INTEGRATING WITH ISCO TO REDUCE RISKS CAUSED BY INTERFERENCE AND JAMMERS

Problem Statement

All wireless networks are affected by RF interference which can cause network performance to degrade and even stop working as planned. Interference can be unintentional or intentional, like a jammer that has the specific purpose of disrupting communications. ISCO's interference cancellation experience along with industry publications show that the sources of interference are widespread and aways changing. When a network is part of mission-critical infrastructure supporting public safety or other essential functions, it's imperative the network includes the ability to react immediately to interference and jammers. This paper will discuss how to accomplish this in Open RAN networks.

Integrating with ISCO

With Open RAN, the network owners and operators are not tied to a single supplier. They can:

- Choose different vendors for different parts of the network
- Select a variety of suppliers for unique functionality that is needed in the network

Since customers now have the flexibility to add features to their network that meet their individual needs, it's important to know how ISCO's interference mitigation and anti-jammer technology can be integrated into the Open RAN network components.

The principles of intelligence and openness are delivered through the decentralized O-RAN architecture shown in Figure 1. The RU, DU and the RIC are all points in the network where specific capabilities or features can be located.

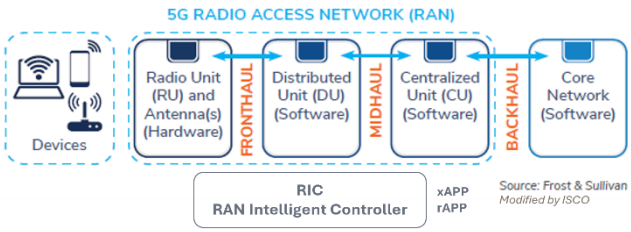

Figure 1: Components of a 5G network

It's also important to know how ISCO's technology works in order to understand how it fits in the Open RAN network. ISCO algorithms perform digital signal processing on the received radio signals, illustrated in Figure 2. This starts with a segment of the received signal being captured and analyzed using a variety of different patented techniques. The analysis detects and classifies interference and jammers, if present. This information is then used to compute a set of parameters to condition the signal and reduce or remove the interference or jammer.

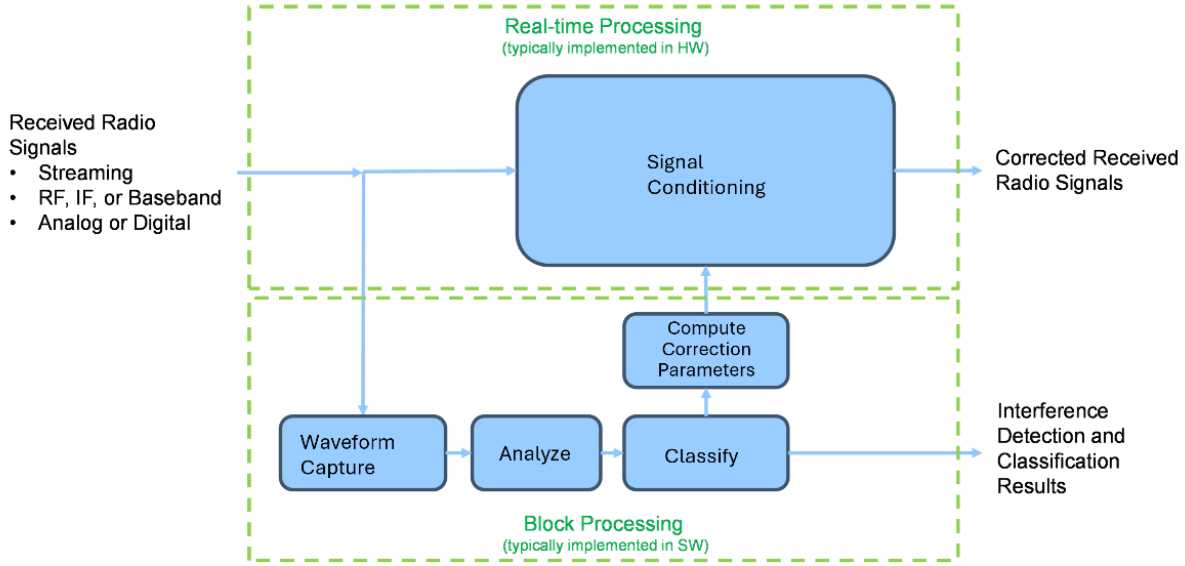

Figure 2: ISCO's process to cancel interference

The method of integrating ISCO into the RU or DU will be specific to each platform and the chipsets that are used. Figure 3 shows the digital signal processing chain of the RU and DU and illustrates where the ISCO cancellation engines can be embedded. In the RU, shown on the right side, ISCO is in the receive path between the digital front end and low-PHY. In the DU, ISCO is inserted on the eCPRI receive path prior to high-PHY.

