How does cloud-based processing work?

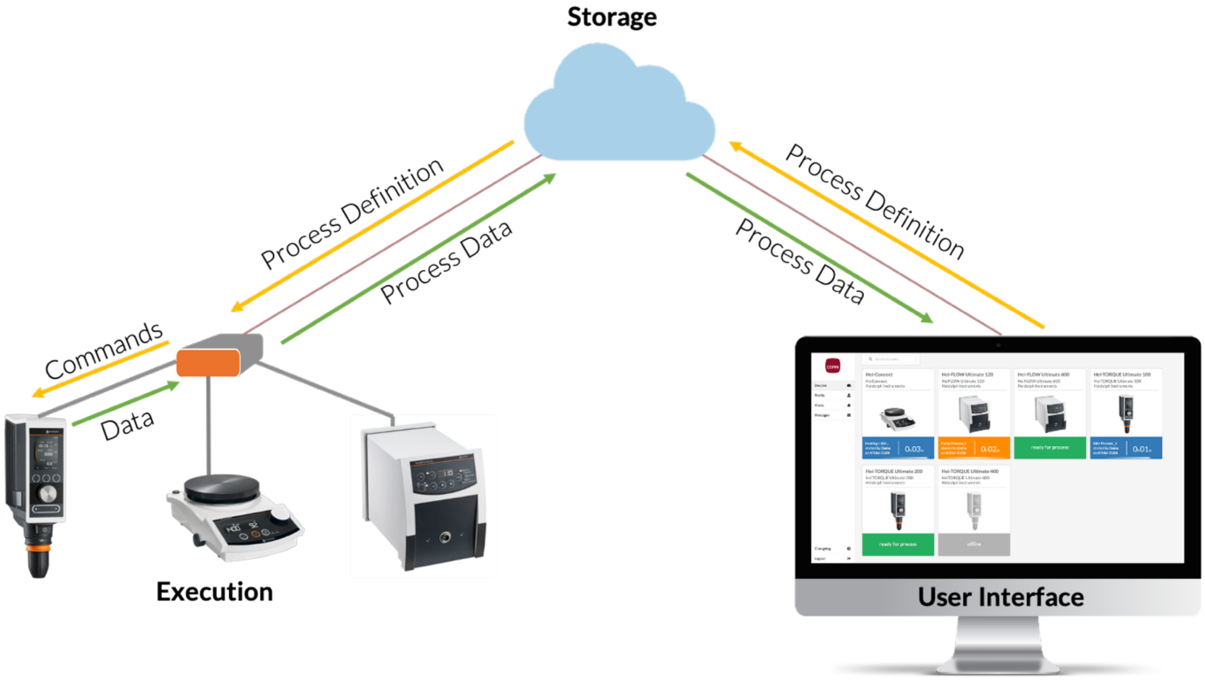
The OSPIN approach to (bio)processing is cloud-based, meaning that we are separating the user interface from the actual devices, allowing a more flexible approach to lab work. We have three very distinct components that are part of this system:

- Browser-based user interface
- Server-based data storage and management
- Localized process execution

The connection between these elements is the internet.

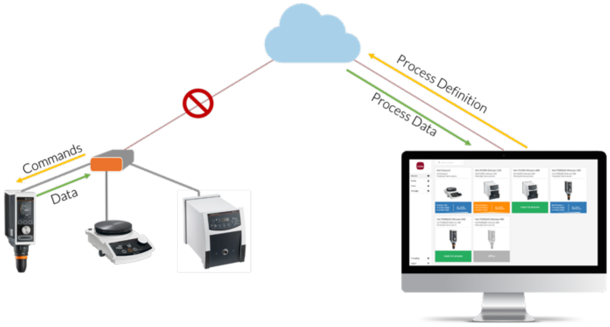
How is a process defined, executed & stored?

The visual interface for process definition is provided in a web-browser. All process parameters and settings are defined there and automatically saved in the OSPIN Cloud. Once the process is fully defined and started by the user, the process definition is sent to the Gateway for localized process execution. Then, based on the process definition, the Gateway sends to each connected device the commands it must execute in each process phase. Once the process is running each device sends to the Gateway the data it produces (e.g. sensor data), which are aggregated and relayed by the Gateway to the OSPIN Cloud, where they are safely stored. By sending the process data down to the users' web-browser, information on the running process is available in real time. Data from past processes are also available in the browser anytime, no matter if the device the data was created on, is turned on or off.



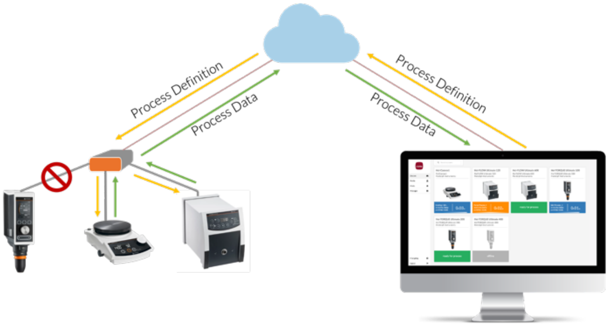
What happens if something goes wrong?

