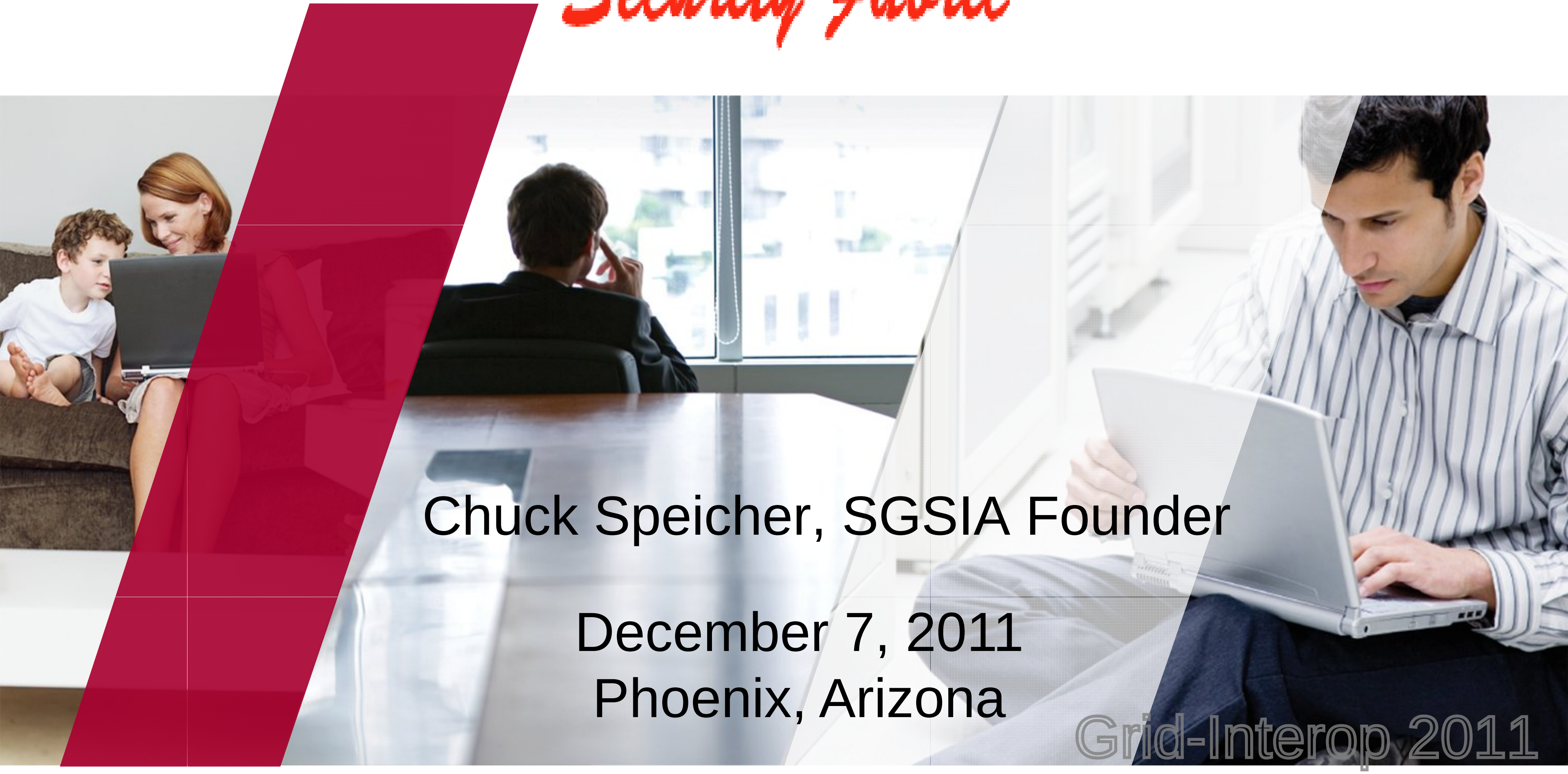
SGIP
Winter

The Smart Grid Security Innovation Alliance

McAfee

intel

Security Fabric



Chuck Speicher, SGSIA Founder

December 7, 2011
Phoenix, Arizona

Grid-Interop 2011

The SGSIA addresses the entire ecosystem.

- The Smart Grid Security Innovation Alliance is a working association dedicated to practical deployment of the smart grid complex system solution in the United States:
  - Utilities
  - Systems integrators
  - Manufacturers
  - Technology partners
  - National certification and interoperability entity
- The alliance is intended to give the CEO of a utility the purview of up-to-the moment knowledge of the options available to make wise investment decisions regarding infrastructure deployment for optimal returns.

The variation includes the proper orientation for large, medium, and small utilities.

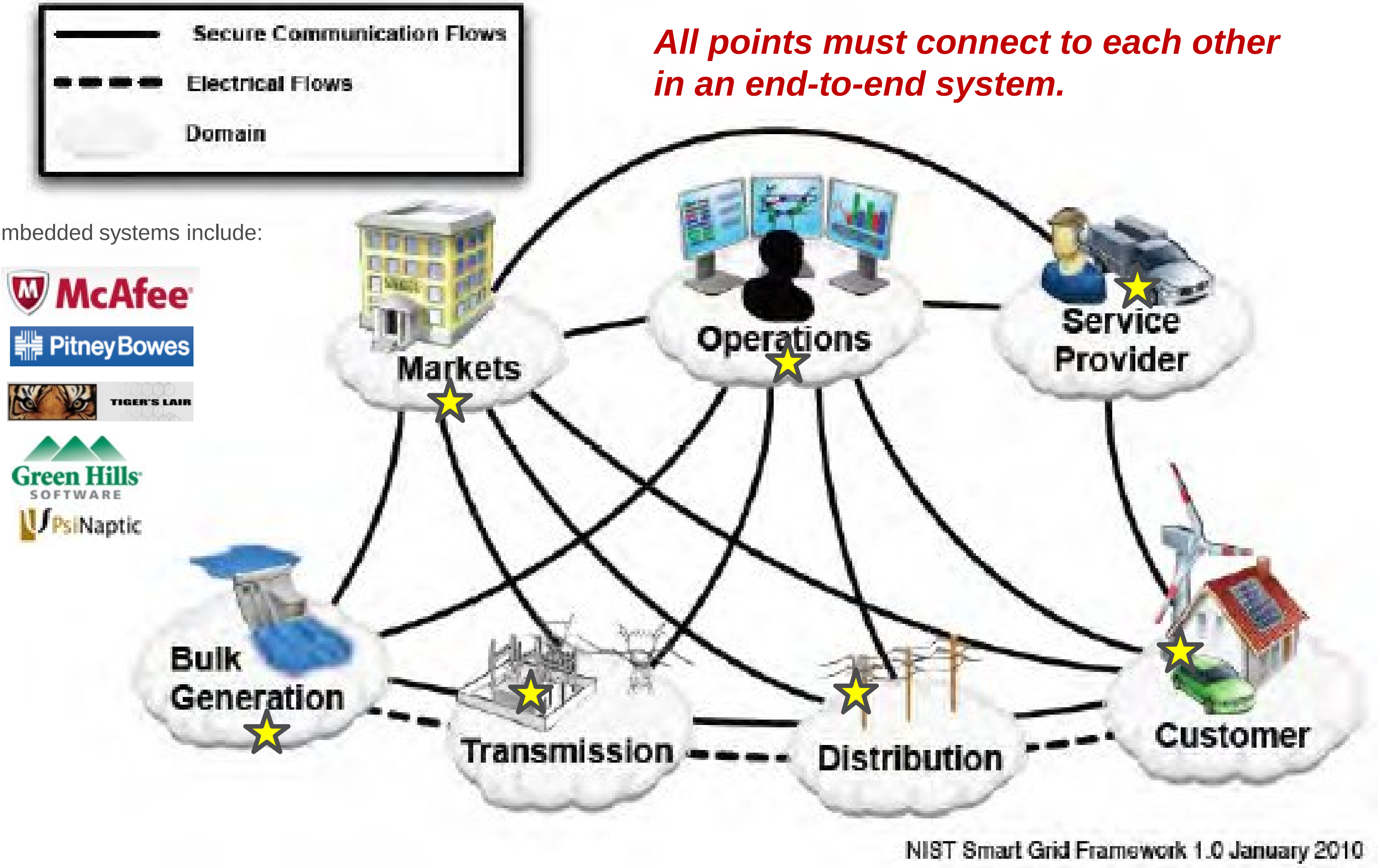
Our strategy is to provide certified interoperability to the key devices controlling the grid.

McAfee

All points must connect to each other in an end-to-end system.

The embedded systems include:

- ★ McAfee
- Pitney Bowes
- TIGER'S LAIR
- Green Hills SOFTWARE
- PsiNaptic



NIST Smart Grid Framework 1.0 January 2010

The McAfee HSM solution would be embedded at each critical point in the energy infrastructure.

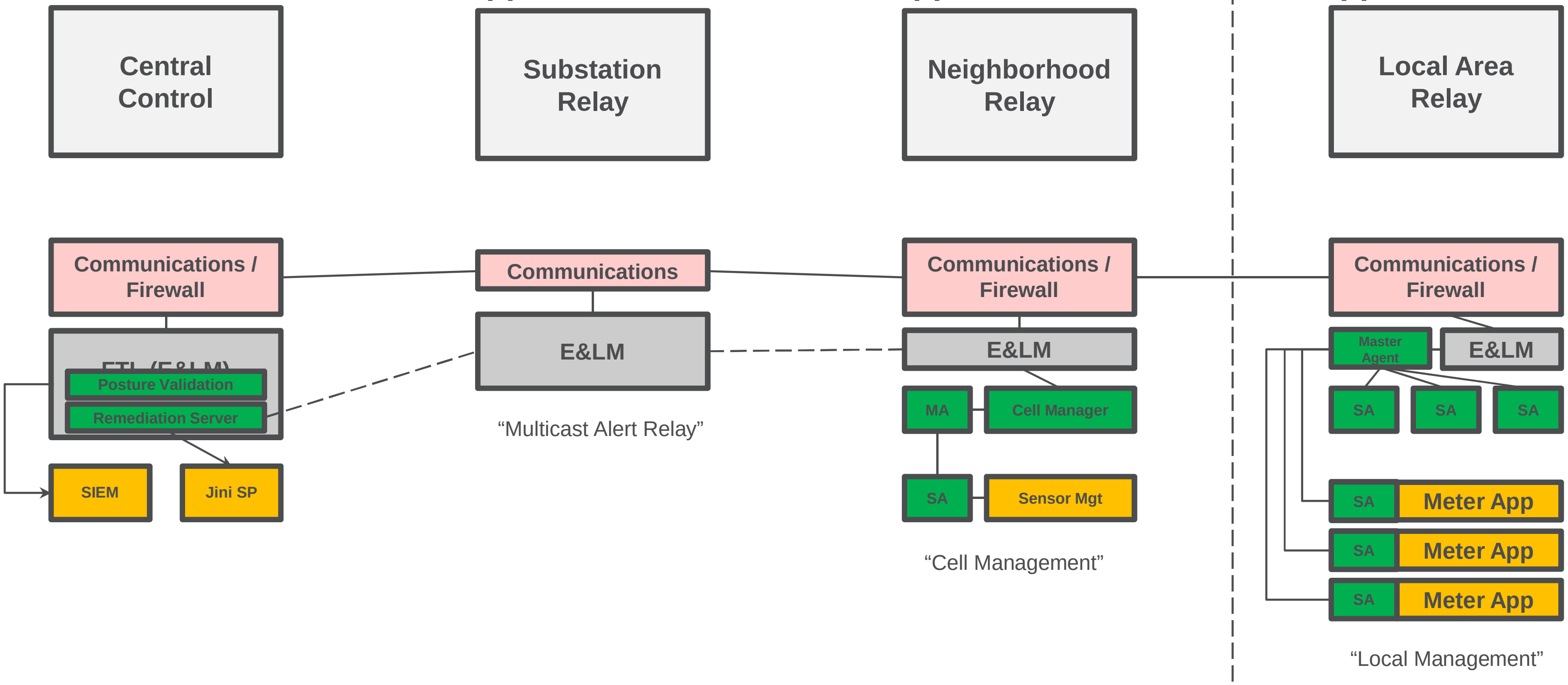
As an example, the general approach to power distribution requires a thin overlay of end-to-end management services.

