Network isolation for the MICE liquid hydrogen controls

MICE LH2 group

July 13, 2017

1 Introduction

The risks concerning running liquid hydrogen in the MICE hall will require special precautions for the controls and monitoring system. On the other hand the pool of experts should have the ability to monitor the system remotely in order to ensure its robustness.

2 Network isolation

The solution we propose is to use a Linux box located in the hydrogen control room that will have two network cards. One network card will be connected to the network switch that the Omron PLCs (Programmable Logic Controller) and the HMI (Human Machine Interface) devices are connected. The other will be connected to MICENet. Currently the network switch that the PLCs and HMI are connected to is also connected to MICENet. This connection will be removed so that no communication with MICENet or other networks will be possible except through the Linux box. The Linux box will run an EPICS ioc that will retrieve information from the PLC using the FINS protocol to set a number of process variables (PVs). An EPICS gateway (also running on the Linux box) will then provide read-only copies of these PVs on MICENet allowing anyone with access to MICENet locally or remotely to monitor the hydrogen system without being able to control it. These PVs (or a subset) can then be archived by the standard EPICS Archiver (eliminating the need to manually copy data off the compact flash card in the HMI) and monitored by the alarm handler in the MICE local control room and the ISIS control room.

A further level of security can be implemented whereby the PLCs are configured to not accept any remote control commands except from specific IP addresses, e.g. the HMI only.

The HMI and the PLC will keep the same static IP addresses that they have on MICENet. The PLCs are configured to operate independently of any communication with any other devices and so can be safely disconnected from MICENet and this has been tested. The Linux box will be in charge of the network isolation of the PLC/HMI

modules, routing only outgoing traffic from the EPICS gateway to MICENet and ignoring all incoming communication from MICENet. This will also prevent direct monitoring and control via the HMI web interface that is currently being used.

An existing software IOC will be revamped while the hardware/network infrastructure will be put in place.