Loss of connection between the Gateway and the Cloud



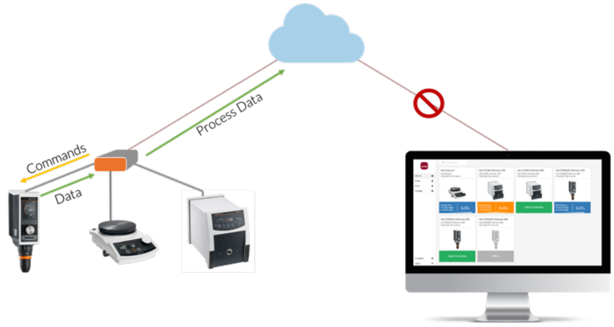
Once a process is started, a disruption of the connection between the Gateway and the OSPIN Cloud has no effect on the running process, as the commands to be sent to each device in each process phase are already on the Gateway. The Gateway is in charge of the process execution and at the appropriate times commands are sent to the connected devices by the Gateway and process data are received. If the data cannot be passed along to the OSPIN Cloud immediately, they are stored in the Gateways internal storage and updated as soon as the internet connection is re-established.

Loss of connection between the lab device and the Gateway



In case of a loss of connection between the lab device performing a process and the Gateway, during the time of disconnection no data is recorded. Once the connection is re-established, data collection automatically begins again. If new commands were to be sent during the time of disconnection, they are updated at this point.

Loss of connection between the web-browser and the Cloud



A loss of connection between the web-browser and the OSPIN Cloud does not have any influence on the running process. Process data are still updated to OSPIN Cloud and available to other users with access to the running process. Other users with the appropriate permission can change, pause or stop the process.

How is information about my process stored?

For each process, the process description is stored on the OSPIN Cloud. While the process has not been executed yet, you, and everyone else with the appropriate permissions, can make changes to every setting option of the process. During a running process, it is still possible to add new phases to the process and change the upcoming phases. Once a phase has been fully executed it cannot be changed anymore.

Once the process has finished, nobody is able to change its definition or the data produced during that process. The data can be reviewed & downloaded but not changed.

Even though, the data are stored on OSPIN Cloud, it is your data. After the process has finished, the only thing we do with it, is keeping it safe.

In the logs of each process, you are able to get information about when and by whom a process was started, stopped or changed.

How is OSPIN keeping your data safe?

User and Browser Security

Access to the OSPIN Cloud is secured by signed requests. Once a user logs in to the OSPIN web application, all communication to and from the server is authorized to that specific user identity. This allows you to track, record, and parse all interaction between your Gateway, bioprocesses, and organization users. All the data you generate, from your user information to your process recipes, is secured in a virtual private cloud (VPC) and encrypted using TLS (Transport Layer Security), a commonly used cryptographic protocol, when in transit.

OSPIN employs AWS Cognito user sign-up, sign-in, and access control that is HIPPA eligible, as well as PCI DSS, SOC, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO 9001 compliant.
As with most authorization schemes where a user password input is required, the biggest security risk lies in users keeping their passwords secure. In addition to the existing requirement of using strong passwords, OSPIN can (upon request) require users of a particular organization to also engage in regular password changes, as well as multi-factor authentication (MFA) security. MFA requires an additional form of security beyond username + password, such as verification via SMS or time-based one-time passwords.

Device Security

All Gateways have individual certificates which are used to communicate with the cloud. Gateways must authenticate themselves with their certificates, after which all communication with the cloud is signed. Every Gateway certificate (and consequentially Gateway identity) is associated with a specific and narrow set of permissions for both the information it can submit to the cloud as well as the information it can receive from the cloud. These permissions are secured in the OSPIN VPC (virtual private cloud) and are tailored to individual Gateways - meaning Gateways can not spy on communication sent to other Gateways and they can not pretend to be other Gateways when submitting data. This means that, even in a worst case scenario in which a Gateways' security has been compromised (e.g. someone hacks in to GatewayA directly on location and changes communication to say "I am GatewayB"), the hacker would -still- be unable to communicate on GatewayB's behalf because the GatewayA's policies, kept securely in the cloud and verified with the Gateways' certificates, would not authorize it.

Data Security

OSPIN does not sell, exchange, or make public client data (be it user/anonymous usage data, Device/Process data, etc.) to any 3rd parties. This includes not tracking users' behavior in browsers anonymously or otherwise. All persistent data generated is secured in a VPC and encrypted using TLS when in transit.

Where do we store the information?

No stored data will be transferred, backed up and/or recovered by OSPIN outside of the European Union.

OSPIN stores account and process data in databases hosted in an Amazon Web Services data center in Germany. Databases are backed up regularly and are stored on file storage at the same geographical location as the database.