Tibco "FTL"
CloudShield MPP
Nitro SIEM

RuggedCom
Application Card

Ambient
Application Card

Intel
Application Card



Central Control

Communications / Firewall

FTL (E&LM)

Posture Validation

Remediation Server

SIEM

Jini SP

Substation Relay

Communications

E&LM

"Multicast Alert Relay"

Neighborhood Relay

Communications / Firewall

E&LM

MA

Cell Manager

SA

Sensor Mgt

"Cell Management"

Local Area Relay

Communications / Firewall

Master Agent

E&LM

SA

SA

SA

SA

Meter App

SA

Meter App

SA

Meter App

"Local Management"

Grid-Interop 2011

A tailored trustworthy space (TTS)

Provides flexible, adaptive, distributed trust environments for a set of devices and applications that can support functional and policy requirements arising from a wide spectrum of activities in the face of an evolving range of threats.

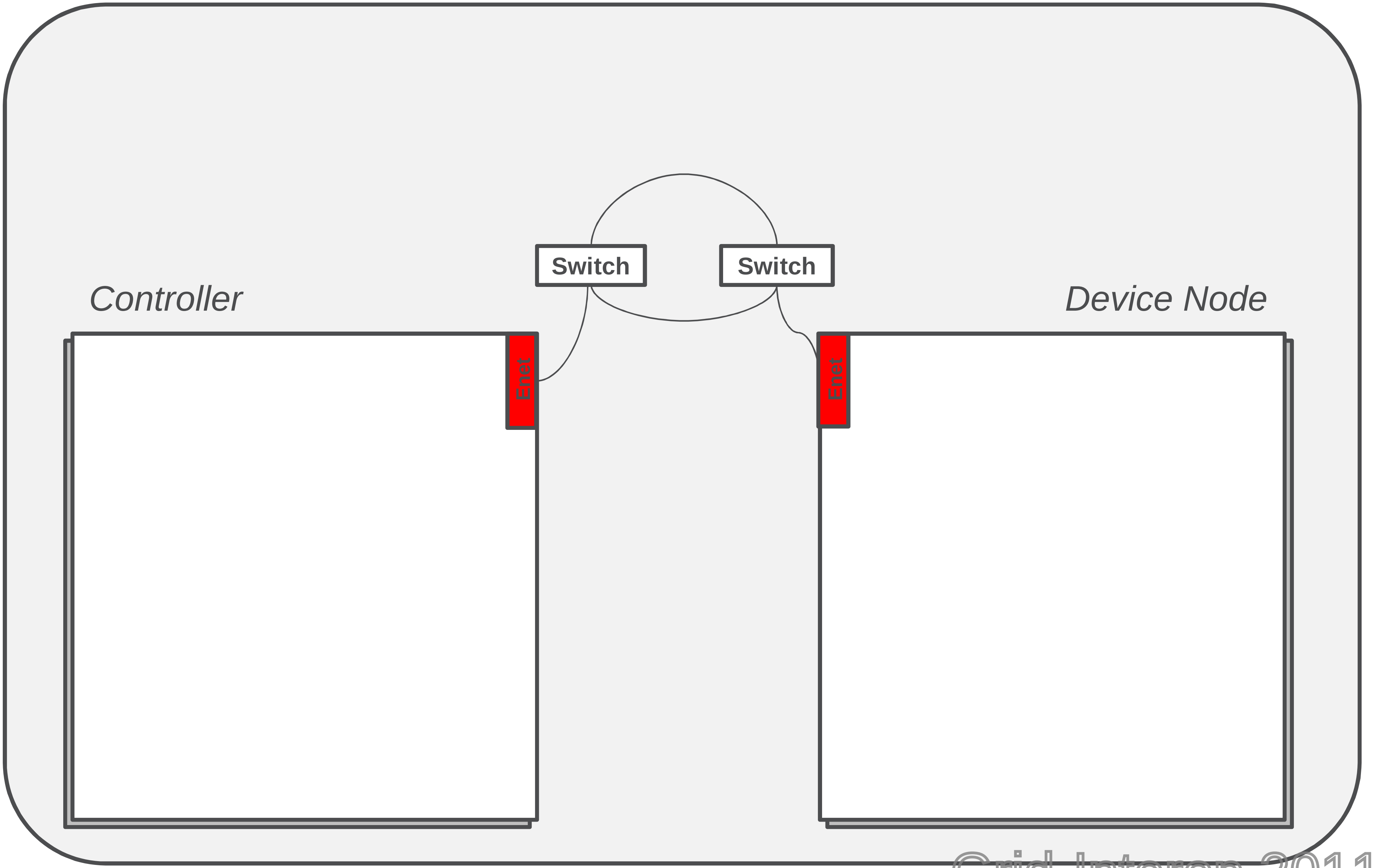
A TTS recognizes a device’s context and evolves as the context evolves.

Let us define the Security Fabric by building a control system.

Generally, there are always a controller element and a controlled element
in any control system environment.

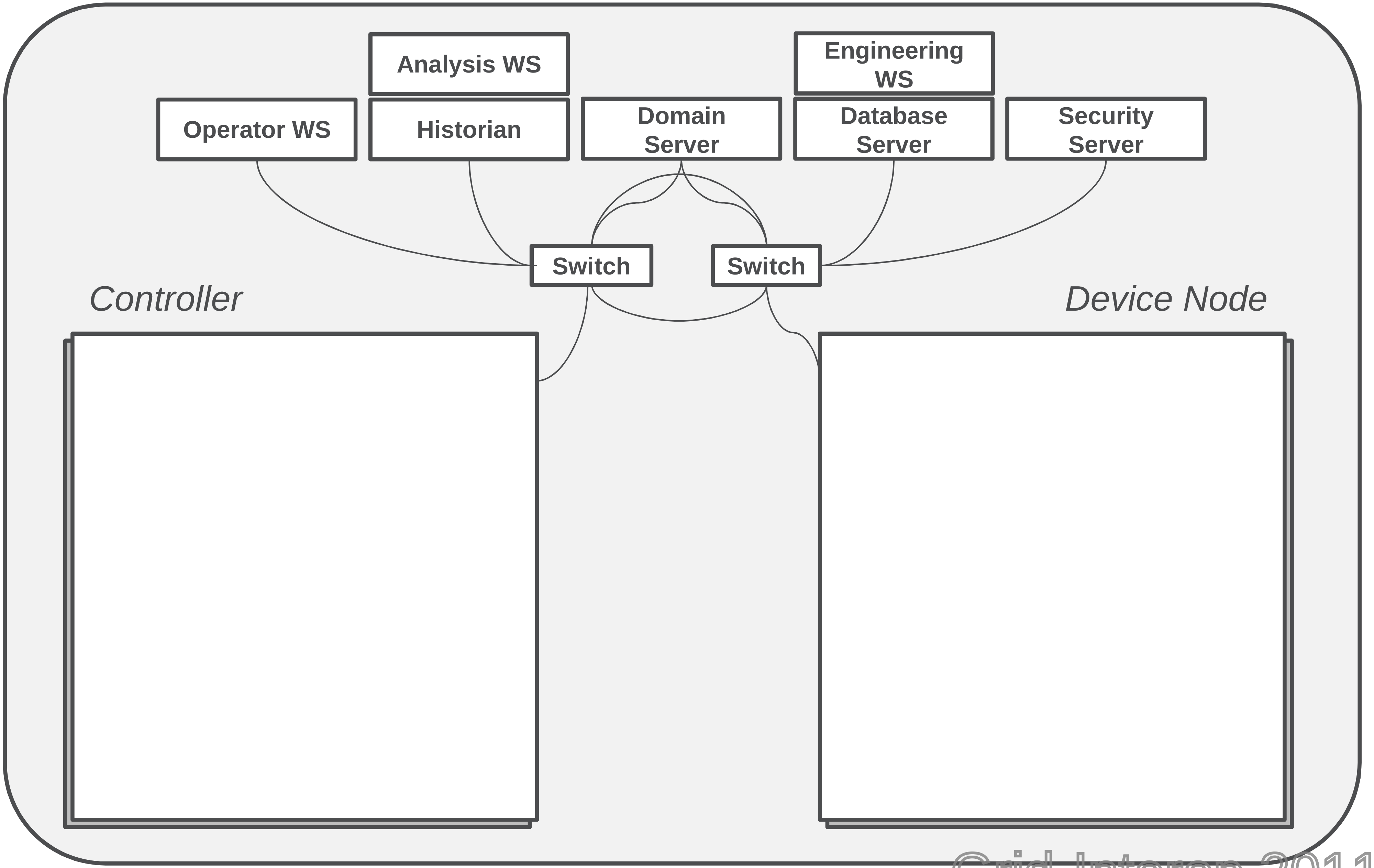
An example of a tailored trustworthy space built using the **Security Fabric** components:

In a contemporary environment they talk to each other using IP-based switches.



An example of a tailored trustworthy space built using the **Security Fabric** components.

They have management workstations and servers that supervise the controller and device nodes.

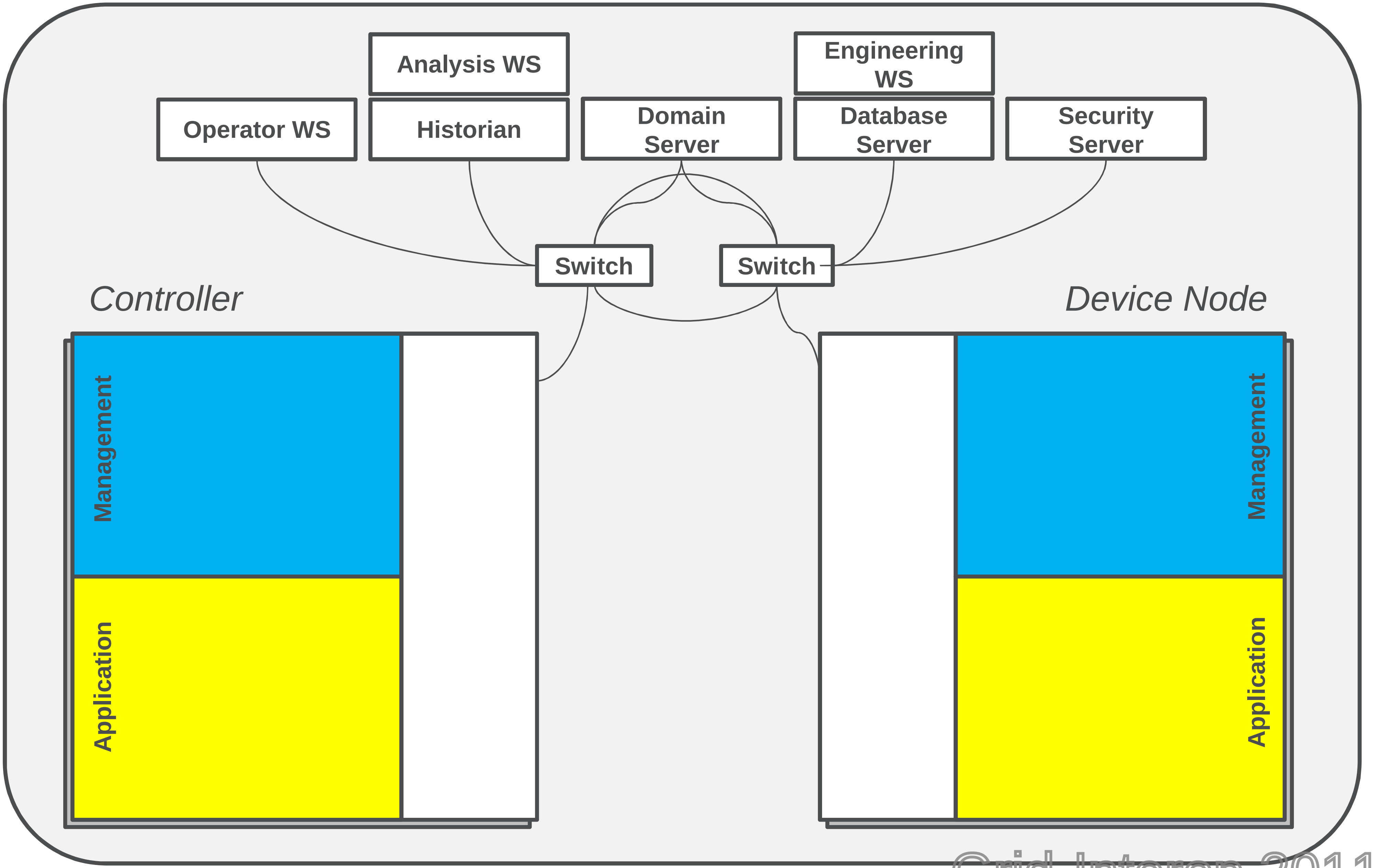


An example of a tailored trustworthy space built using the **Security Fabric** components.

