# Building Secure Bharatiya Cyber Physical Drone Stack

## Key to Atmanirbharta and Global Drone Hub Vision 2030

***Sai Pattabiram****

Unmanned systems like drones are being deployed across battlefields the world over in numbers like never seen before, for a range of missions like surveillance, logistics, terrain-mapping to kinetic attack in the form of Loitering Munitions (LMs). The categories of drones being deployed covers the entire range of Nano, Micro, Small, Medium, Large and beyond, across both fixed and rotary wing. Their operational envelope covers every layer of the airspace from just being a few feet from the ground till the edge of space.

The prices of drones vary from a couple of hundred dollars to millions of dollars depending on their size and complexities of operations. The recent mass deployment of drones in the theatre of war, while unlocking a range of possibilities for defence planners, has also bought with it the need for them to raise the bar in terms of ensuring the integrity of these machines from a cyber security perspective, given the unique perspective they provide from a situational awareness point of view.

* Mr Sai Pattabiram is Managing Director at Zuppa Geo Navigation Technologies, Chennai, India.

*ISSN 0976-1004 (print); 2583-7567 (online)*

*Journal of Defence Studies, Vol. 18, No. 3, July–September 2024, pp. 250–260*

The security of the voluminous data generated by drones during regular operations is also a matter of concern, as it can compromise their operators' location apart from resulting in Denial-of-Service (DoS), data theft and other forms of cyber attacks on the drones operating systems.

This commentary attempts to study the various layers of an Unmanned Aerial Vehicle (UAV), usually referred to as a drone, the Cyber Physical System (CPS) and identify the vulnerabilities to various forms of attack both at the Control and Information Layers. The commentary also suggests development and deployment of vulnerability mitigation strategies by way of the 'Bharatiya Cyber Physical Drone Stack' (BCPDS) and goes on to highlight the long-term benefits both in terms of domestic consumption and export potential of BCPDS thereby propelling India's vision of becoming the Global Drone Hub by 2030.

It also intends to draw the attention of policy-makers to look beyond the visible physical device to cyber physical layer where the opportunities and the threats to national security lie.

## Background

The recent wars starting with the Azerbaijan-Armenia war through the ongoing Russia–Ukraine, Israel–Hamas conflicts to the Houthi Red Sea attacks, unmanned systems, more specifically drones, are proving to be major game-changers by shifting the asymmetry of warfare for the first time from being cost-escalative to de-escalative as a result of the usage of COTS (Commercial Off The Shelf) components and solutions.

As these wars are progressing and as more and more drones are being deployed, realisation is growing among policy-makers and military strategists that drones are here to stay and are in fact Cyber Physical Systems (CPS), hence all the typical vulnerabilities associated with such systems are beginning to manifest themselves in the drones being used by them.[1]

Indian manufactured drones used by the defence forces along the frontline have been hacked and compromised in the recent past, as a result of the rampant use of Open Source Cyber Physical Stacks leading to introspection at the highest levels within the Ministry of Defence. Therefore, there is a very visible push for indigenisation resulting in modifications to the provisions of Defence Acquisition Procedure 2020 (DAP 2020) by the Defence Acquisition Council (DAC).[2]

Further to maximising indigenisation, the DAC has accorded approval for a major amendment in DAP 2020. It has been decided that henceforth,

in all categories of procurement cases, minimum 50 per cent of indigenous content shall be used in the form of material, components and software that are manufactured in India.

## Geo-political Shift in Global Defence Drone Supply Chain

With Iran, Turkey and China emerging as drone powers globally, India needs to evolve and develop its own competencies rapidly. India's predicament is further compounded by the fact that both its key defence equipment suppliers—Russia and Israel—are at war with the former procuring drones from Iran and China to strengthen its war efforts.

Further, the Indian drone ecosystem's dependency on China as the origin of its drone supply chain coupled with the rampant use of open source Cyber Physical Stacks among defence drone manufacturers in India poses a huge risk that needs to be mitigated immediately.[3]

The immediate priority for India from a national security perspective is to develop indigenous capabilities for development, manufacturing and deployment of a secure indigenous Cyber Physical Stack. It is therefore important for policy-makers across India's drone ecosystem to recognise and accept drones as 'Cyber Physical Systems' and focus on mitigating their vulnerabilities by building a secure 'Bharatiya Cyber Physical Drone Stack'.

