Contribution ID: **8** Type: **not specified**

A study of network vulnerability in embedded devices

Sunday 11 October 2009 10:00 (30 minutes)

Recently many TCP/IP devices are used in accelerator-control system.
Not only computers but also embedded devices are used in the accelerator-control system.
Since the embedded devices are designed with limited hardware resources, many devices are consists of subset of the TCP/IP components.
The limited resources and components therefore cause many problems such as vulnerabilities of network traffic.

SPring-8 is one of the largest synchrotron-radiation facilities in the world, and many embedded devices are used to control accelerator complex.
Originally, the control network of SPring-8 is designed as single segment without any routers, it is the best solution for a small-scale control network from a point of high reliability by the simplification.
However, by increasing the number of embedded devices in the single network, more trouble have arisen such as packet flooding, hang up of devices, and so on.
We study network vulnerabilities on these embedded devices used in SPring-8.
And then, we found vulnerability on iTRON-based embedded devices.[1]
We also performed improvement of implementation on vulnerable devices and refinement of network into multi-segmented L3 network design.
In this presentation, we report result of the refinement to improve reliability of the control system.

[1] T.Sugimoto, M.Ishii, T.Masuda, T.Ohata, T.Sakamoto, and R.Tanaka, Proceedings of PCaPAC2008, THX03 (2008)

Author: SUGIMOTO, Takashi (Japan Synchrotron Radiation Research Institute)

Co-authors: ISHII, Miho (Japan Synchrotron Radiation Research Institute); TANAKA, Ryotaro (Japan Synchrotron Radiation Research Institute); MASUDA, Takemasa (Japan Synchrotron Radiation Research Institute); SAKAMOTO, Tatsuaki (Japan Synchrotron Radiation Research Institute); OHATA, Toru (Japan Synchrotron Radiation Research Institute)

Presenter: SUGIMOTO, Takashi (Japan Synchrotron Radiation Research Institute)