The Security Fabric permeates the distributed management functions, but is mostly separate from the application functions..

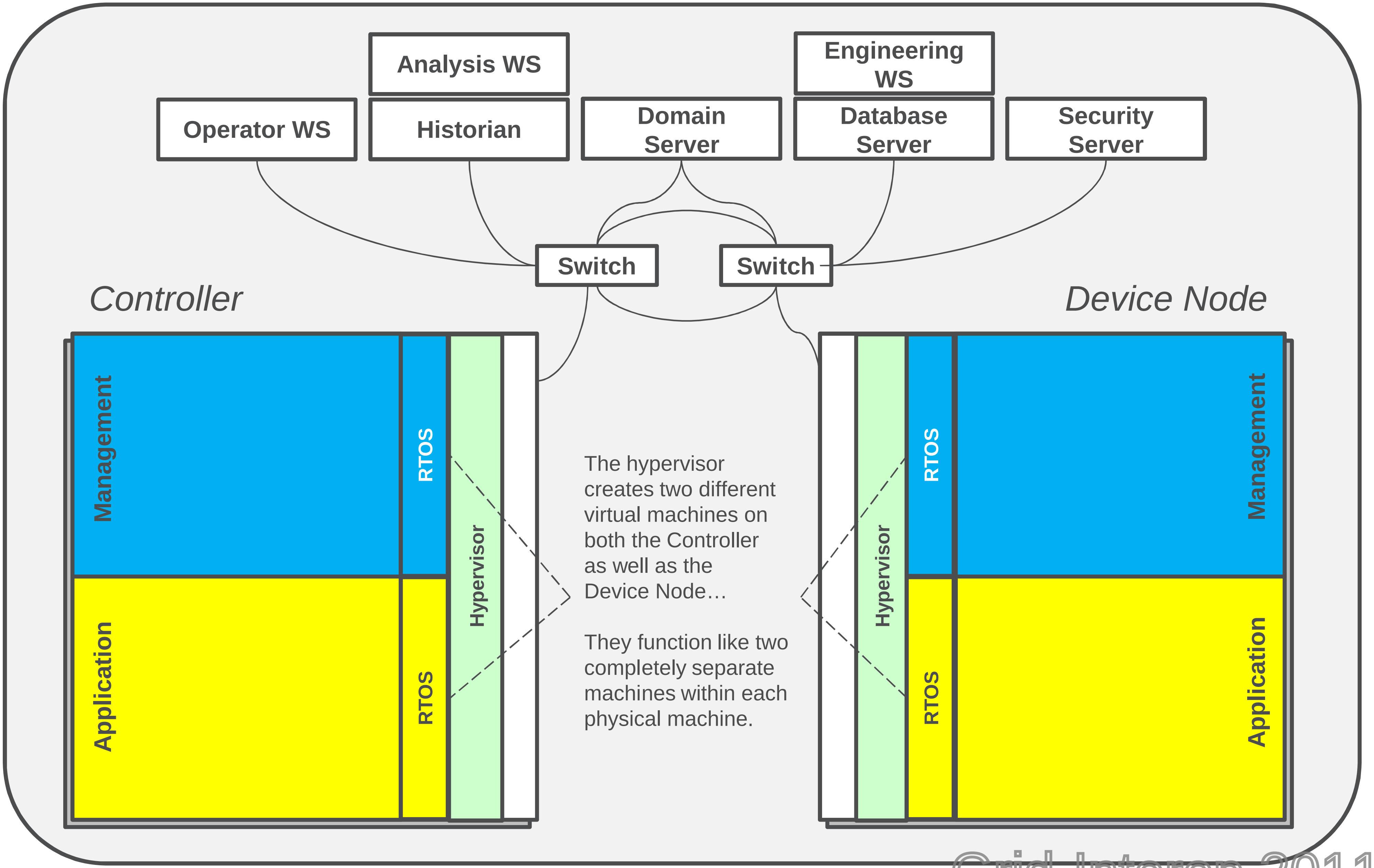
Our strategy is to separate the management functions from the application functions as much as possible… so that if the application becomes compromised or inoperable, the management system can easily be used to remediate the problem.

With this in mind, both the Controller and the Device Node keep the management functions separate from the application.



An example of a tailored trustworthy space built using the **Security Fabric** components.

This is done using a separation kernel to keep the application from ever interfering with the management functions.



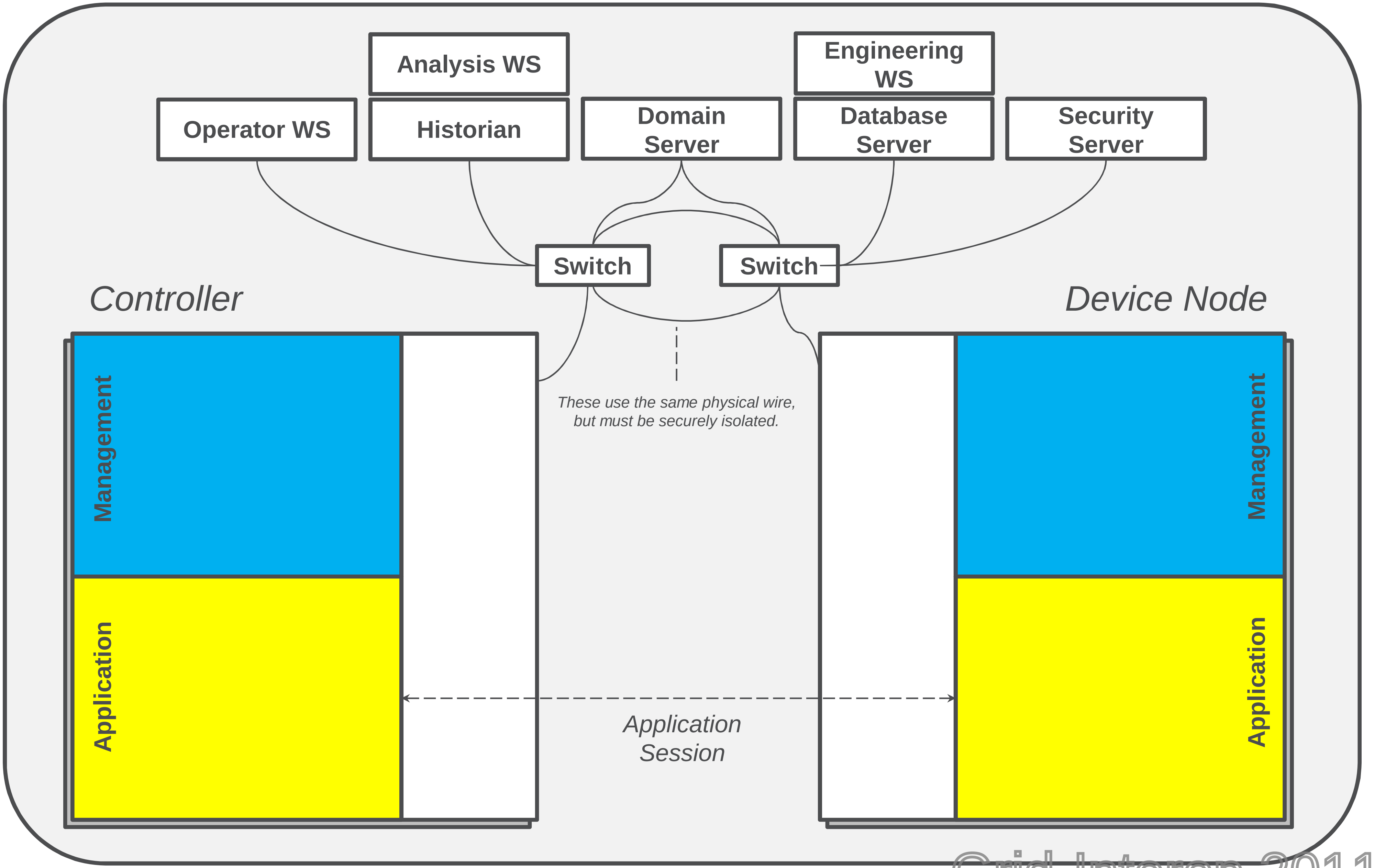
The hypervisor creates two different virtual machines on both the Controller as well as the Device Node…

They function like two completely separate machines within each physical machine.

An example of a tailored trustworthy space built using the **Security Fabric** components.

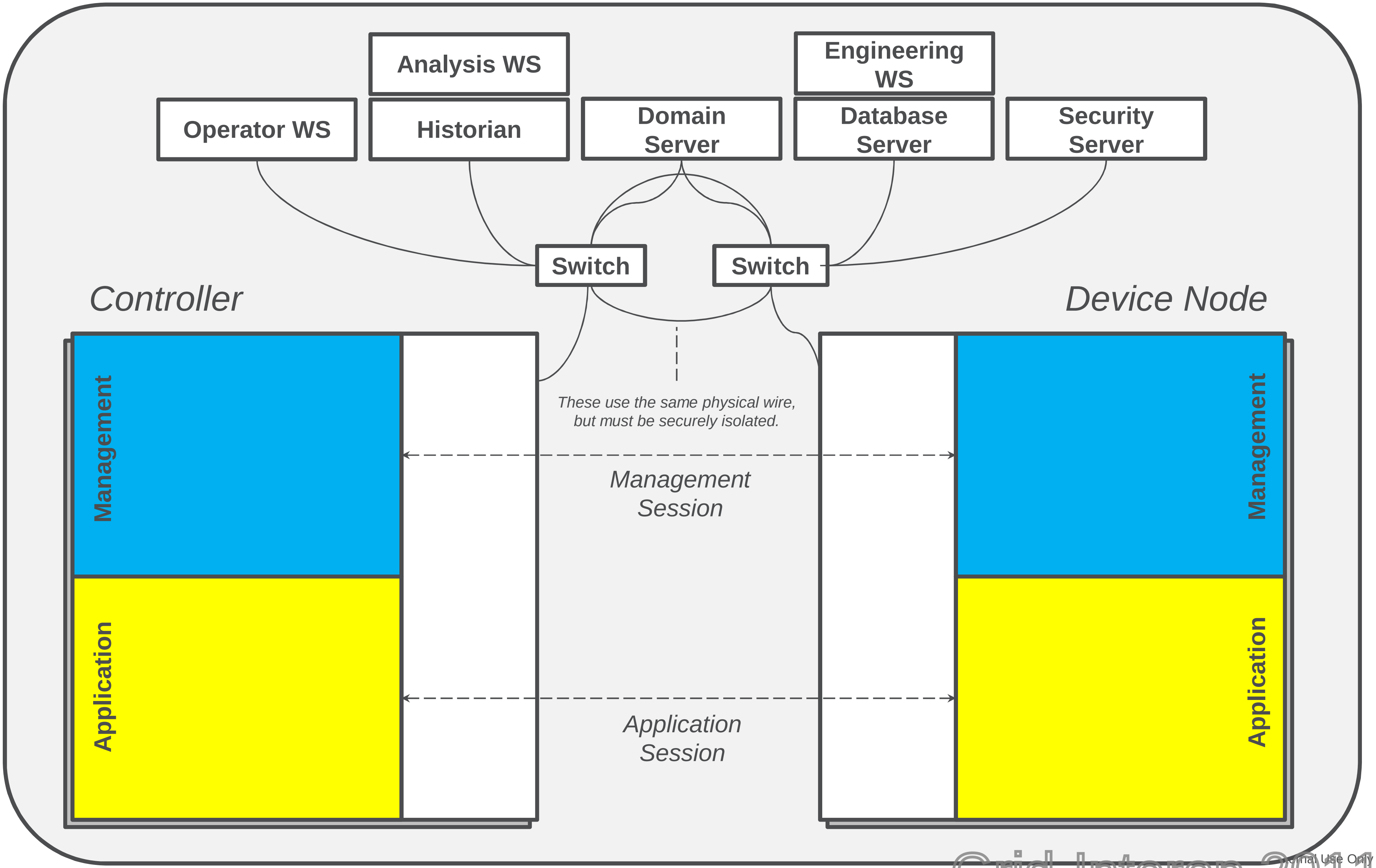
The application in the controller monitors and controls the application in the device node.