## Cyber Physical Systems

Cyber Physical Systems employ electronic computational power to monitor and control physical devices using real-time sensory inputs through a network of actuators by deploying a continuous feedback loop.

Cyber Physical Systems deploy an embedded real-time loop that involves continuous sensing, computing, actuating and communicating a physical systems overall performance, safety and reliability.

The autopilot of a drone is Reactive Computer that interacts with the environment through running continuous input and output closed loops to electronically execute multiple tasks that control the drone's altitude, position, heading, navigation concurrently and simultaneously in real-time.

Real-time monitoring of the operational performance of this Reactive Computer the autopilot onboard the drone is achieved through it being connected wirelessly to the Ground Control Station Software (GCS).

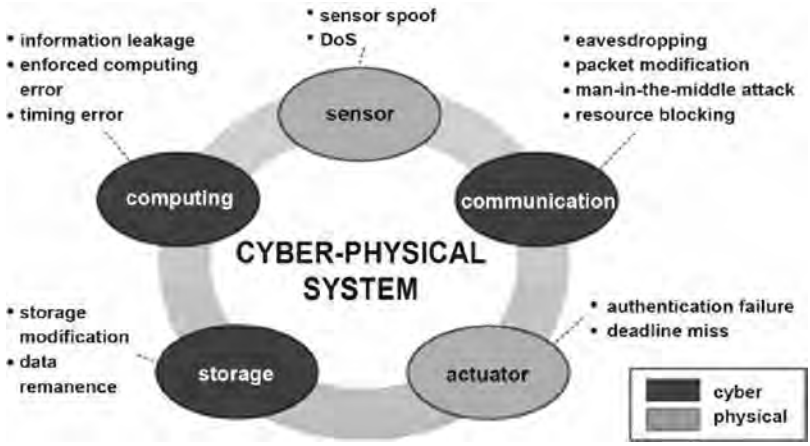


**Figure 1** Vulnerability of Cyber Physical Systems

*Source*: Deepika Sharma and Arvind Selwal, 'An Intelligent Approach for Fingerprint Presentation Attack Detection Using Ensemble Learning with Improved Local Image Features', *Multimedia Tools and Applications*, Vol. 81, 2022, pp. 1–33, available at https://link.springer.com/article/10.1007/s11042-021-11254-8.

This complete close loop electronic control and communication suite is that sub-system on a drone that enables it to be operated remotely in an unmanned mode, hence is the most critical part of the drone during operations. This suite is what makes the drone a Cyber Physical System (CPS).

Since this electronic suite controls the drone's operations, it logically becomes the target for hacking, remote commandeering, DoS and other such attacks by enemy forces to restrict an opponent's defences.

Majority of drone applications involve continuous generation and transmission of sensitive high-resolution geo-tagged image/video from the drone over wireless channels to the GCS as well as other locations over mobile networks either directly or indirectly, thus rendering the communication system most vulnerable to hacking and data theft.

Drones as Cyber Physical Systems are therefore quite vulnerable to attacks both at the physical and cyber levels, as shown in Figure 1.[4]

## Origins of Globally Adopted Vulnerable Open Source Drone Tech

The DIY drones forum[5] based out of the US is the origin of open source flight control technology for drones with the development of 'Ardupilot' that

subsequently evolved into 'Pixhawk Cube' which in turn is being replicated and commercially produced as Cube Orange, Cube Pilot, X7 Pro and a myriad other clones manufactured by Chinese companies.