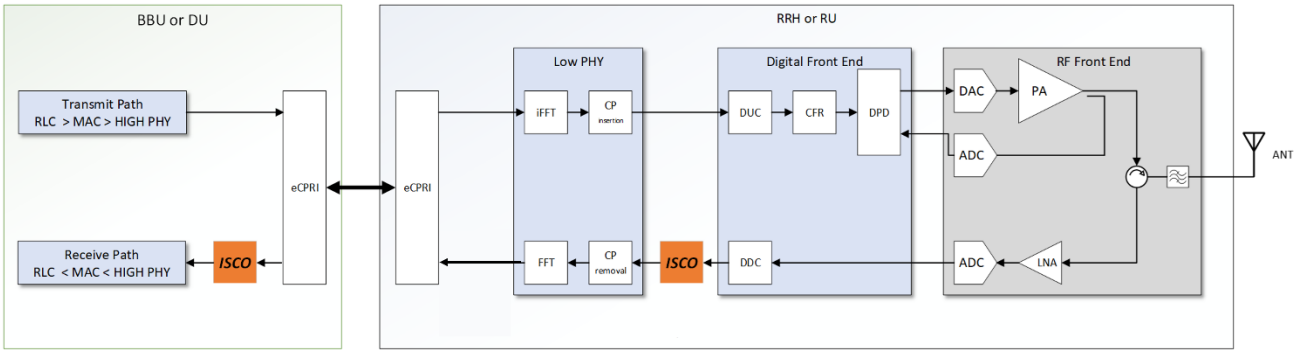

Figure 3: Interference cancellation in the RU or DU

Important Considerations

We know that the amount of FPGA resources and CPU resources depends on many variables that need to be coordinated in partnership with the RU and DU vendors we work with. These variables are related to the details of the RU or DU architecture provided by a vendor, the desired features and capabilities of the ISCO software, and the specifics of the product to be offered to the ultimate buyer of the network component. These are some examples of the variables that need to be defined for each category to prepare for a successful integration partnership:

Vendor Variables

RU and DU vendor variables are similar, but the DU may be implemented without the use of FPGA based acceleration.

- Overall radio architecture and how the 5G stack is implemented
- Models and types of FPGA used
- Models and types of embedded processors used
- Current utilization of the FPGA and the embedded subsystems
- Current latency across the 5G stack
- Amount of DDR RAM allocated to the FPGA and embedded subsystems and their current utilization
- Possibility of additional modules/components to be added to the FPGA and the embedded subsystems
- DU: eCPRI implementation, including DL and UL IQ data path, control path, ORAN functional split, access to time domain or frequency domain IQ data
- DU: model and type of the CPU, number of cores, available RAM, operating system, and other server specs

ISCO Software Variables

- Number of algorithms to be included
- Type(s) of interference and jammers to be addressed
- FDD and/or TDD requirements

Product Specific Variables

- Number of simultaneous carriers that need to be protected
- Bandwidth, subcarrier spacing and other 5G parameters of the carriers to be protected.

ISCO is consistently performing testing in our lab with our software against different types of jamming signals. New jammers will always be introduced, and this ensures our cancellation capabilities continue to be effective in hardening the Open RAN equipment against threats from interference and jammers.

Conclusion

Today's solutions which are not integrated into RU or DU components are costly, can take a long time to get to final resolution, and impact the desired operation of user applications. Most importantly, they do not include anti-jammer capabilities.

ISCO has a rich history of providing interference management technology and patented algorithms in a standalone product that is connected into the RAN over the CPRI link, but it can also be embedded into Open RAN RU and DU devices to improve speed and performance of networks and protect against jammers. Our experience with building hardware with embedded FPGA, embedded software and application software translates directly to the RU and DU in an Open RAN network. This allows RAN equipment providers to offer their customers a product for detecting, identifying and cancelling interference and jammers.

Even without Open RAN, network owners and operators can talk to suppliers about including interference detection and cancellation in their products. Our years of building products that integrate our interference cancellation software with COTS hardware has prepared us for integrating that software with other existing hardware products like a radio or test and measurement equipment.

With the growing importance of 5G wireless networks to national security and defense, public safety and countless applications ranging from healthcare to our power grid to transportation, the exposure to random unintended interference and jammers is becoming more pronounced and unacceptable. It is especially unacceptable now when technology exists to add safeguards that can be seamlessly integrated into the network at very little incremental cost.

About ISCO

ISCO is a private company based in Schaumburg, Illinois. Founded in 1989, ISCO has over 250 patents with algorithms and supporting trade secrets all specific to managing many types of radio frequency interference. With thousands of devices deployed in Tier-1 Mobile Network Operator radio access networks, ISCO technology is proven and can be used by suppliers of wireless products and software to ensure the networks their customers rely on perform as expected.