Network packet inspection using port mirroring provides the ultimate tool for understanding complex behaviors in large distributed control systems. The timestamped captures of network packets embody the full spectrum of protocol layers and uncover intricate and surprising interactions. No other tool is capable of penetrating through the layers of software and hardware abstractions to allow the researcher to analyze an integrated system composed of various operating systems, closed-source embedded controllers, software libraries and middleware. Being completely passive, the packet inspection does not modify the timings or behaviors. The completeness and fine resolution of the network captures present an analysis challenge, due to huge data volumes and difficulty of determining what constitutes the signal and noise in each situation. We discuss the development of a deep packet inspection toolchain and application of the R language for data mining and visualization. We present case studies demonstrating off-normal analysis in a distributed real-time control system. In each case, the toolkit pinpointed the problem root cause which had escaped traditional software debugging techniques.