The open source community of thousands of developers who developed the Ardupilot also developed its Cyber Physical Stack including its PCB schematic, firmware, MavLink command and control protocol as well as the QGCS software, all of which are available on the open-source repositories like GIT HUB:

1. Pixhawk Hardware[6]
2. Pixhawk Firmware[7]
3. Ardupilot Autopilot[8]
4. Mavlink Control and Command Protocol[9]
5. Q GCS Ground Control Software[10]

This open source initiative was never intended for commercial and professional use, but given the ready availability of this core drone technology at a fraction of the cost of available secure proprietary options like Micropilot, UAV Navigation's Vector Embition , Microkopter, etc., while offering higher flexibility led to it being rapidly commercialised and evolved as a standard among drone assemblers across the world, including practically every Indian drone developer and manufacturer (assembler).

The fact that open source Cyber Physical Stacks satisfied the immediate need of end-users led to manufacturers quickly adopting them and scaling revenues.

The vulnerability of such autopilots when used in defence equipment doesn't seem to have been considered by either defence policy-makers nor the manufacturers till the time Russia–Ukraine conflict started, when Commercial Off The Shelf (COTS) drones and components started being mass deployed by Ukraine.

It is only when these drones started failing to deliver the desired outcomes to end-users, and in fact started turning into threats under actual operational conditions due to vulnerabilities at the Cyber Physical level, did the stakeholders in defence wake up to the need to evaluate their security layers.[11]

Indian Army personnel faced a jarring and demoralising awakening around mid-2022 and more recently on 23 August 2024, when drones being used by them started falling prey to hackers from across the border on both the eastern and western frontier and they realised that their adversary was in fact a prime supplier of the Cyber Physical Drone Stack being used on their drones.

## Identifying Vulnerabilities at the Cyber Physical Level in Drones

Having accepted drones to be Cyber Physical Systems, the next logical step is to identify the Cyber Physical Stack within a drone to fully appreciate its vulnerabilities and arrive at strategies to mitigate them.


**Figure 2** Cyber Physical Drone Stack

The vulnerability of a Cyber Physical System exists at two levels (as shown in Figure 2):

- *Control Vulnerability*: Involves any threats to the operator's ability to safely and confidently operate the drone. This vulnerability is particularly important and relevant today with the advent of Loitering Munitions (LMs) given that a vulnerable LM is as much a threat as it is an asset.
- *Information Vulnerability*: Involves threats to the security, integrity, authenticity, storage of the voluminous data (high-resolution geo-tagged imagery) acquired and transmitted by the drone during its operations.

In the case of drones especially used in national security roles, Control Vulnerability should take precedence over Information Vulnerability as any compromise in the control integrity of the equipment can result in catastrophic outcomes directly impacting both the national security and the safety of its operator.[12]

With the large-scale deployment of drones employing open source autopilots across the globe, the most common form of drone hacking adopted is the use of a parallel GCS to access their autopilots and trigger

commands that compromise the drones' integrity through their open source Firmware and command and control protocols (Figure 3).[13]

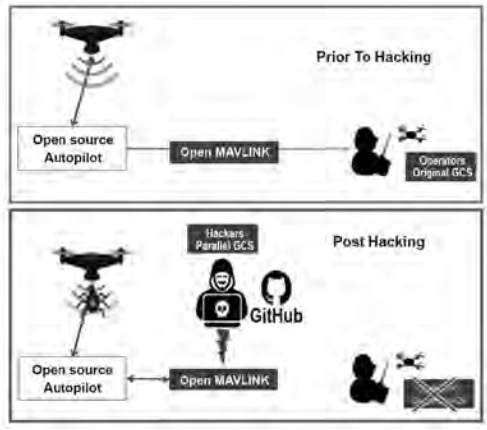


**Figure 3** Control Vulnerability

Commands that can be triggered by the Parallel GCS can largely be classified as DoS attacks, some of which are listed below.

*Locational Data Modification Commands (GPS Spoofing)*
- Change Home point
- Change Route/Flight plan
- Disable GPS

*False Data Modification Commands*
- Fuzzing hardware by overload of data leading to system crash
- Disabling Original Communication link
- Disabling failsafe commands through data modification
- Blacklisting original operators command link

## Information Vulnerability

Wireless communication channels are normally the first line of attack for gaining access to a drone because of its heavy reliance on such modes of communication for its routine operations.