McAfee



An example of a tailored trustworthy space built using the **Security Fabric** components.

And the management functions and policies in the controller supports the management agent in the device node.



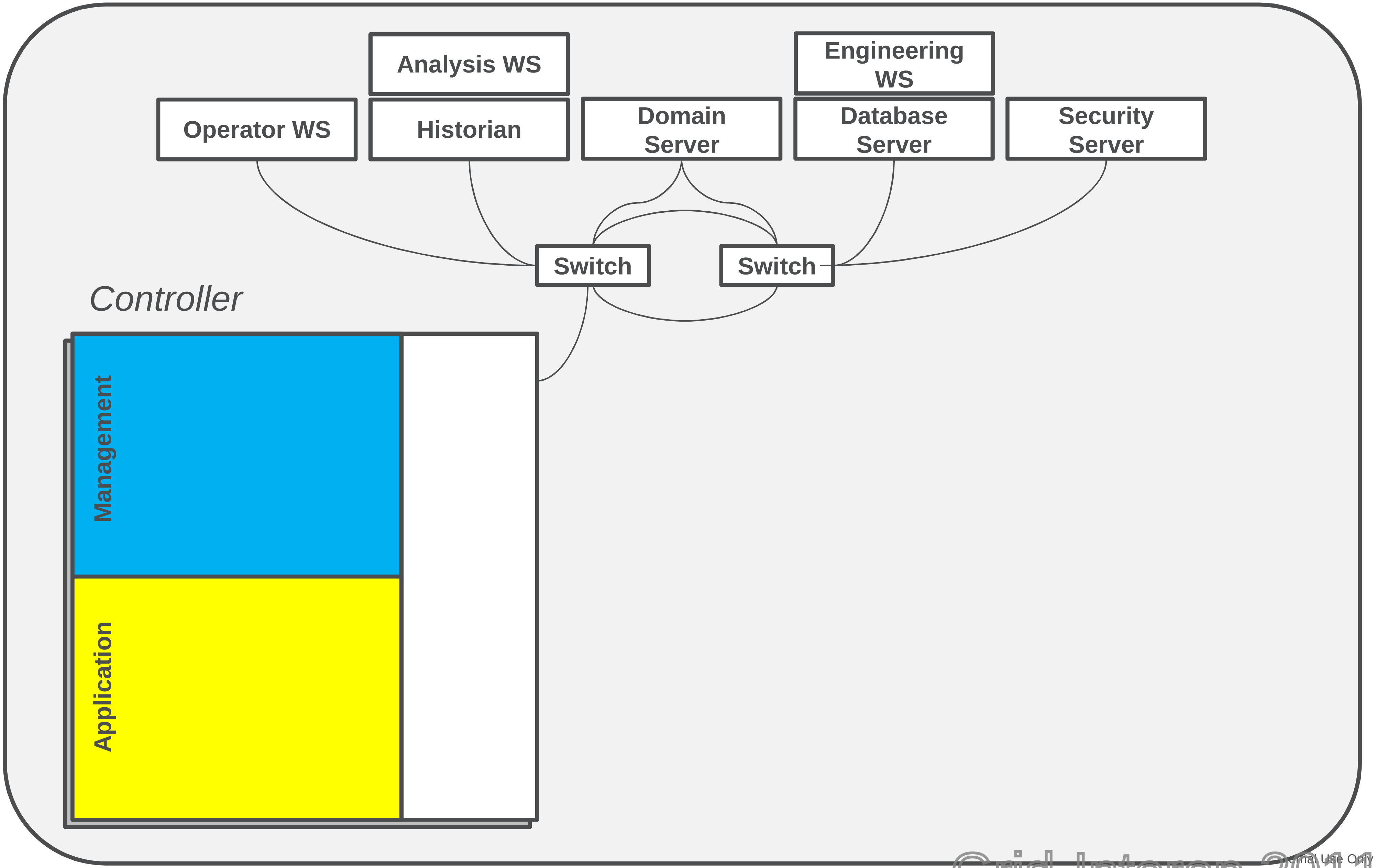
An example of a tailored trustworthy space built using the **Security Fabric** components:

These are the eight tenets of security as described in the NIST-IR 7628 Guidelines.

1. Identity Management
   - Ensures the device identity is established genuinely
2. Mutual Authentication
   - Allows both the Device Node and the Controller to verify the trustworthiness their identity to each other.
3. Authorization
   - Manages permission to proceed with specific operations.
4. Audit
   - Records noteworthy events for later analysis
5. Confidentiality
   - Encrypts sensitive data for matters of privacy.
6. Integrity
   - Ensures that messages have not been altered.
7. Availability
   - Prevents denial of service attacks
8. Non-Repudiability
   - Ensures that the authority for events cannot be denied after the fact.

To establish the secure communications from the Controller to the Device Node using the Security Fabric elements, let us proceed in chronological order.

The Controller must power on before any of the device nodes can use it.

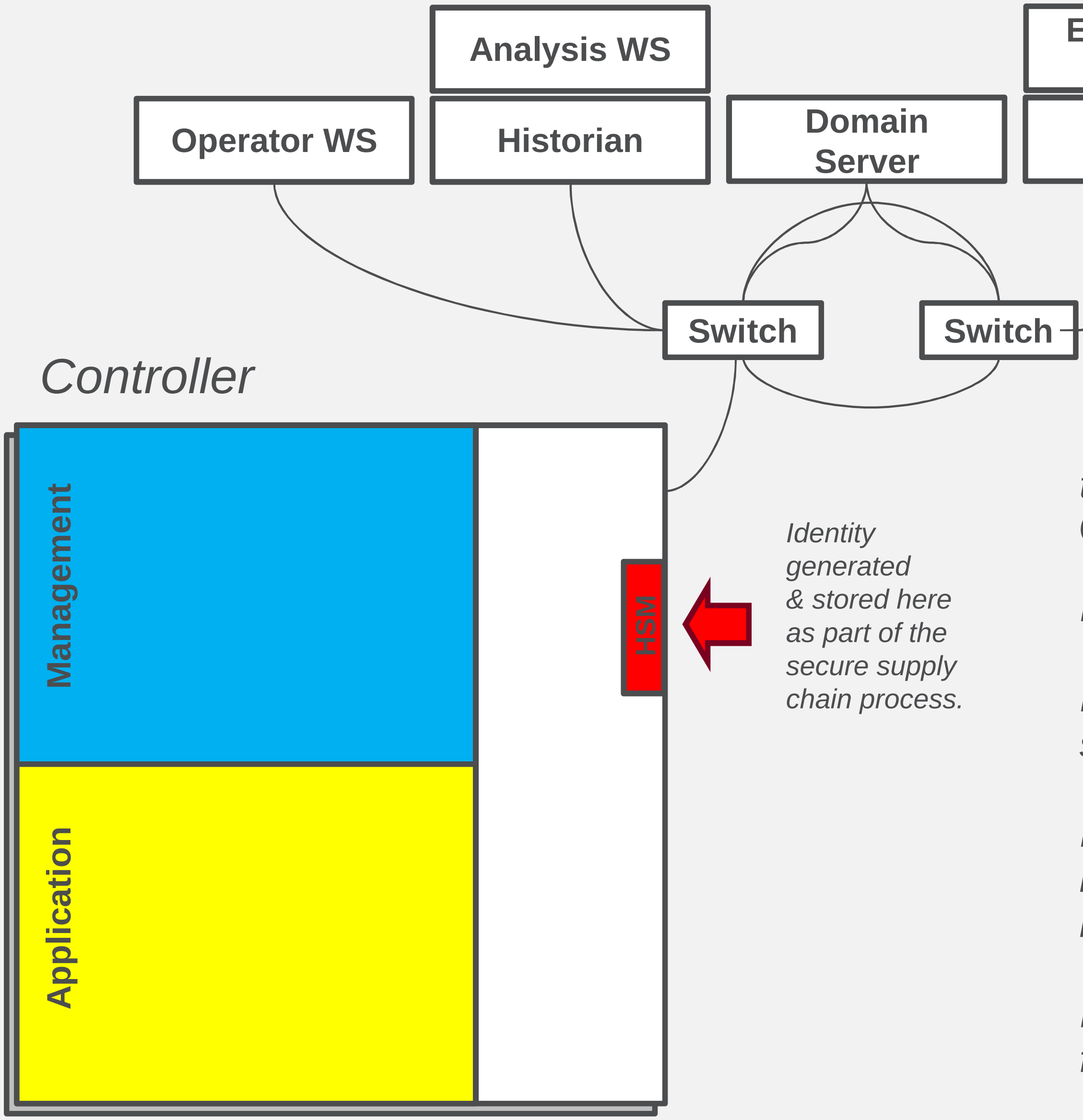


An example of a tailored trustworthy space built using the **Security Fabric** components:

Identity Management is the most crucial aspect of embedded security

we use a Hardware Security Module to protect the unique identity of the Controller.

McAfee



Identity generated & stored here as part of the secure supply chain process.

Identity Management

This is a special purpose ASIC that is FIPS 140-2 level 3 certified.
(Environmentally tamper resistant)

It houses an array of crypto functions.

