Apps for the F-35

Has Israel set a precedent?

U.S. AIR FORCE

Eric Tegler Washington

Israel has announced it will equip the F-35s it starts receiving this December with its own command, control, communications and computing (C4) system. The software, produced by Israel Aerospace Industries (IAI), is an upgrade of an existing C4 system the Israeli air force flies on its F-15 and F-16s.

By adapting proprietary software to the F-35, Israel has leveraged the strike fighter's open-architecture software design long touted by Lockheed Martin and the Joint Program Office (JPO). In effect, IAI has written the first "app" for the F-35 and, arguably, set a precedent for F-35 software independence.

"Imagine putting some new applications on your mobile phone," says Benni Cohen, general manager of IAI's Lahav Division. "It is not difficult. You can do it without touching the mission systems."

His metaphor is a useful one. While the specifics are not exactly the same, think of the F-35's software backbone as an "operating system" like Apple's iOS and IAI's C4 software, which sits atop it as an "application." With the right application interface, developers can write new apps for the F-35, adding new functionality.

"Yes it is straightforward to tap into that [F-35 system] data and build upon that information to make new applications or add new functionality that benefits the overall fight," says John Clark, director of mission systems and software at Lockheed Martin's Skunk Works, which he adds, has worked with the U.S. Air Force to craft a protocol for F-35 software called Open Mission Systems (OMS).

By standardizing the process for moving data around the F-35's open architecture backbone, OMS fosters rapid software development and mission systems integration. But the protocol was not created just to speed software development internally. Its complimentary purpose is to give the U.S. a measure of control over what software and functionality is developed for the Joint Strike Fighter (JSF).

By working independently, Israel may have changed the game. "The folks at IAI doing that will certainly bring up [the issue] as more partner nations have the desire to do that," says Clark. "But it is also a double-edged sword. They do not get the benefits of the rest of the ecosystem the F-35 has by deviating."

Clark points out the F-35 program has a defined joint standards process intended to align partner nations with common enterprise support across the board, for software or hardware.

"Each country has the choice to make on how much value it puts on the enterprise support structure to

caption 11/11 Scout Bold ragged right flushed left Bold ragged right flushed left

maintain systems long-term," he says. "If there is an interoperability issue with one, you see it get fixed and the fix applies to all, as opposed to an interoperability issue that may exist with an IAI one-off."

The crux of the issue is how many other JSF partners will look at what Israel is pioneering and decide they desire similar one-offs. Their motivations could range from strategic/tactical independence to the timing of JSF program software releases and, possibly, commercial concerns. Ironically, the open architecture design of F-35 systems potentially abets such desires.

"The open architecture gives the Israeli air force the option to operate new systems and to address, let us say, special needs without needing to change versions of the airplane's software," says Cohen.

Cohen cites one such "special need": "It gives the Israeli air force the capability for EW [electronic warfare] that is not part of the software for the normal F-35."

That aligns with comments made to Aviation Week in 2012 by a senior Israeli air force official: "We think the stealth protection will be good for 5-10 years, but the aircraft will be in service for 30-40 years, so we need EW capabilities [on the F-35] that can be rapidly improved. The basic F-35 design is OK. We can make do with

adding integrated software." (*AW&ST* Aug. 6, 2012, p. 28)

The ability to write its own apps is consistent with Israel's general desire for a level of independence from U.S. control. This emphasis on flexibility is evidenced by its push for an exemption from the JPO to carry out maintenance work in-country, rather than at predetermined Lockheed Martin-established logistics centers in Europe and elsewhere.

"The idea is to give the [Israeli air force] the opportunity and capability to add new applications without the [backbone] system blocking that opportunity," Cohen adds. "If you decide to add another system, another missile, another capability, you do not need to touch the mission system, you just add the new application."

LOCKHEED MARTIN

caption 11/11 Scout Bold ragged right flushed left Bold ragged right flushed left

Simply adding a new application sounds appealing and efficient, but the JPO sounds a cautionary, and possibly conflicting, tone on the precedent of JSF partners writing their own apps.