Two-way wireless data radios are extensively employed by drones as downlinks for information generated on the drone and as uplinks for commands transmitted to the drones from the GCS.

- *Wireless Jamming*: Majority of the drones world over use Citizen Band Open frequencies of 2.4 G and 5.8 G, as a consequence are vulnerable to jamming, hacking and interference.
- *Communication Protocols Vulnerabilities*: Widely used open source communication protocols like MavLink amplify the information vulnerabilities by facilitating easy access and visibility to the drones operational data as well as creating channels for forwarding of that data to unauthorised locations.

**Table 1** Mapping Vulnerabilities of Drones

| Sr No | Drone Sub System | Components | Vulnerability |
|---|---|---|---|
| 1 | **Cyber Physical Stack** (***Electronics***) | Autopilot, Control Protocol, GCS | **Cyber Security Risk**: Hacking & Remote Commandeering |
| 2 | **Wireless Communication** (***Electronics***) | Radio link – 2-way telemetry, remote controller | **Cyber Security & Data Theft Risk** access to Cyber Physical Stack, locational & operating data (Potential Gateway for Take Over/Hacking Risk) |
| 3 | **Payload** (***Electronics***) | Cameras, Lidars, Radars | **Cyber Security & Data Theft Risk** access to Cyber Physical Stack, locational & operating data in case integrated wireless video systems used in micro & small drones |
| 4 | **Propulsion System** (*Electrical & **Electronics)*** | Electric Motor, Electronic Speed Controller, Propeller, Engine | **Supply Chain Risk (Hurdles in Wars or Large Orders)**: Neodymium magnets used in motors and MOSFETS used in speed controllers |
| 5 | **Airframe** (*Mechanical*) | Carbon Fibre Tubes, Cloth, Sheets, Composite frames, moulded thermoplastics & other mechanicals ….. | **Limited Risk/Unwarranted Dependencies** Alternative materials and manufacturing processes like composites, injection moulding, 3D printing, etc., can be used as replacements |

## Mitigation of Vulnerabilities in Drones as Cyber Physical Systems

The underlying philosophy for defining strategies for mitigation of vulnerabilities for drones should be 'Denial of Access' from the whole Cyber Physical System perspective and not independently securing each layer of the system.

Denial of Access can be applied to either or both types of vulnerabilities namely:

- Control
- Information

Control vulnerabilities should be accorded highest priority as far as Denial of Access from applications involving national security.

India's vulnerability mitigation strategy for drones has to be by way of Developing Qualitative Requirements (QRs) that are based on established standards for testing and certification of component sub-systems and manufacturing processes by certifying bodies within India (Table 2).

**Table 2** Established standards for testing and certification of component sub-systems and manufacturing processes

| Subsystem Type | Components | Testing / Certification Standard | Testing Labs |
|---|---|---|---|
| Electronic Hardware | *Autopilot , Power Module, Electronic Speed Controller ( ESC ) Wireless radio and telemetry modules, Electronic and electro optic payload* | IPC 6012 Class 3 | Process Certification Like ISO 9001 |
| | | IPC-A-610 ( RoHS compliant ) | |
| Software ( Code ) | Firmwares for all hardware, Command control & communication protocols, Ground Control Software (GCS) and any other code elements existing in the system | Cyber Security Std OWASP 4. Level 3 | ERTL North https://www.stqc.gov.in/ertlnorth |
| Motor Subsystem (BLDC Motors) | Magnets (Neodymium) | IEC 60034-1 | NABL / IPC |
| | Copper Winding | IPC 2221/IEC60034-1 | |
| | Aluminum Housing | IEC 60529 (IP Rating) | |
| | 0.2mm Silicon Steel | IEC 60034-1 | |
| | Rotor/Stator Design | IPC 2221 | |
| Batteries | Lithium Battery Pack | BIS. IS 16046 (Part 2): 2018/ IEC 62133-2:2017 | |
| Mechanical and Aero structures, Propeller ... | CFRP/Carbon Fiber | ISO 10303-242 (Structural Integrity) | |
| | Machining & Assembly | IPC610 | |
| | Coating & Erosion Protection | ASTMB117 | |
| Manufacturing Process Certification | Organisational Process Quality Assurance | ISO 9001 2015 | NABL Accredited Certification Body |

## Mitigation of Vulnerabilities to a Drone's Cyber Physical Layer: Key to the National Global Drone Hub Vision 2030

For the first time in history, drones are being deployed in large numbers across all the recent conflicts and wars currently underway globally. Such a scale of deployment of drones has never been witnessed in the past.

