i3 Systems Operational Concepts

An I3 node manages the information flows between applications (information consumers) and devices (information producers).

I3 assumes the information network which runs on top of the data network, is collectively managed by many individual *groups*. Each group is responsible for some, but not all, of the devices and applications running within a collaborative information network.

Each group is tasked with running a set of devices, a set of applications, or a collection that consists of some applications and some devices. The devices that are managed by a group are contained within a defined *device space*.

Within a group, some users are classified as administrators and the group members are users. *Group administrators* have the ability to add new users to their group whereas non-administrative users cannot add new users. With the exception of the group administrators, every member of that group is able to manage the resources assigned to the group. Group members are considered to be part of a team that works together to support the group's assigned resources.

In the i3 System there are also *system administrators* that manage the I3 information fabric. These i3 system administrators can create I3 device spaces or application spaces. The system administrators also define the various *data types* that are utilized across the information network. When the system administrator first creates an application or a device space, they assign a group administrator that has the ability to add other users to the same space. The *super system administrators* have the ability to add new system administrators to the system whereas normal system administrators cannot create new system administrators.

A *data type* describes an information fragment that is derived from data submitted to the information network. As an example, data type might come from a device and be delivered to an application. Inside the i3 information network, a single message coming from a device might be passed through the information network as a basic information unit, it might be subdivided into multiple information elements, or it might be combined with other information elements before it is transmitted through the information network. Different devices from different suppliers can generate the same information units making the information network device agnostic. A single *data type* can be constructed from data messages transmitted with different formats making the i3 information network a natural vehicle to equalize information flows to a common information model.

The i3 permissioning process allows data owners to grant access to the data types that are generated by their devices.

When an application is looking for information, it can see the data types being produced by each device in an information directory. When an application identifies information it wishes to receive, that information is identified by the device name and the data type. To create a data stream, the application uses the device and data type names to submit a request for access to that information. This request includes descriptive information that allows the device space owners to determine whether to grant access to the information their devices are generating. This descriptive information includes information about the organization's data policies, the specific use case for this request, and any incentives that may be associated with this request. When the device space users receive such a request from an application, the device space users are able to approve or deny the application's request.

The information flows between a device and an application are simplex. One or more data types flow from a device to one or more applications. If a device requires any specific handshaking between the device and any upstream service logic, those handshaking procedures can be built into a device wrapper (or into an application wrapper as appropriate). If an application wants to actively manage a device by sending it various commands, a secondary command channel is created to allow messages (commands) to flow from the application to the device. By separating information and command flows into different data streams, the applications that have been granted control permission can be different from the applications that have been granted access to a device's information.

Note: The term ‘device’ may refer to a physical IoT (Internet of Things) device, a front-end processor that supports many IoT devices, or an application that produces an information stream similar to a smart IoT device.