"By U. S. Government policy, any integration of F-35 software must be done with U.S. Government oversight and with the two prime contractors' involvement. Having open architecture systems on the F-35 will make it easier to integrate future improvements onto the aircraft, but it does not equate to every country or industry having free rein to integrating their own add-on software and systems."

Whether or not JSF partners add their own apps and functionality, the schedule for U.S. software updates once the program concludes its developmental phase, could provide additional motivation to operate independently.

According to the JPO, hardware and software releases will alternate on a four-year schedule. A software release will be followed two years later by a hardware release and so on. But it is a schedule which simply does not align with software development and operational realities.

"This is the idea of our system," Cohen says. "Instead of waiting two years or four years for another [software update] version we can [update] it in 4-5 months."

"The speed at which you could make [software] changes could certainly play a role in what is motivating partner nations," Clark allows. "I do not know that it is the only factor but I don't have firm data to say one way or the other."

The JPO does not acknowledge the timing of its software releases as problematic: We are working with all partners and [Foreign Military Sales (FMS)] customers to ensure we all have timely updates to meet various sovereign requirements in the coming years."

If Israel and other partners are sufficiently motivated to write their own apps, several questions arise, starting with interoperability. While commonality is foundational to the F-35 program, Skunk Work's Clark says conflicts can be managed.

"The Israelis are very innovative," he says. "I would expect they will work in their own way, but that does not preclude having interoperability with other standards. It just means that when interoperability is sought, they'll have to ensure that whatever implementation they have built on top of the data provided via F-35 can operate with other pieces of software or hardware. . . . With our [OMS] effort we are trying to minimize the upfront systems engineering required to do those sorts of things."

Interoperability will not be an issue, the JPO assures, again citing U.S. oversight of the two prime contractors involved (Lockheed and IAI). The office adds that it "applies strong systems engineering rigor and discipline to all software development efforts supporting both partners and FMS customers."

The prospect of writing apps for the F-35 also raises the issue of cybersecurity. Commercial software development security experts repeatedly point out that the intersection of manufacturer and vendor software is perhaps the chief point of vulnerability for integrated systems.

Clark concedes that developing apps for the F-35 is analogous but stresses the program has sufficient security assurance in place. "We all see the news in the broader context of what is going on in the cyberenvironment," he says. "If you look at what the banking industry has to deal with, those are the type of [security] technologies that we are exploring and evaluating to try to apply to our airborne avionics environment."

The F-35's open architecture design follows strict principles on the provision of data for third-party evaluation, according to Lockheed. There are high assurance guards within the system which can integrate cross-domain devices while keeping mission systems and outside apps separate.

IAI's Cohen says the company is confident its C4 software will not have any influence on the security of the overall system. But what if a partner nation does not strictly adhere to correct security protocols, or makes a mistake?

"It depends on what application you are talking about and what data that system is trying to access. There is no one easy answer on that," Clark admits.

Another questions is whether, if F-35 users can create their own apps, could they share or potentially sell them? Would IAI consider that possibility?

"Yes," Cohen answers. "We would need special permission to export [new applications]. We would need an export license."

Surely, F-35 users must have U.S. government authorization to market, sell or discuss non-U.S. add-ons, software updates, non-U.S. weapons, or any other F-35 equipment the program office stresses. But the JPO does not completely shut the door to partner-to-partner nation add-on/software sales, saying, "The U.S. government will review each situation individually as countries discuss their intent with us."

Could the possibility of JSF user-to-user sales combined with the issues of software control, independence, updates and security see the F-35 program again mimic the Apple mobile device world? Could the U.S. set up its own "F-35 App Store?"

Lockheed has "brainstormed" the idea, Clark confirms. "It could provide for a greater ecosystem of software developers and tailorization of the system for unique needs, but we are still sorting out how we would manifest that in a way that would not just be a marketing pitch," he says.