Creating High Confidence in a Separation Kernel. W.B. Martin, P.D. White, and F.S. Taylor. *Automated Software Engineering*, Vol. 9 no. 3, August 2002, pp. 263-284.

Abstract: Separation of processes is the foundation for security and safety of properties of systems. This paper reports on a collaborative effort of Government, Industry, and Academia to achieve high confidence in the separation of processes. To this end, this paper will discuss (1) what a separation kernel is, (2) why the separation of processes is fundamental to security systems, (3) how high confidence in the separation property of the kernel was obtained, and (4) some of the ways government, industry, and academia cooperated to achieve high confidence in a separation kernel.

What is separation? Strict separation is the inability of one process to interfere with another. In a separation kernel, the word *separation* is interpreted very strictly. Any means for one process to disturb another, be it by communication primitives, by sharing data, or by subtle uses of kernel primitives not intended for communication, is ruled out when two processes are separated.

Why is separation fundamental? Strict separation between processes enables the evaluation of a system to check that the system meets its security policy. For example, if a red process is strictly separated from a black process, then it can be concluded that there is no flow of information from red to black.

How was high confidence achieved? We have collaborated and shared our expertise in the use of Specware. Specware is a *correct by construction* method, in which high level specifications are built up from modules using specification combinators. Refinements of the specifications are made until an implementation is achieved. These refinements are also subject to combinators. The high confidence in the separation property of the kernel stems from the use of formal methods in the development of the kernel.

How did we collaborate? Staff from the Kestrel Institute (developers of Specware), the Department of Defense (DoD), and Motorola (developers of the kernel) cooperated in the creation of the Mathematically Analyzed Separation Kernel (MASK). DoD provided the separation kernel concept, and expertise in computer security and high confidence development. Kestrel provided expertise in Specware. Motorola provided its own expertise with that of DoD and Kestrel in creating MASK.