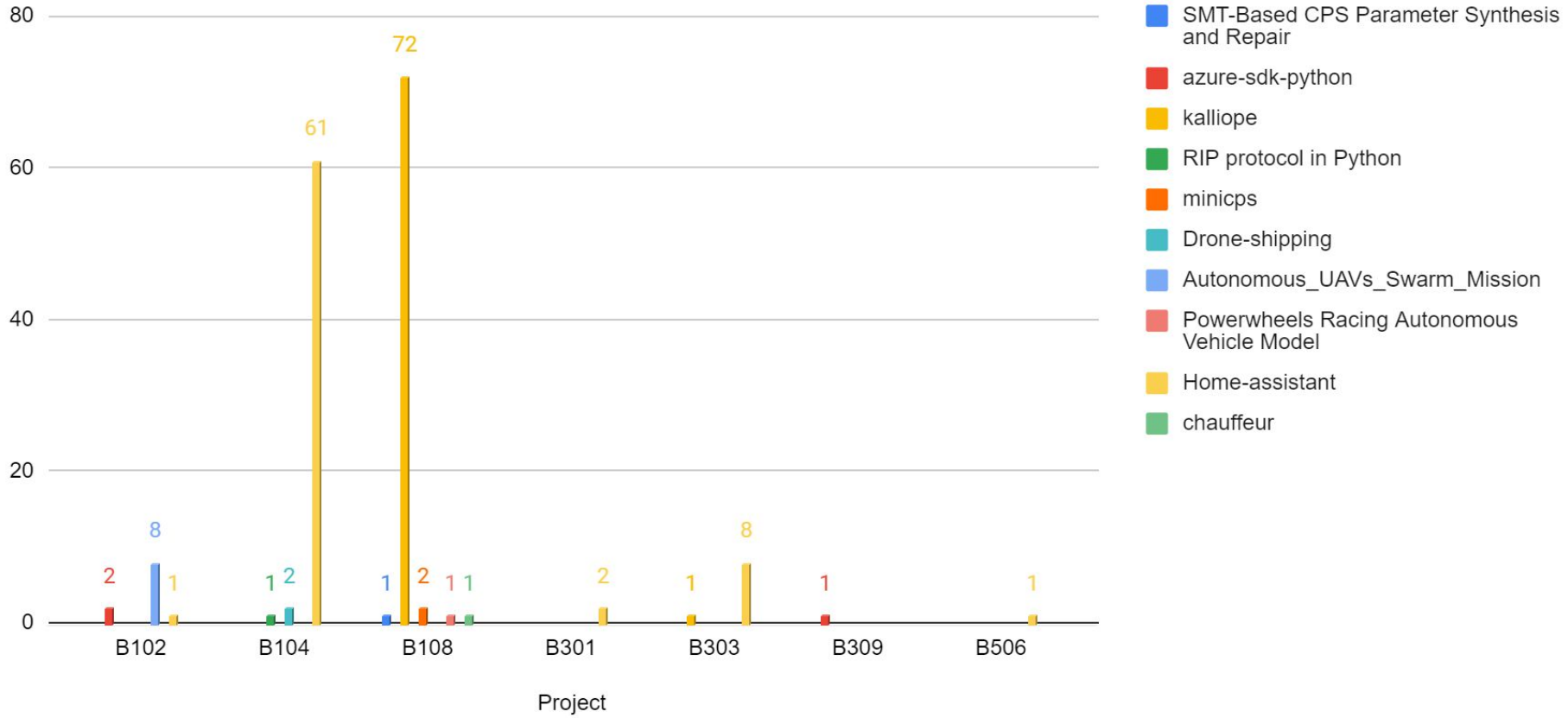

Number of Errors (Severity)
Low
Medium
High
80
60
40
20
0
4 0 0
4 0 0
44 3 0
0 0 0
73 26
82 0 0
14 1 5
34 2 0
18 0 1
22 73 4
22 0 0
3 15
26 0 0
0 2 0
6 0 0
0 8 3
13 0 0
16 1 0
13 1 0
88 0 4
61 0 0
Autumn
cg23
chauffer
rambo
home-assistant
MONAI
Powerwheels-Rac…
MiniCPS
pyvit
Kalliope
Smart-IOT-Planting
Azure-iot-sdk-pyt…
Self-Driving Car S…
Drone-Shipping
Air-Sim
Autonomous_UAV…
DynamicAttention…
RIP Protocol in Py…
SMT-Based CPS…
PythonRobotics
PyAdvancedControl
Platform


Number of Issues (Confidence)
Low
Medium
High
200
150
100
50
0
0 4
0 4
3 44
0 0
0 200
0 82
1 19
2 34
0 19
77 22
1 21
42 200
0 26
2 0
0 6
0 11
0 13
1 16
1 13
0 92
0 61
Autumn
cg23
chauffer
rambo
home-assistant
MONAI
Powerwheels-Rac…
MiniCPS
pyvit
Kalliope
Smart-IOT-Planting
Azure-iot-sdk-pyt…
Self-Driving Car S…
Drone-Shipping
Air-Sim
Autonomous_UAV…
DynamicAttention…
RIP Protocol in Py…
SMT-Based CPS…
PythonRobotics
PyAdvancedControl
Platform

Type-wise: High Issue Count:



Type-wise: Medium Issue Count:



Security Vulnerabilities

HomeAssistant
>> Issue: [B401:blacklist] A telnet-related module is being imported. Telnet is considered insecure. Use SSH or some other encrypted protocol.
Severity: High   Confidence: High

PowerWheels Racing
>> Issue: [B322:blacklist] The input method in Python 2 will read from standard input, evaluate and run the resulting string as python source code. This is similar, though in many ways worse, then using eval. On Python 2, use raw_input instead, input is safe in Python 3.
 Severity: High   Confidence: High

Kalliope
>> Issue: [B605:start_process_with_a_shell] Starting a process with a shell, possible injection detected, security issue.
   Severity: High   Confidence: High

Autonomous UAV Swarm
>> Issue: [B102:exec_used] Use of exec detected.
   Severity: Medium   Confidence: High

Python Robotics
>> Issue: [B602:subprocess_popen_with_shell_equals_true] subprocess call with shell=True identified, security issue.
Severity: High   Confidence: High

Challenges

- Issues with original Approach
- Issues with running Steering Models
- False Positives
- Hardware requirements for dynamic testing
- Less symbolic testing tool for Python
- CPS with deep learning models