With drones being developed, produced and deployed effectively in attack roles as LMs across a range of sizes starting from the sub-2 kg micro FPV drones to MALE UCAVs like Bayraktars and medium category Iranian Shahed 136 and Russian Lancet's playing a telling role in these wars, the demand for such systems is going to exponentially scale going forward.

This is bound to fuel a significant jump in demand for Zero Trust Access Denied proven Cyber Physical Drone Stacks, given the inherent need for these types of drones, especially LMs.

India's reputation as a responsible, trusted technology partner in the IT sector can be leveraged for gaining strong market acceptance for the Bharatiya stack. Additionally, given the fact that the use of the Ardupilot open source stack has been rampant across the world due to its own internal demand for 'Access Denied Zero Trust Cyber Physical Drone Stacks', India can leverage economies of scale to evolve into a supplier of trusted proven such drone stacks to the global drone industry. This will also provide opportunities for Indian manufactures to export their drones globally, considering the fact that they will be built around the proven Bharatiya Cyber Physical Drone Stack.

## Conclusion

In conclusion, the development, deployment and implementation of a Bharatiya Cyber Physical Drone Stack based on testable, certifiable, verifiable international standards will ensure that drones manufactured in India will offer both its domestic as well as international customers secure non-Chinese alternatives thereby fast-tracking India's vision of evolving into a global drone hub by 2030.

## Notes

1. Jean-Paul A. Yaacoub, Ola Salman, Hassan N. Noura, Nesrine Kaaniche, Ali Chehab, Mohamad Malli, 'Cyber-Physical Systems Security: Limitations, Issues and Future Trends', *Microprocessors and Microsystems*, Vol. 77, 2020, available at https://www.sciencedirect.com/science/article/pii/S0141933120303689?via%3Dihub, accessed on 19 September 2024.

2. 'Defence Acquisition Council Approves Capital Acquisition Proposals Worth Rs 2.23 lakh crore to Enhance the Operational Capabilities of the Armed Forces', Press Information Bureau, Ministry of Defence, Government of India, 30 November 2023, available at https://pib.gov.in/PressReleasePage.aspx?PRID=1981135.
3. Jean-Paul A. Yaacoub, Ola Salman, Hassan N. Noura, Nesrine Kaaniche, Ali Chehab, Mohamad Malli, 'Cyber-Physical Systems Security: Limitations, Issues and Future Trends', n. 1.
4. Deepika Sharma and Arvind Selwal, 'An Intelligent Approach for Fingerprint Presentation Attack Detection Using Ensemble Learning with Improved Local Image Features', *Multimedia Tools and Applications*, Vol. 81, 2022, pp. 1–33, available at https://link.springer.com/article/10.1007/s11042-021-11254-8.
5. See https://diydrones.com
6. Pixhawk Hardware: https://github.com/pixhawk/Hardware
7. Pixhawk Firmware: https://github.com/PX4
8. Ardupilot Autopilot: https://github.com/ArduPilot/ardupilot
9. Mavlink Control and Command protocol: https://github.com/mavlink
10. GCS Ground control software: https://github.com/mavlink/qgroundcontrol
11. Deepika Sharma and Arvind Selwal, 'An Intelligent Approach for Fingerprint Presentation Attack Detection Using Ensemble Learning with Improved Local Image Features', n. 4.
12. A. Shafique, A. Mehmood and M. Elhadef, 'Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles', in *IEEE Access*, Vol. 9, pp. 46927–46948, 2021, available at https://ieeexplore.ieee.org/abstract/document/9380688.
13. Ibid.