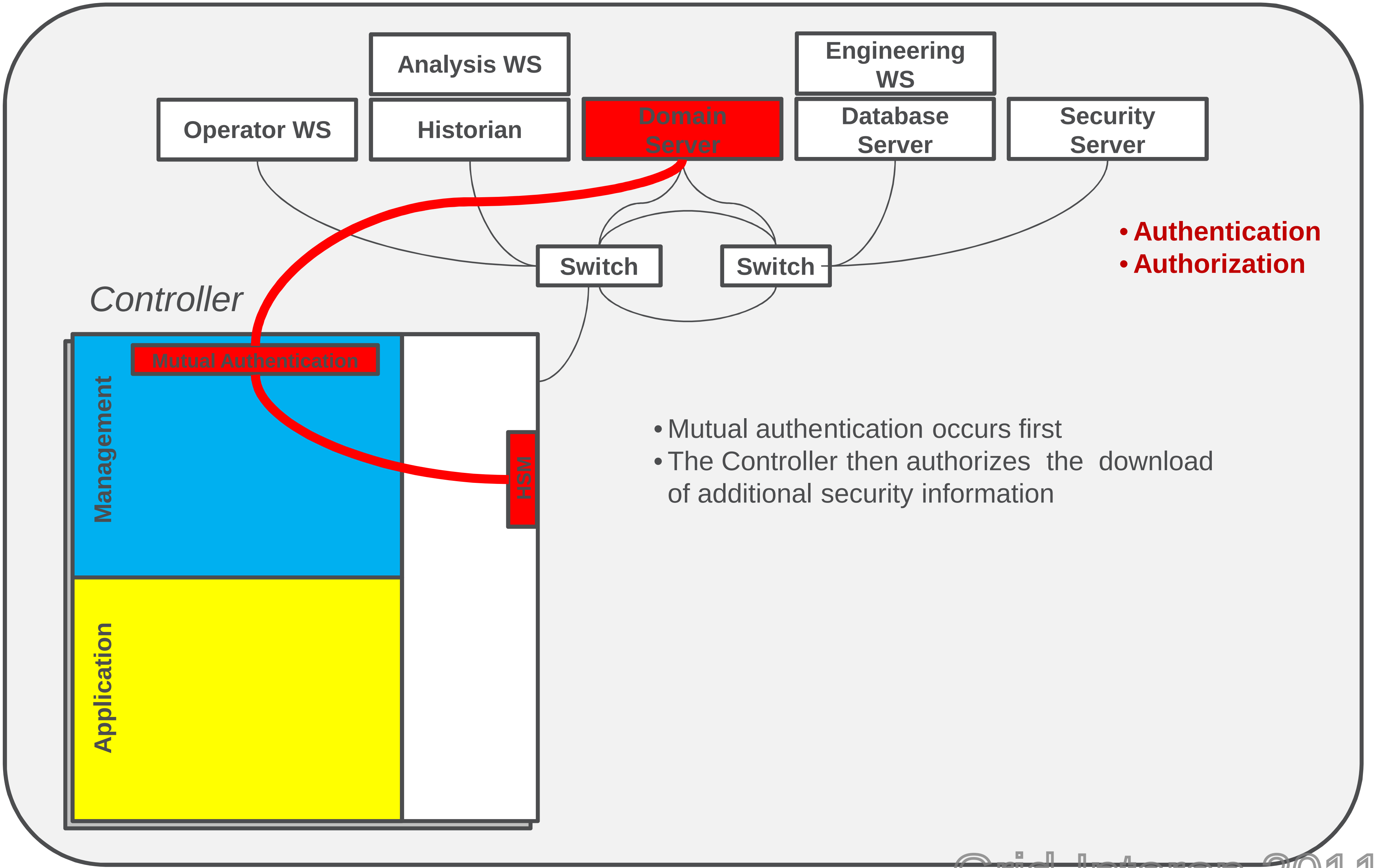
It self-generates and hides the secret key that identifies the device.

It manages the public key as well as the key management functions over the lifetime of the device.

It also maintains the secure clock for the device.

An example of a tailored trustworthy space built using the **Security Fabric** components:

Step two is to use the secure identity to mutually authenticate and get credentials from the Domain Server that uses Active Directory and its Kerberos PKINIT service meant to support embedded devices.



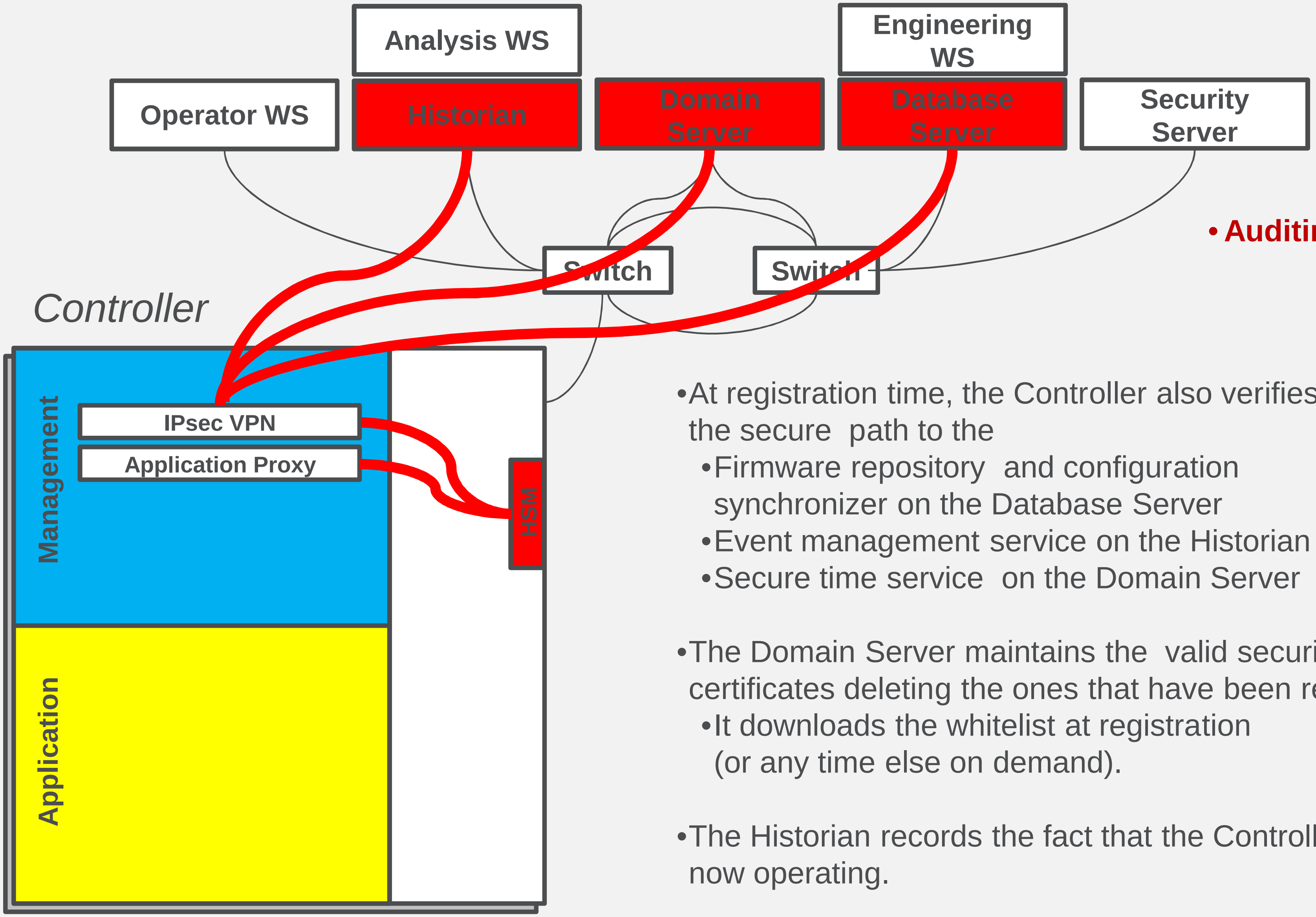
- **Authentication**
- **Authorization**

- Mutual authentication occurs first
- The Controller then authorizes the download of additional security information

An example of a tailored trustworthy space built using the **Security Fabric** components.

Step three is to use the secure credentials exchange to determine the authentic paths to important management servers, and to download the up-to-date whitelist.

McAfee



- **Auditing**

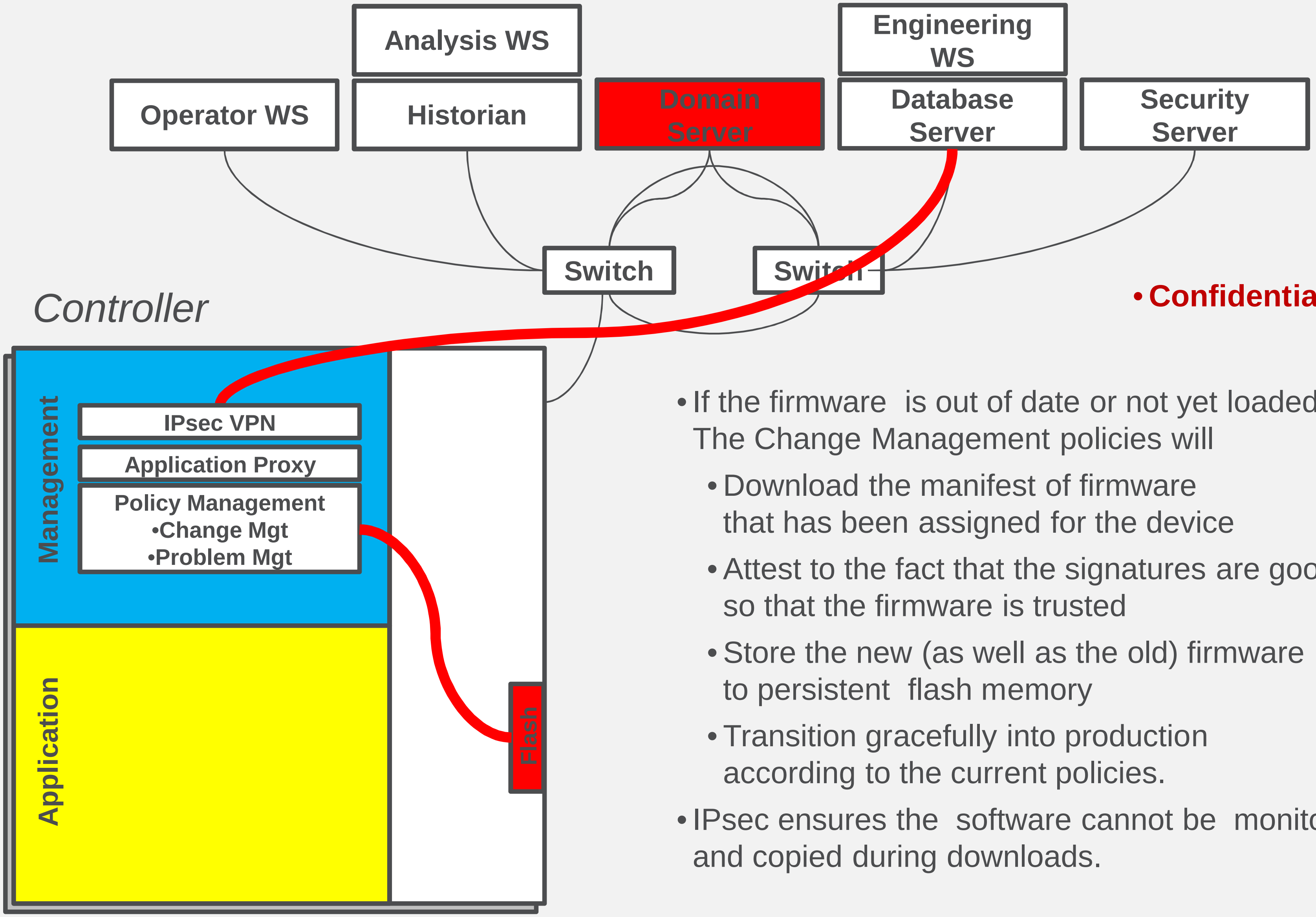
- At registration time, the Controller also verifies the secure path to the
  - Firmware repository and configuration synchronizer on the Database Server
  - Event management service on the Historian
  - Secure time service on the Domain Server

- The Domain Server maintains the valid security certificates deleting the ones that have been revoked
  - It downloads the whitelist at registration (or any time else on demand).

- The Historian records the fact that the Controller is now operating.

An example of a tailored trustworthy space built using the **Security Fabric** components.

Step four is to update the firmware to the latest rev if it is out of date.

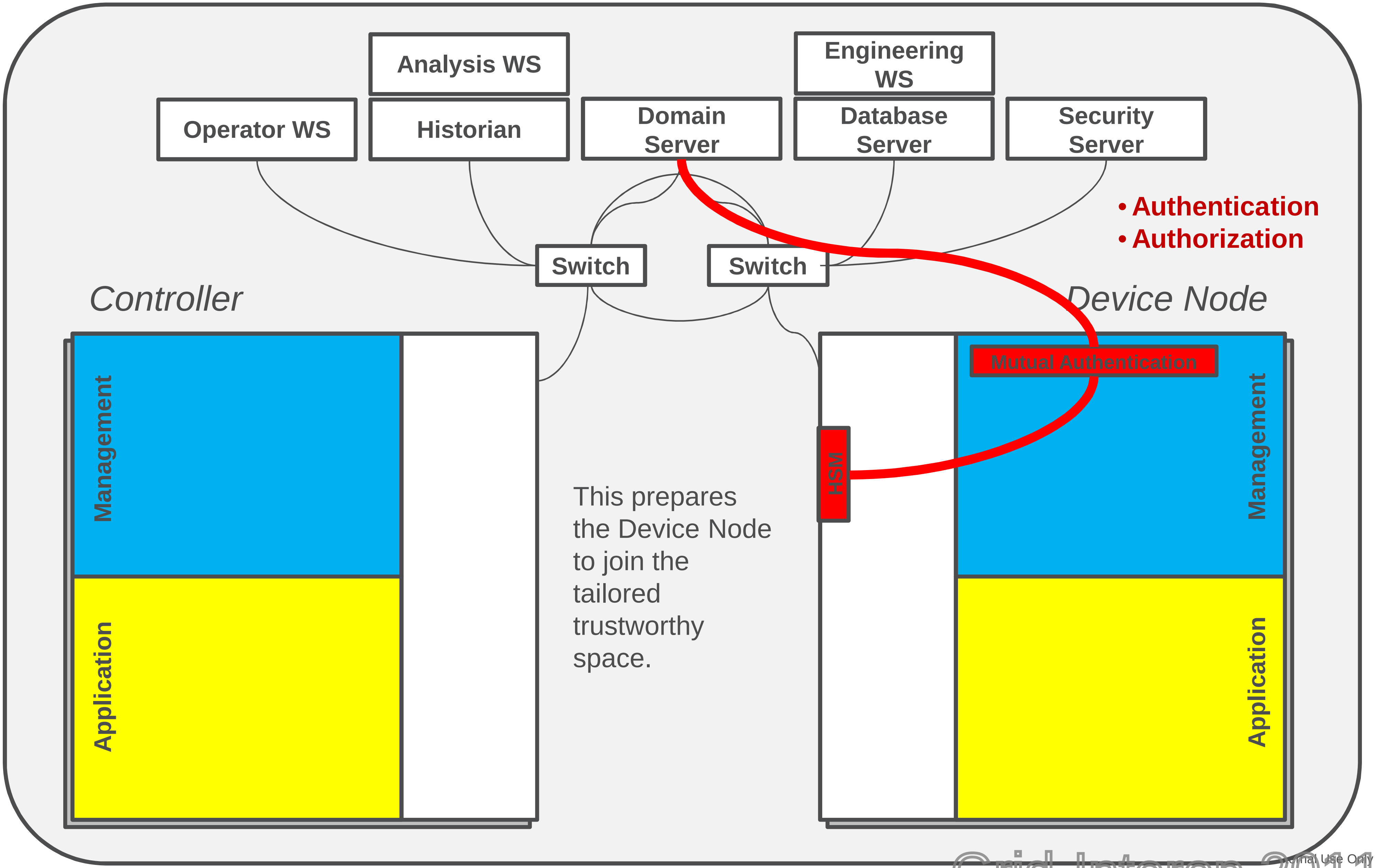


- **Confidentiality**

- If the firmware is out of date or not yet loaded. The Change Management policies will
  - Download the manifest of firmware that has been assigned for the device
  - Attest to the fact that the signatures are good so that the firmware is trusted
  - Store the new (as well as the old) firmware to persistent flash memory
  - Transition gracefully into production according to the current policies.
- IPsec ensures the software cannot be monitored and copied during downloads.

An example of a tailored trustworthy space built using the **Security Fabric** components.

All Device Nodes that want to be part of the Security Fabric must also authenticate with the Domain Server (the trusted third party) whenever they power up.

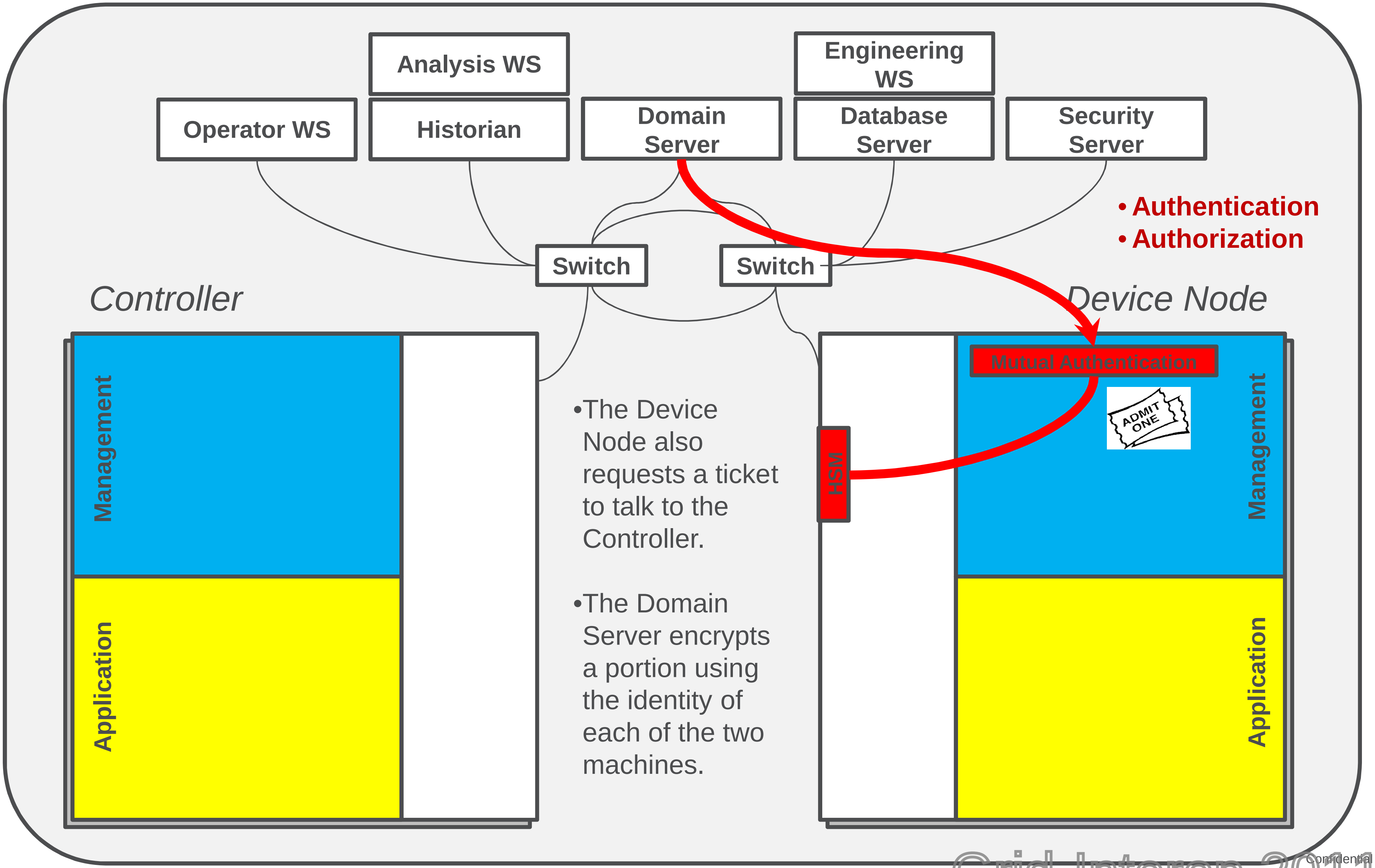


- Authentication
- Authorization

This prepares the Device Node to join the tailored trustworthy space.

An example of a tailored trustworthy space built using the **Security Fabric** components.

The authentication ticket received from the Domain Server contains a section encrypted by the Device Node public identity key plus a section encrypted by the Controller public identity key.

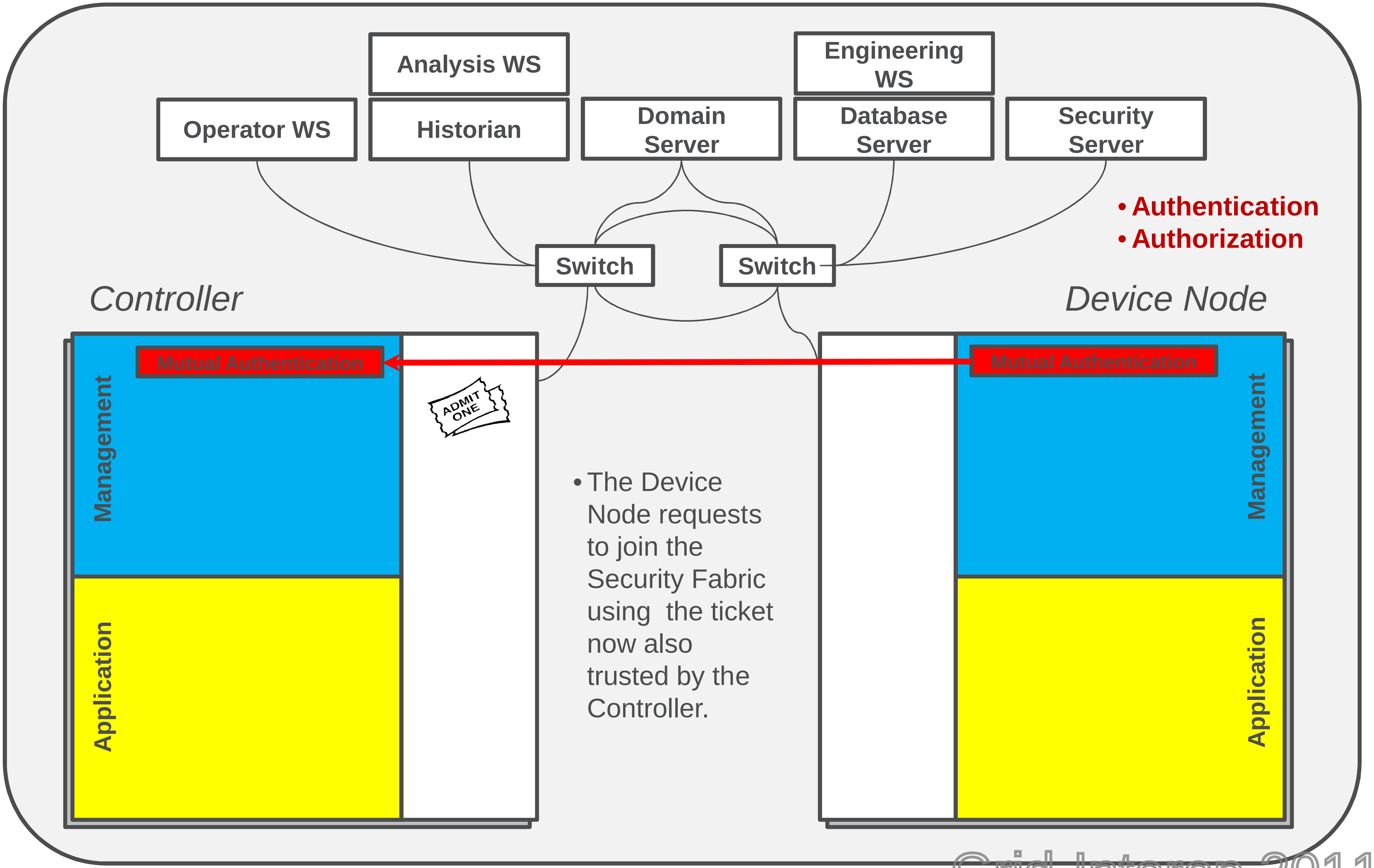


- **Authentication**
- **Authorization**

- The Device Node also requests a ticket to talk to the Controller.
- The Domain Server encrypts a portion using the identity of each of the two machines.

An example of a tailored trustworthy space built using the **Security Fabric** components.

The next step is for the Device Node to establish secure communications with the Controller.

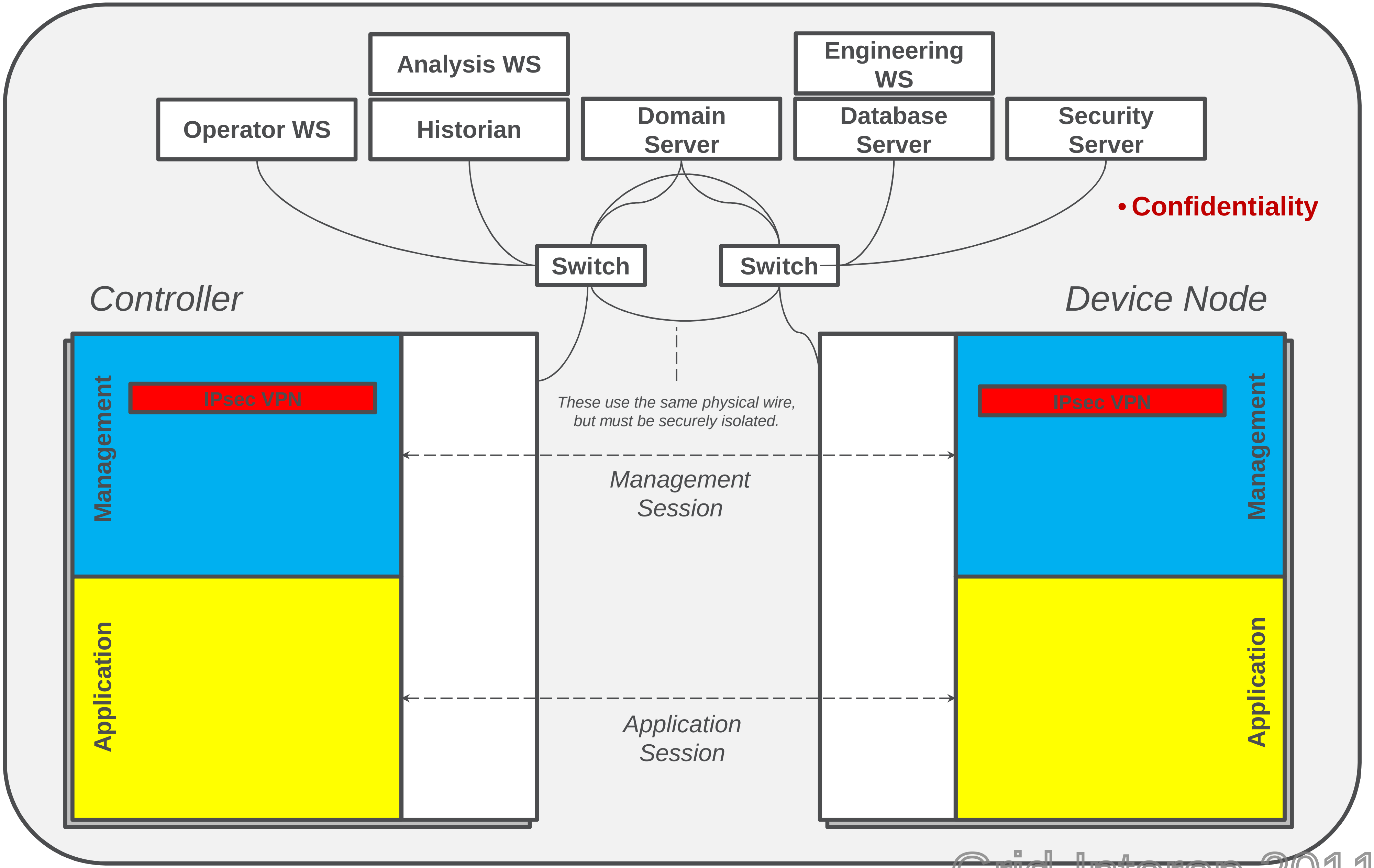


- **Authentication**
- **Authorization**

- The Device Node requests to join the Security Fabric using the ticket now also trusted by the Controller.

An example of a tailored trustworthy space built using the **Security Fabric** components.

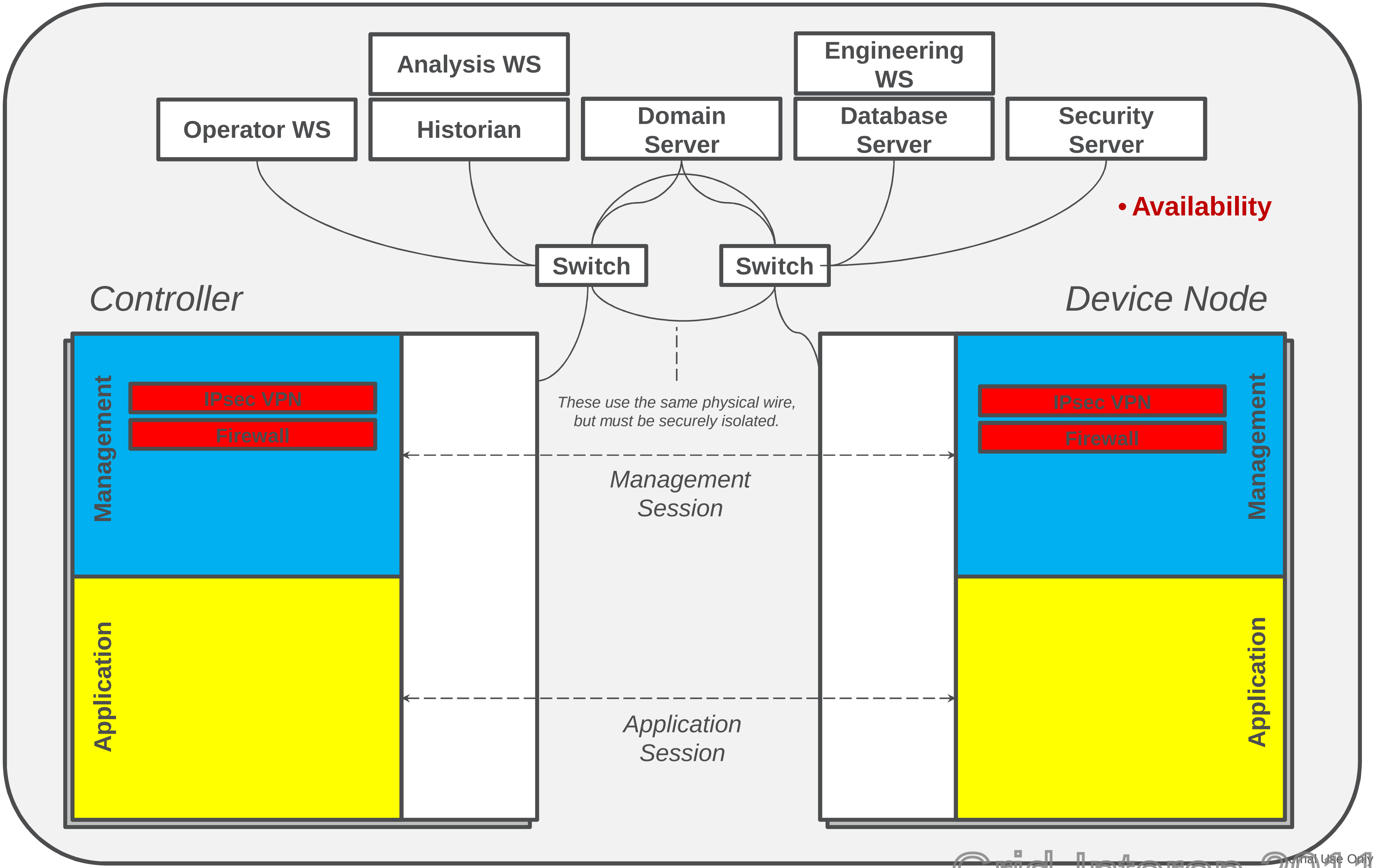
Once authenticated, the device node can proceed to establish two secure paths to the Controller: one for management purposes and one for application purposes.



- Confidentiality

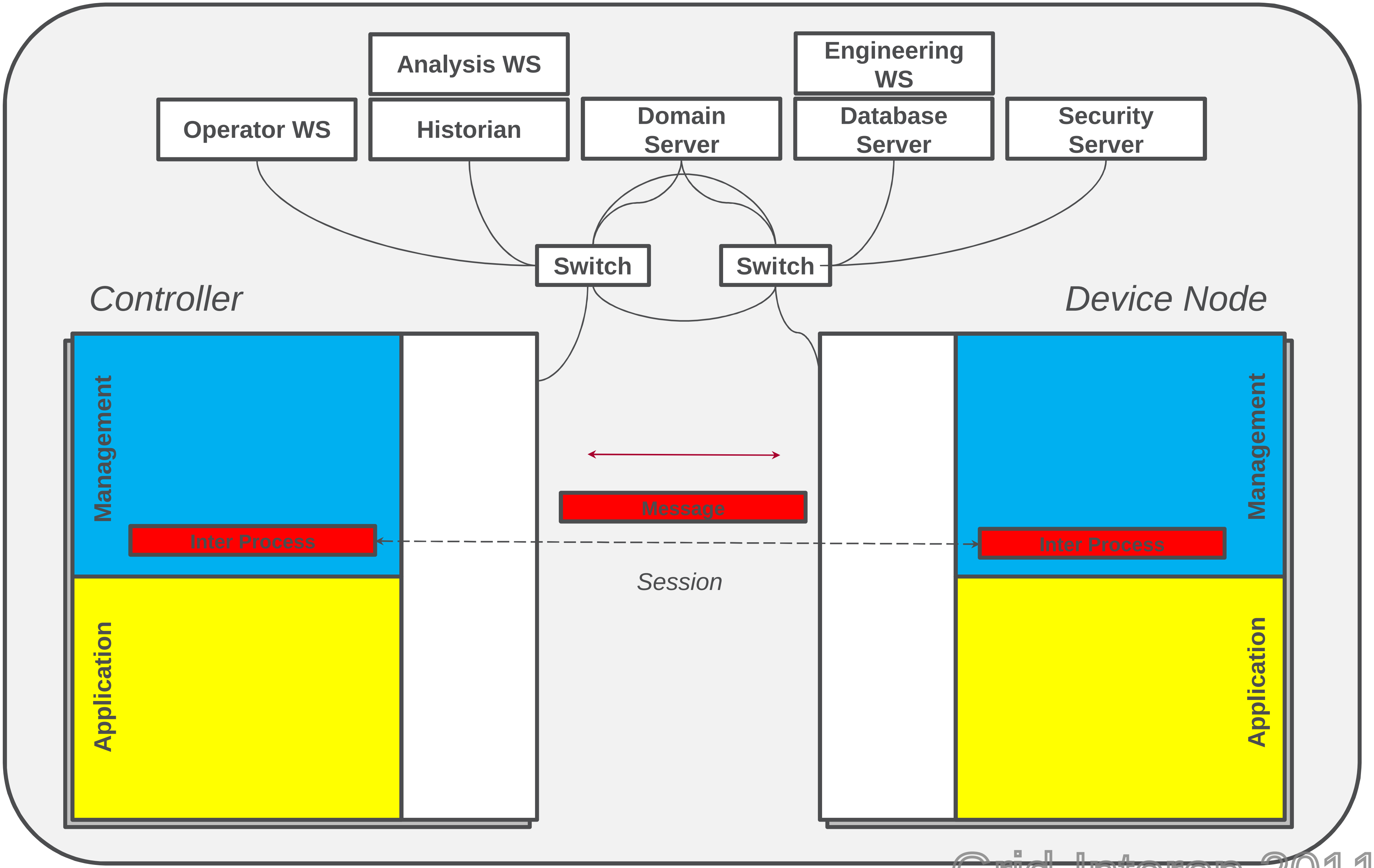
An example of a tailored trustworthy space built using the **Security Fabric** components.

The small embedded firewall in the communications path protects against denial of service attacks as well as a number of sophisticated malware attacks.



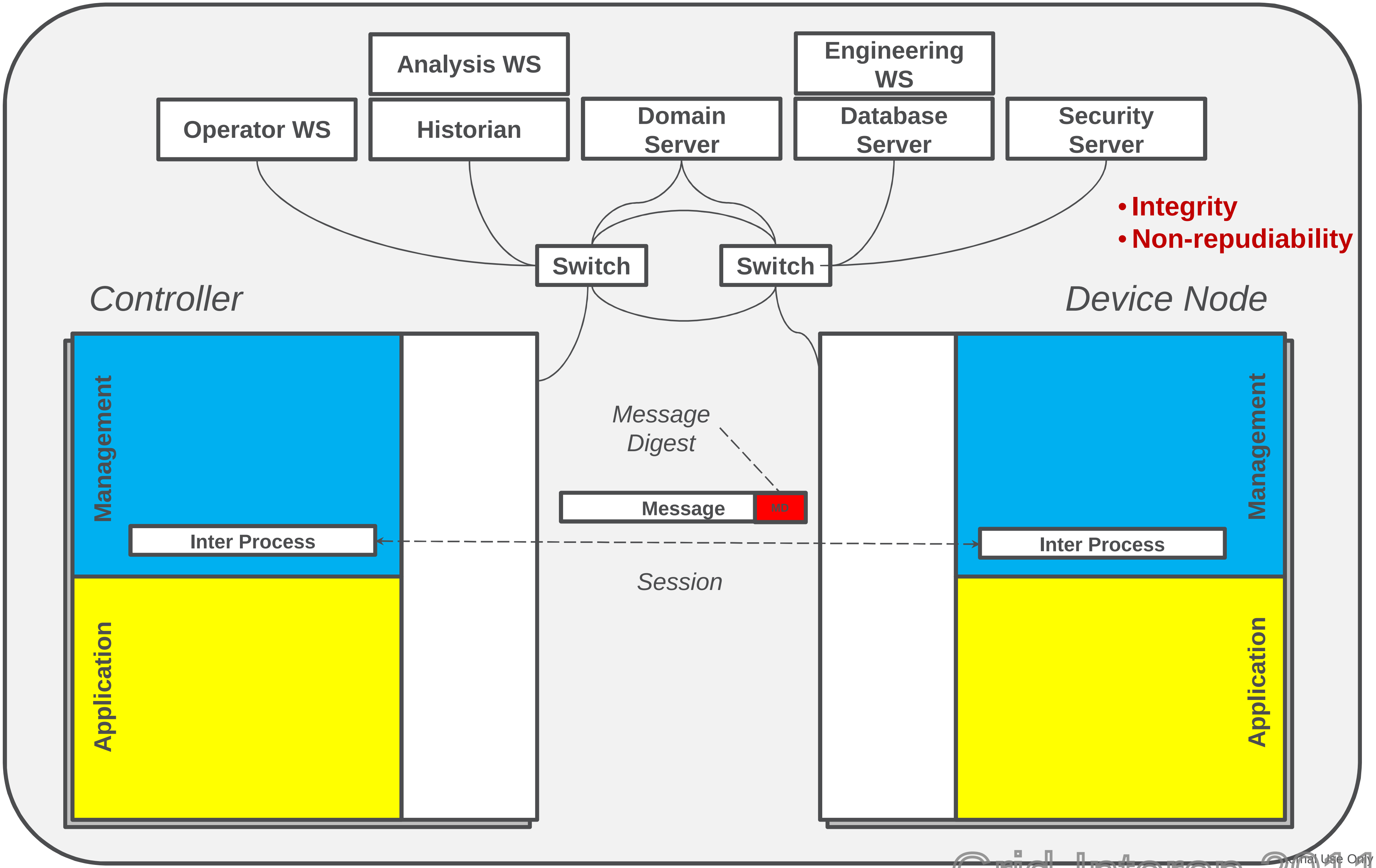
An example of a tailored trustworthy space built using the **Security Fabric** components.

The inter-process communications services of the middleware uses messages to communicate back and forth between the Controller and the Device Node over the secure sessions.



An example of a tailored trustworthy space built using the **Security Fabric** components.

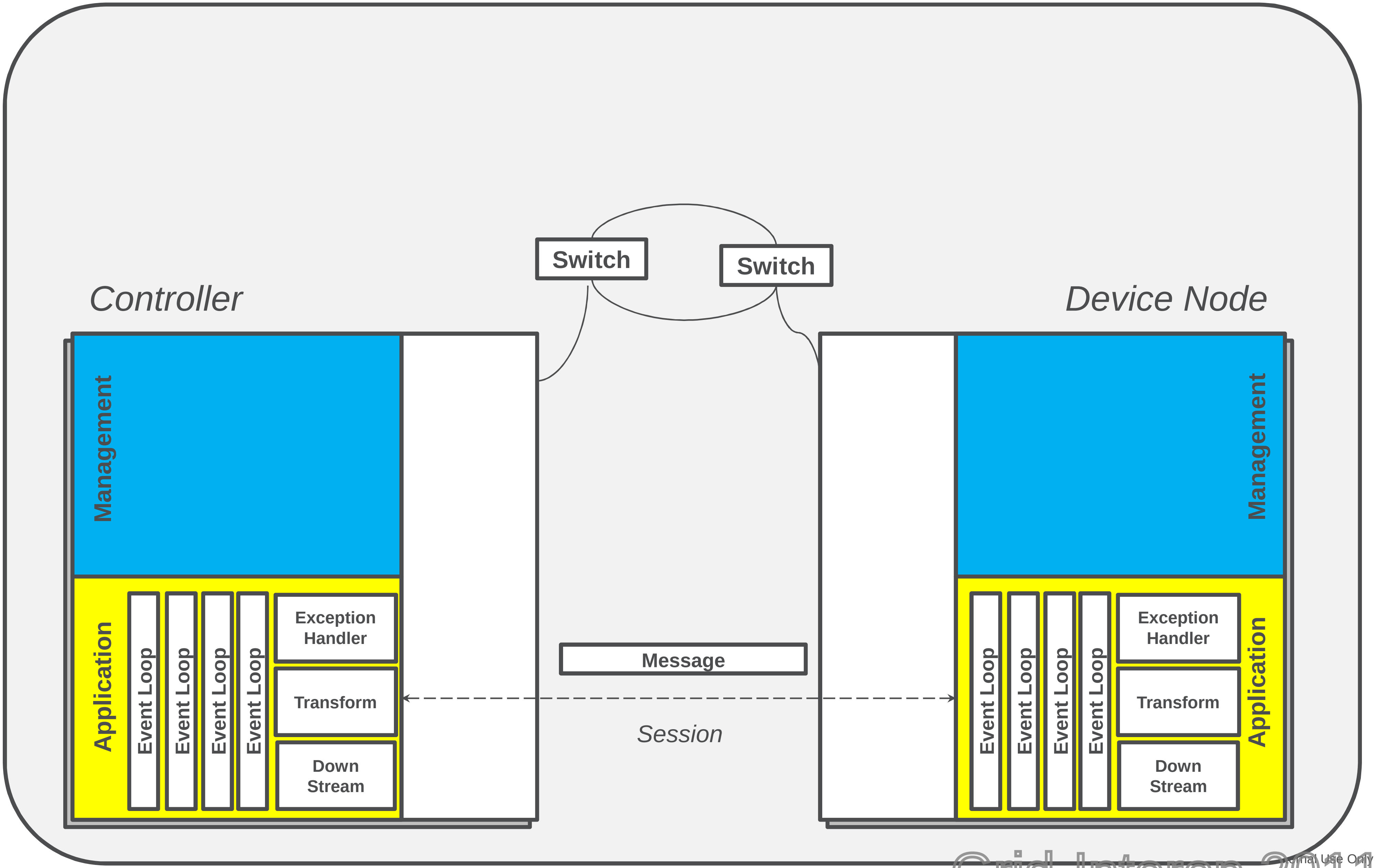
The inter-process communications services computes a secure message digest and appends it to the end of each message to ensure that the message is never altered in flight.



- Integrity
- Non-repudiability

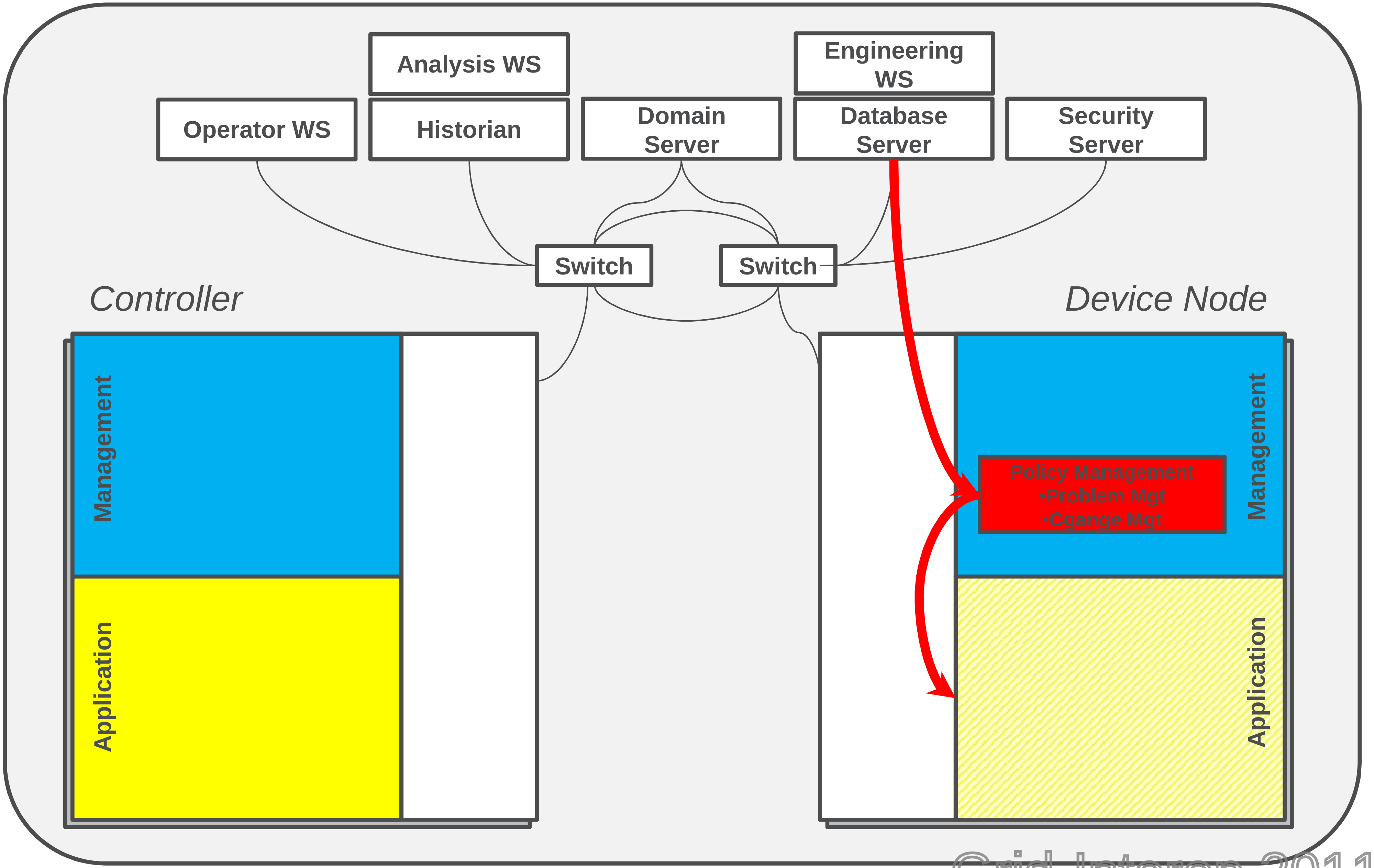
An example of a tailored trustworthy space built using the **Security Fabric** components.

So now, the Controller and the Device Node can commence doing real work without ever having to think about the security aspects of the system.



An example of a tailored trustworthy space built using the **Security Fabric** components.

If necessary, you can have the management system automatically download extra telemetry to monitor an attack while it is occurring or safely download a repaired application for remediation.



An example of a tailored trustworthy space built using the **Security Fabric** components.

In Summary,

SGIP
Winter

Security Fabric

provides the features for embedded security based on the NIST-IR 7628 guidelines.

It also provides a framework for a tailored trustworthy space.