Table 1 NSCL Control System Vulnerabilities

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Vulnerability** | **Description** |  |
| 1 | Control Network is not isolated from rest of the network. | The IOCs, embedded controllers, PLCs and other instruments/devices can be accessed directly from the office network. |  |
| 2 | Physical access to the Control Network is not restricted. | There is no policy governing physical access to the control network. Anyone can connect any device to it, as long as they can find a port, and assign an IP address. |  |
| 3 | Shared accounts. | Access to shared accounts (k800 etc) is easy. Passwords to them are easily available. |  |
|  | Experiment accounts | Experiment accounts (e06030 etc) stay around for a long time. Passwords to them are shared and easily available. Experimenters can still use them (ssh) after they have left. |  |
| 4 | Field Consoles and Control Consoles are easily accessible. | Anyone can walk up to a logged-in field console, and change settings for any device. |  |
| 5 | Simple passwords |  |  |
| 6 | Outdated Controls Gateway ACL | There is no process to manage the ACL: who gets on the list, who authorizes it, how long can an account stay on the list, etc |  |
| 7 | Control network is accessible from the Internet |  |  |
|  |  |  |  |

Table 2 NSCL Control System Threats

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Threat** | **Description** | **Prob** | **Impact** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
|  |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |